БАКАЛАВРСЬКА РОБОТА

БР. ІП - 30.00.00.000 ПЗ

Група ІП-21-2

Мазур Ніна

2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Мазур Ніна Богданівна

(прізвище, ім'я, по батькові)

УДК 004.4

(індекс)

БАКАЛАВРСЬКА РОБОТА

Імплементація концепцій та протоколів безпеки локальної обчислювальної мережі

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач освітнього рівня Мазур Н.Б.

(підпис, ініціали та прізвище здобувача)

Науковий керівник Храбатин Роман Ігорович, к.ф.-м.н., доцент

(підпис, прізвище, ім'я, по батькові, науковий ступінь, вчене звання керівника)

Допущено до захисту
Завідувач кафедри

доц. Бандура В.В.

(посада) (підпис) (дата) (ініціали та прізвище)

Івано-Франківськ – 2025

Міністерство освіти і науки України
Івано-Франківський національний технічний університет нафти і газу

Інститут, факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Освітньо-кваліфікаційний рівень бакалавр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**
доц. В.В. Бандура
“ ____ ” _____2025 р.

ЗАВДАННЯ

НА ДИПЛОМНУ РОБОТУ БАКАЛАВРА СТУДЕНТОВІ

Мазур Ніні Богданівні

(прізвище, ім’я, по-батькові)

1. Тема проекту (роботи) “ Імплементація концепцій та протоколів безпеки локальної обчислювальної мережі ”

керівник проекту (роботи) Храбатин Роман Ігорович

затверджені наказом закладу вищої освіти від “ 28 ” квітня 2025 р. № 264/7

2. Строк подання студентом проекту (роботи) 11 червня 2025 р.

3. Вихідні дані до проекту (роботи) Результати і матеріали отримані під час проходження переддипломної практики

4. Зміст розрахунково - пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз технологій, стандартів і протоколів безпеки локальної обчислювальної мережі
2. Методологія дослідження та умови проведення моделювання
3. Принципи безпеки і техніки шифрування бездротових мереж
4. Імплементація стандартів та протоколів безпеки локальної обчислювальної мережі
5. Опис процесів імітаційного моделювання злому ключів безпеки

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

1. Алгоритм потокового шифрування RC4 (рис. 1.1)
2. Архітектура та еволюція стандартів безпеки Wi-Fi Protected Access (WPA) (рис. 1.2)
3. Фази і операції стандарту IEEE 802.11i (рис. 1.3)
4. Кадр IEEE 802.11 (рис. 2.1)
5. Конструкція розширеного MPDU WEP (рис. 2.3)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання **28 квітня 2025 р.**

Керівник _____
(підпис)

Завдання прийняв до виконання_____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту	Примітка
1	Аналіз технологій, стандартів і протоколів безпеки локальної обчислювальної мережі	11.05.2025	виконано
2	Методологія дослідження та умови проведення моделювання	23.05.2025	виконано
3	Принципи безпеки і техніки шифрування бездротових мереж	29.05.2025	виконано
4	Імплементація стандартів та протоколів безпеки локальної обчислювальної мережі	04.06.2025	виконано
5	Опис процесів імітаційного моделювання злому ключів безпеки	07.06.2025	виконано
6	Оформлення пояснювальної записки дипломної роботи завідувачем кафедри	11.06.2025	виконано

Студент – дипломник _____
(підпис)

Керівник роботи _____
(підпис)

АНОТАЦІЯ

Бакалаврська робота містить 76 сторінок, 36 рисунків, список використаних джерел із 34 найменуваннями.

Метою роботи є аналіз стандартів і протоколів безпеки WLAN, дослідження їхніх вразливостей, а також імітаційне моделювання атак з метою оцінки стійкості кожного із розглянутих рішень.

Об'єктом дослідження є протоколи безпеки бездротових локальних мереж, а предметом – методи їх реалізації та захисту інформації в умовах реальних і змодельованих атак.

Предмет дослідження - методи та протоколи забезпечення інформаційної безпеки в бездротових локальних мережах, зокрема WEP, WPA, WPA2 та їх реалізації.

В першому розділі проведено всебічний аналіз протоколів WEP, WPA, WPA2, їхніх слабких місць та типових атак, що підтверджує необхідність вдосконалення існуючих рішень.

В другому розділі розглянуто основи шифрування та аутентифікації в WLAN, визначено технічні характеристики та вразливості WEP, WPA і WPA2, що дозволило зрозуміти природу їх компрометації.

В третьому розділі моделювання показало, що протоколи WEP і WPA-TKIP уразливі до атак, тоді як WPA2 демонструє вищий рівень стійкості, однак також потребує додаткових заходів безпеки в складних середовищах.

Висновок: проведено аналіз архітектури протоколів, алгоритмів шифрування й автентифікації, а також здійснено імітаційне моделювання типових атак на WLAN з використанням спеціалізованого програмного забезпечення.

КЛЮЧОВІ СЛОВА: ЛОКАЛЬНА ОБЧИСЛЮВАЛЬНА МЕРЕЖА; WLAN; ІНФОРМАЦІЙНА БЕЗПЕКА; ПРОТОКОЛИ WEP, WPA, WPA2; TKIP; МОДЕЛЮВАННЯ АТАК; ШИФРУВАННЯ; АВТЕНТИФІКАЦІЯ.

ANNOTATION

The bachelor's thesis contains 76 pages, 36 figures, a list of used sources with 34 names.

The purpose of the work is to analyze WLAN security standards and protocols, study their vulnerabilities, as well as simulate attacks in order to assess the stability of each of the considered solutions.

The object of the study is security protocols of wireless local area networks, and the subject is methods of their implementation and information protection in conditions of real and simulated attacks.

The subject of the study is methods and protocols for ensuring information security in wireless local area networks, in particular WEP, WPA, WPA2 and their implementation.

The first section provides a comprehensive analysis of the WEP, WPA, WPA2 protocols, their weaknesses and typical attacks, which confirms the need to improve existing solutions.

The second section considers the basics of encryption and authentication in WLAN, determines the technical characteristics and vulnerabilities of WEP, WPA and WPA2, which allowed us to understand the nature of their compromise.

In the third section, the simulation showed that the WEP and WPA-TKIP protocols are vulnerable to attacks, while WPA2 demonstrates a higher level of resilience, but also requires additional security measures in complex environments.

Conclusion: The analysis of the protocol architecture, encryption and authentication algorithms was carried out, and simulation of typical attacks on WLAN was carried out using specialized software.

KEYWORDS: LOCAL AREA NETWORK; WLAN; INFORMATION SECURITY; WEP, WPA, WPA2 PROTOCOLS; TKIP; ATTACK MODELING; ENCRYPTION; AUTHENTICATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AES - Advanced Encryption Standard

AP - Access point

ARC4 - Alleged RC4

BSSID- Basic Service Set Identifier

BSS - Basic Service Set

CCMP- Counter Mode with Cipher Block Chaining Message

CRC - Cyclic Redundancy Check

DA - Destination Address

DS - Distribution System

EAPOL- Extensible Authentication Protocol Over LAN

EAP - Extensible Authentication Protocol

ESSID- Extended Service Set Identifier

FCS - Frame Check Sequence

IV - Initialization Vector

KSA - Key Scheduling Algorithm

LLC - Logical Link Control

LSB - Least Significant Bit

MIC - Message Integrity Code

MPDU- MAC Protocol Data Unit

OP - Operation

PRNG- Pseudo Random Number Generator

SA - Source Address

ВСТУП

У сучасних умовах широкого впровадження бездротових технологій передавання даних питання інформаційної безпеки у локальних обчислювальних мережах (ЛОМ), зокрема бездротових (WLAN), набуває особливої ваги. Зростання кількості пристроїв, підключених до мереж, підвищує ризики несанкціонованого доступу, витоку даних, маніпуляцій із трафіком та інших видів кіберзагроз. Незважаючи на наявність усталених стандартів безпеки (WEP, WPA, WPA2), значна частина вразливостей все ще може бути експлуатована зловмисниками, особливо у випадках неправильного налаштування або використання застарілих протоколів. У зв'язку з цим актуальним є проведення системного аналізу рівня захищеності різних протоколів, а також практична перевірка ефективності їх імплементації в умовах змодельованого середовища.

Забезпечення захисту інформації в локальних обчислювальних мережах, особливо бездротових, є однією з ключових проблем інформаційної безпеки. З розвитком технологій Wi-Fi все більше даних передається повітряним середовищем, що робить такі мережі вразливими до перехоплення трафіку, атак типу «людина посередині», підбору ключів та інших типів несанкціонованого доступу. Водночас впровадження належних криптографічних протоколів та автентифікаційних механізмів може істотно підвищити рівень безпеки таких систем.

Актуальність роботи

У сучасному світі стрімке зростання використання бездротових технологій, зокрема Wi-Fi, зумовлює потребу в надійних механізмах забезпечення інформаційної безпеки. Бездротові локальні обчислювальні мережі (WLAN) широко використовуються в державних установах, бізнесі та побуті, однак вони залишаються вразливими до різноманітних атак, пов'язаних із перехопленням трафіку, підміною автентифікації та

компрометацією ключів шифрування. Через це особливої ваги набуває дослідження стандартів безпеки WLAN — WEP, WPA, WPA2 — та їхніх слабких місць. Вивчення уразливостей, тестування моделей атак і дослідження ефективності захисних протоколів має як теоретичне, так і практичне значення, сприяючи вдосконаленню механізмів захисту інформації в умовах зростаючої кіберзагрози.

У науковій та технічній літературі приділяється значна увага питанням стандартизації безпеки WLAN, однак реальна ефективність протоколів значною мірою залежить від їх практичної реалізації та конфігурації. Застарілі протоколи, як-от WEP, вже не здатні забезпечити прийнятний рівень захисту, у той час як більш сучасні – WPA2 і WPA3 – потребують правильного впровадження й постійного оновлення для протидії новітнім загрозам.

Метою цієї роботи є аналіз стандартів і протоколів безпеки WLAN, дослідження їхніх вразливостей, а також імітаційне моделювання атак з метою оцінки стійкості кожного із розглянутих рішень.

Завдання дослідження

1. Провести аналіз сучасних технологій та стандартів безпеки WLAN.
2. Дослідити алгоритми шифрування та методи автентифікації у WEP, WPA, WPA2.
3. Виконати імітаційне моделювання атак на бездротові протоколи.
4. Виявити практичні уразливості та оцінити ефективність реалізованих протоколів.
5. Надати висновки щодо доцільності використання стандартів у реальних умовах.

Об’єктом дослідження є протоколи безпеки бездротових локальних мереж, а предметом – методи їх реалізації та захисту інформації в умовах реальних і змодельованих атак.

Предмет дослідження - методи та протоколи забезпечення інформаційної безпеки в бездротових локальних мережах, зокрема WEP, WPA, WPA2 та їх реалізації.

Методи дослідження

- Теоретичний аналіз протоколів безпеки IEEE 802.11.

- Моделювання атак із використанням спеціалізованого ПЗ (наприклад, Aircrack-ng).

- Порівняльний аналіз ефективності протоколів.

- Метод імітаційного моделювання для практичної перевірки вразливостей.

Наукова новизна

Полягає у розробці та моделюванні сценаріїв атак на основі сучасних протоколів WPA та WPA2 з метою експериментального підтвердження їх уразливостей та формування рекомендацій щодо підвищення захищеності WLAN.

Практичне застосування

Результати можуть бути використані в адміністраторами мереж, системними безпековими аналітиками та IT-фахівцями для удосконалення систем захисту бездротових мереж в організаціях, підприємствах та домашньому середовищі.

Бакалаврська робота містить 77 сторінок, 37 рисунків, 3 розділи список використаних джерел із 34 найменуваннями.

РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЙ, СТАНДАРТІВ І ПРОТОКОЛІВ БЕЗПЕКИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

1.1. Дослідження вразливостей бездротових локальних мереж (WLAN)

Бездротова безпека визначається як сукупність заходів, спрямованих на запобігання несанкціонованому доступу до комп'ютерних систем, що функціонують у бездротових мережах, а також їх пошкодженню. Серед ранніх та найпоширеніших стандартів бездротової безпеки виділяють Wired Equivalent Privacy (WEP) та Wi-Fi Protected Access (WPA). Проте, WEP є відомо слабким стандартом, і його ключ може бути скомпрометований за лічені хвилини з використанням базового апаратного забезпечення та загальнодоступного програмного забезпечення [1]. WPA був розроблений як оперативна альтернатива для посилення безпеки порівняно з WEP. Незважаючи на це, залишаються вразливості в стандартах безпеки, що пропонуються цими протоколами, що створює значні виклики для розробки витончених механізмів безпеки інформації та забезпечення надійного захисту даних під час передачі [2].

У сучасному цифровому ландшафті бездротові локальні мережі (WLAN) набули повсюдного поширення, ставши невід'ємною частиною інфраструктури в таких місцях, як університетські кампуси, міжнародні аеропорти, приватні помешкання та публічні заклади харчування. Зі зростанням цієї експоненціальної інтеграції безпека бездротових мереж стає критично важливою для забезпечення конфіденційності, цілісності та доступності даних. Це дослідження присвячене аналізу механізмів безпеки, що використовуються в WLAN, зокрема Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) та 802.11i (WPA2). Основною метою роботи є демонстрація вразливостей цих систем через здійснення практичних атак.

Надається короткий огляд принципів роботи, архітектури та алгоритмів, що лежать в основі кожного протоколу. Експериментальна частина включає успішні атаки на мережі WEP та WPA2, які були проведені в ad-hoc конфігурації з використанням трьох ноутбуків, оснащених Wi-Fi модулями.

Широке впровадження технологій WLAN, заснованих на стандартах IEEE 802.11, революціонізувало спосіб підключення до мережі, пропонуючи гнучкість та мобільність, недосяжні для дротових систем. Однак ця зручність супроводжується значними проблемами безпеки. Відкритий ефірний простір, через який передаються дані, робить бездротові мережі особливо вразливими до перехоплення, несанкціонованого доступу та інших зловмисних дій. Історично розробка стандартів безпеки для WLAN була поступовим процесом, що відображає еволюцію загроз та вдосконалення криптографічних методів. Це дослідження систематизує знання про ключові протоколи безпеки WLAN та емпірично демонструє їхні слабкі сторони.

Еволюція безпеки WLAN відбувалася через кілька ітерацій, кожна з яких намагалася виправити недоліки попередньої.

1.2. Представлення алгоритму стандарту безпеки Wired Equivalent Privacy (WEP)

WEP був першим стандартом безпеки для 802.11, розробленим для забезпечення рівня конфіденційності, порівнянного з дротовими мережами. Він використовує потоковий шифр RC4 (Rivest Cipher 4) для шифрування даних та 24-бітовий вектор ініціалізації (IV) разом з статичним попередньо погодженим ключем для генерації потоку ключа.

Принцип роботи полягає в тому, що відправник об'єднує статичний ключ з IV, передає їх через RC4 для створення потоку ключа, який потім XOR-ується з даними. IV передається у відкритому вигляді.

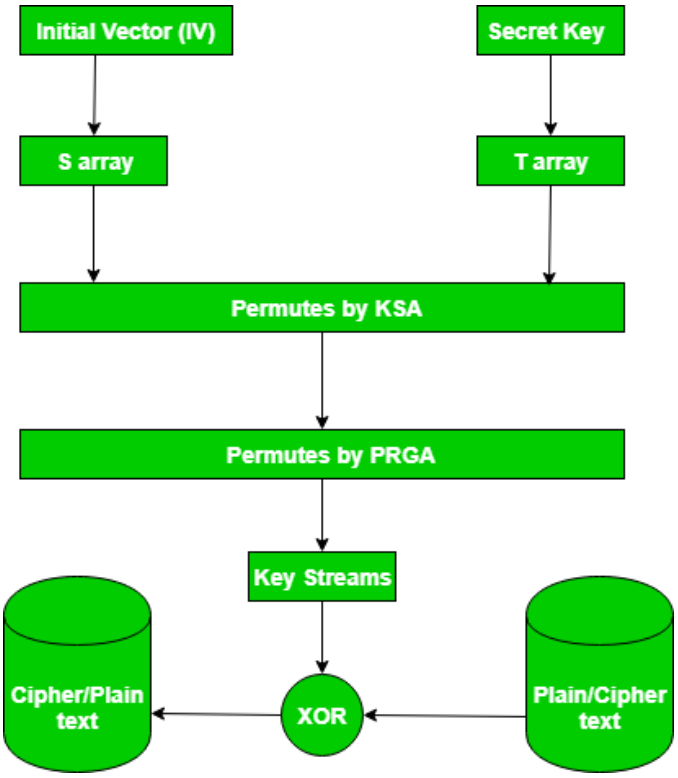

Рисунок 1.1 - Алгоритм потокового шифрування RC4

Ось як працює RC4, згідно з представленим алгоритмом (рис. 1.1):

1. Ініціалізація (Key Scheduling Algorithm - KSA)

На початковому етапі відбувається ініціалізація та пермутація внутрішнього стану RC4 за допомогою секретного ключа та, у випадку WEP, вектора ініціалізації.

- Initial Vector (IV). Це 24-бітовий вектор ініціалізації, який додається до секретного ключа в деяких реалізаціях (як WEP). Він змінюється для кожного сеансу або пакета, щоб уникнути повторного використання того ж потоку ключа.

- Secret Key. Це основний секретний ключ, узгоджений між відправником і отримувачем. Його довжина може варіюватися.

- S array (S-масив). Це внутрішній стан алгоритму, який є масивом з 256 байтів, проіндексованих від 0 до 255. Спочатку він ініціалізується послідовно: S[i]=i для i=0…255.

- T array (T-масив). Цей масив також має 256 байтів. Він використовується для зберігання розширеного секретного ключа. Якщо секретний ключ коротший за 256 байтів, він повторюється по T-масиву; наприклад, T[i]=Key[i(modKeyLength)].

Після ініціалізації, відбувається етап "Permutes by KSA" (перестановка за допомогою алгоритму розкладу ключів):

- S-масив проходить через процес перестановки, керований T-масивом. Це робиться для того, щоб зробити S-масив "випадковим" чином перетасованим на основі секретного ключа. Це гарантує, що два різних ключі призведуть до абсолютно різних початкових перестановок S-масиву.

2. Генерація потоку ключів (Pseudo-Random Generation Algorithm - PRGA)

Після фази KSA, коли S-масив вже перемішаний, починається генерація власне потоку ключа. Цей етап позначений як "Permutes by PRGA" (перестановка за допомогою псевдовипадкового генератора).

Алгоритм використовує два покажчики, i та j, які спочатку встановлюються в 0.

На кожній ітерації:

- i збільшується на 1 (за модулем 256).
- j збільшується на S[i] (за модулем 256).
- Елементи S[i] та S[j] міняються місцями.
- Індекс t обчислюється як S[i]+S[j] (за модулем 256).
- Байт S[t] вибирається як наступний байт потоку ключа.

Цей процес генерує послідовність псевдовипадкових байтів, які формують "Key Streams" (потік ключів). Довжина цього потоку ключів дорівнює довжині даних, які потрібно зашифрувати або розшифрувати.

3. Шифрування/Дешифрування

Фінальний етап шифрування або дешифрування є симетричним і надзвичайно простим:

- Plain/Cipher text (Відкритий/Зашифрований текст): Це ваші вихідні дані (plaintext) для шифрування або зашифровані дані (ciphertext) для дешифрування.

- XOR: Кожен байт потоку ключів побайтно XOR-ується з відповідним байтом відкритого тексту (для шифрування) або зашифрованого тексту.

Результатом цієї операції XOR є Cipher/Plain text (Зашифрований/Відкритий текст). Якщо ви XOR-уєте відкритий текст з потоком ключа, ви отримуєте зашифрований текст. Якщо ви XOR-уєте зашифрований текст з тим самим потоком ключа, ви відновлюєте вихідний відкритий текст. Це робить RC4 дуже ефективним для двосторонньої роботи.

Незважаючи на початкові наміри, WEP виявився надзвичайно вразливим. Основні недоліки включають:

- Короткий IV: 24-бітовий IV є недостатнім, що призводить до частих повторень IV, особливо в мережах з високим трафіком. Це дозволяє атакуючим збирати пакети з однаковими IV та використовувати їх для криптоаналізу.

- Статичний ключ: Використання статичного ключа в поєднанні з повторюваними IV дозволяє дедуктивно виводити частини ключа або навіть весь ключ.

Недоліки в реалізації RC4, такі як вразливість до атак, заснованих на слабких IV (наприклад, атака Флуксера, атака Корека), дозволяють відновити ключ за відносно невелику кількість зібраних пакетів. CRC32, що використовується для перевірки цілісності, не є криптографічною хеш-функцією, що дозволяє зловмиснику маніпулювати пакетами без виявлення.

1.3. Опис Wi-Fi Protected Access (WPA)

WPA був розроблений Wi-Fi Alliance як тимчасове рішення для усунення критичних недоліків WEP до повного затвердження стандарту

802.11i. Він зберігає сумісність з існуючим обладнанням WEP, оновлюючи програмне забезпечення.

WPA вводить Temporal Key Integrity Protocol (TKIP) як основний протокол шифрування, який є обгорткою для RC4, додаючи покращення для уникнення проблем WEP. Включає:

- Динамічна зміна ключа: Ключі сесії автоматично змінюються для кожного пакета, значно зменшуючи ризик повторного використання IV.

- Розширена ініціалізація вектора: 48-бітовий IV робить повторення набагато менш імовірними.

- Message Integrity Code (MIC): Додано для забезпечення сильнішої перевірки цілісності повідомлень, запобігаючи несанкціонованим модифікаціям пакетів.

Хоча WPA є значним покращенням порівняно з WEP, його архітектура, все ще заснована на RC4 (через TKIP), робить його потенційно вразливим до певних атак, хоча й складніших, ніж для WEP.

Основними атаками є атаки, спрямовані на 4-стороннє рукостискання (Four-Way Handshake) та словникові атаки на попередньо погоджені ключі (PSK).

На верхньому рівні (рис. 1.2) знаходиться "WIFI Security" (Безпека Wi-Fi), що є загальним терміном, який охоплює всі протоколи та механізми, призначені для захисту бездротових мереж. Далі схема розгортається, показуючи еволюцію стандартів безпеки, об'єднаних під парасолькою "WPA (WIFI Protected Access) Standard".

Схема показує хронологічну послідовність та ієрархію основних протоколів безпеки Wi-Fi:

- WEP (Wired Equivalent Privacy). Хоча WEP не є частиною сімейства WPA, він згадується як початковий, але нині застарілий та вкрай вразливий стандарт безпеки. Схема відображає його окремо, підкреслюючи, що він був попередником WPA.

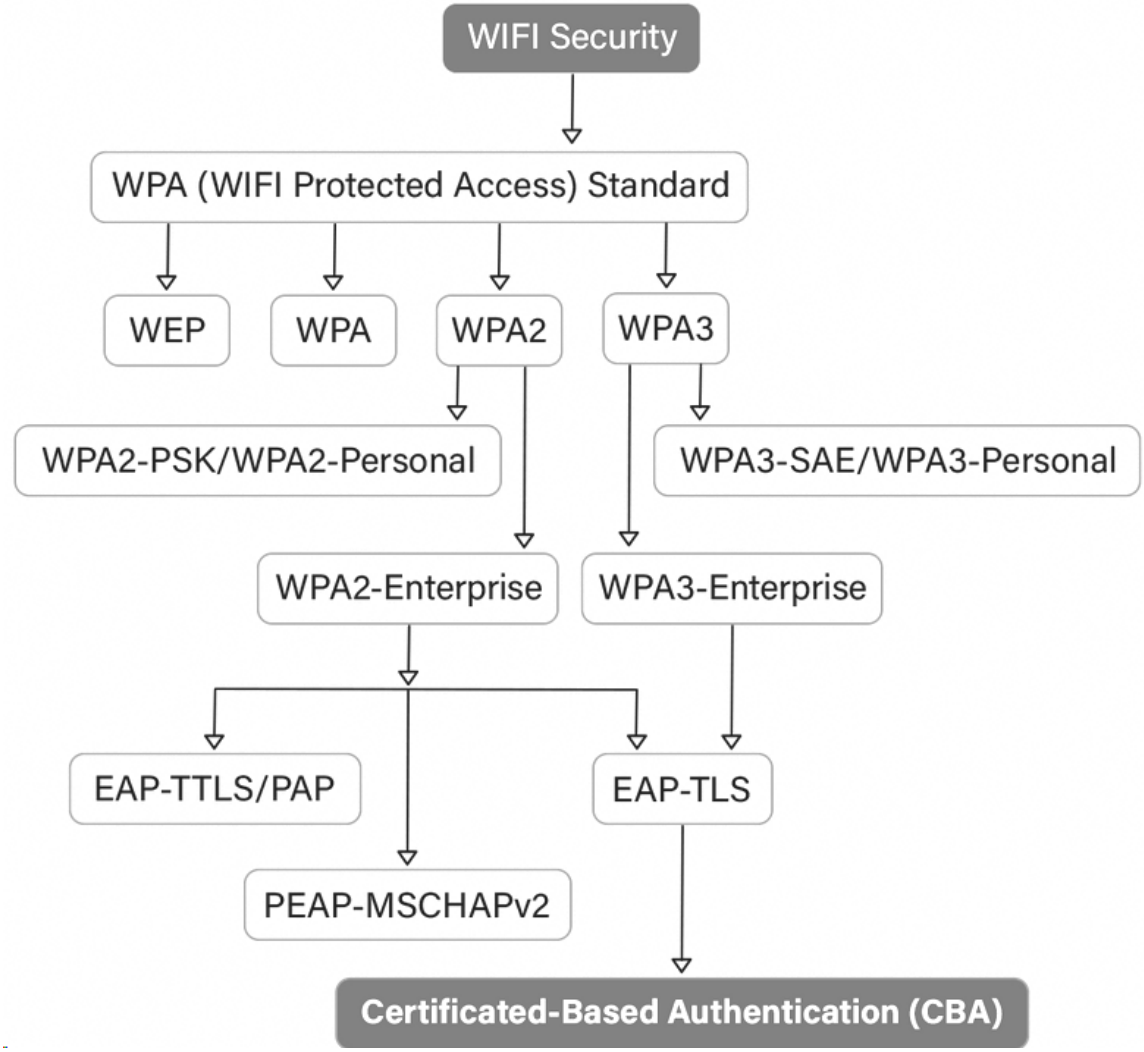

Рисунок 1.2 - Архітектура та еволюція стандартів безпеки Wi-Fi Protected Access (WPA)

- WPA2 (Wi-Fi Protected Access 2) - стандарт є поточний та найбільш широко використовуваний протокол безпеки Wi-Fi. Він базується на стандарті IEEE 802.11i і використовує AES (Advanced Encryption Standard) та CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), що робить його значно надійнішим за WEP та WPA.

- WPA3 (Wi-Fi Protected Access 3) - найновіший стандарт безпеки Wi-Fi, представлений у 2018 році. Він пропонує посилену безпеку порівняно з WPA2, включаючи більш надійне рукостискання, покращений захист від атак грубої сили та індивідуальне шифрування даних.

Обидва стандарти, WPA2 та WPA3, підтримують два основні режими роботи, призначені для різних сценаріїв використання:

WPA2-PSK / WPA2-Personal (Personal Mode):

- Призначений для домашніх мереж та малих офісів.

- Аутентифікація відбувається за допомогою попередньо погодженого ключа (Pre-Shared Key - PSK), тобто пароля, який потрібно ввести на кожному пристрої для підключення до мережі.

WPA2-Enterprise (Enterprise Mode):

- Призначений для великих організацій та підприємств.

- Використовує архітектуру на основі 802.1X та EAP (Extensible Authentication Protocol). Це дозволяє централізовану аутентифікацію користувачів за допомогою сервера аутентифікації (наприклад, RADIUS).

WPA3-SAE / WPA3-Personal (Personal Mode) - це аналог WPA2-Personal, але використовує протокол SAE (Simultaneous Authentication of Equals). SAE значно покращує безпеку рукостискання, надаючи захист від офлайн-атак грубої сили та забезпечуючи форвардну секретність.

WPA3-Enterprise (Enterprise Mode) - покращений варіант WPA2-Enterprise, що пропонує додаткові функції безпеки, такі як 192-бітова криптографічна сила та посилений захист від криптографічних атак.

Для режимів "Enterprise" (WPA2-Enterprise та WPA3-Enterprise) схема деталізує протоколи, що використовуються в рамках EAP для автентифікації:

EAP-TTLS/PAP (Tunneled Transport Layer Security / Password Authentication Protocol) - метод створює зашифрований тунель (TLS) для захисту процесу аутентифікації. Всередині цього тунелю можуть використовуватися менш захищені протоколи, такі як PAP, для передачі облікових даних (імені користувача та пароля).

PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol / Microsoft Challenge-Handshake Authentication Protocol, version 2) схожий на EAP-TTLS, також створює зашифрований TLS-тунель. Всередині тунелю для

аутентифікації часто використовується MSCHAPv2. Цей метод є дуже поширеним у корпоративних середовищах.

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) це найбільш безпечний метод аутентифікації EAP. Він вимагає як клієнтських, так і серверних цифрових сертифікатів для взаємної аутентифікації. Забезпечує найвищий рівень захисту та конфіденційності під час процесу аутентифікації.

На нижньому рівні схеми знаходиться "Certificated-Based Authentication (CBA)" (Аутентифікація на основі сертифікатів). Це кінцева мета для найбільш захищених корпоративних мереж, де аутентифікація не базується на паролях, а на цифрових сертифікатах, які набагато складніше скомпрометувати. EAP-TLS є ключовим протоколом, що забезпечує цю форму аутентифікації.

Узагальнюючи, схема демонструє, як бездротова безпека еволюціонувала від простих, але ненадійних методів до складних, багатошарових систем, які використовують криптографію високого рівня та сертифікати для захисту даних та автентифікації користувачів.

1.4. Особливості стандарту безпеки 802.11i (WPA2)

802.11i, комерційно відомий як WPA2, є поточним стандартом безпеки для WLAN, що забезпечує найвищий рівень захисту. Він замінив TKIP на CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), який використовує Advanced Encryption Standard (AES).

AES є блоковим шифром і значно надійнішим за RC4. CCMP забезпечує як конфіденційність (шифрування), так і цілісність (аутентифікацію) даних.

WPA2 підтримує два основні режими:

- WPA2-Personal (PSK) - використовує попередньо погоджений ключ (PSK) для автентифікації, що ідеально підходить для домашніх та малих офісних мереж.

- WPA2-Enterprise (802.1X/EAP) - використовує сервер автентифікації (наприклад, RADIUS) та Extensible Authentication Protocol (EAP) для автентифікації користувачів, забезпечуючи більш надійний та масштабований захист для великих організацій.

Незважаючи на свою міцність, WPA2 не є абсолютно невразливим. Основними векторами атак залишаються:

- Атаки на 4-стороннє рукостискання: Зловмисник може перехопити пакет, що містить хеш пароля під час 4-стороннього рукостискання між клієнтом та точкою доступу. Після захоплення цього хешу може бути здійснена офлайн-атака методом грубої сили або словникова атака для визначення PSK.

- Атаки KRACK (Key Reinstallation Attacks). Виявлені в 2017 році, KRACKs експлуатують вразливості в самому протоколі 4-стороннього рукостискання, дозволяючи зловмиснику маніпулювати або дешифрувати дані. Проте ці вразливості були усунені оновленнями програмного забезпечення.

Схема (рис. 1.3) візуалізує п'ять фаз встановлення та підтримки захищеного з'єднання у бездротовій мережі, що відповідає стандарту IEEE 802.11i (який комерційно відомий як WPA2). Вона показує взаємодію між основними учасниками процесу.

Учасниками процесу є:

STA (Station) - бездротова станція або клієнтський пристрій, який намагається підключитися до мережі (наприклад, ноутбук, смартфон).

- AP (Access Point) - точка доступу Wi-Fi, яка забезпечує бездротове підключення для STA до більш широкої мережі.

- AS (Authentication Server) - сервер автентифікації (наприклад, RADIUS-сервер), який перевіряє облікові дані STA та надає дозвіл на доступ. Він є центральним компонентом для корпоративних мереж (WPA2-Enterprise).

- End Station - кінцева станція або ресурс у мережі, з яким STA має намір взаємодіяти після успішного підключення.

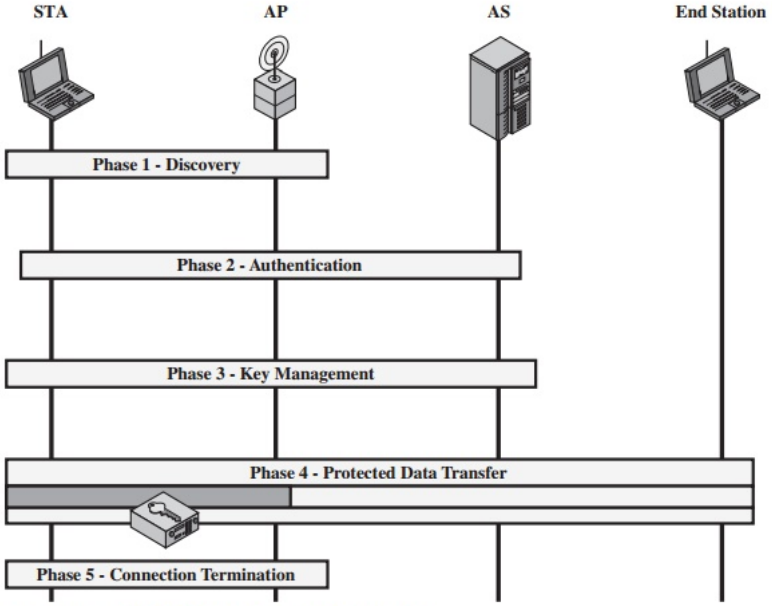

Рисунок 1.3 – Фази і операції стандарту IEEE 802.11i

Розглянемо фази IEEE 802.11i.

Фаза 1 - Discovery (Виявлення)

STA починає процес, шукаючи доступні AP. Це може відбуватися шляхом пасивного прослуховування маякових кадрів (beacon frames), які розсилають AP, або активного надсилання зондувальних запитів (probe requests) для виявлення AP в зоні дії.

AP відповідає на ці запити, надаючи інформацію про свої можливості та налаштування безпеки. На цьому етапі AS та End Station не беруть безпосередньої участі.

Фаза 2 - Authentication (Автентифікація)

Після виявлення AP, STA ініціює процес автентифікації. AP виступає як посередник, перенаправляючи запити автентифікації від STA до AS. AS перевіряє облікові дані STA (наприклад, ім'я користувача та пароль, сертифікат). Якщо автентифікація успішна, AS інформує AP про це. На цьому етапі може використовуватися протокол EAP (Extensible Authentication Protocol).

Фаза 3 - Key Management (Управління ключами)

Після успішної автентифікації починається етап управління ключами. На цьому етапі AP та STA виконують 4-стороннє рукостискання (4-Way Handshake). Метою цього рукостискання є генерація та обмін тимчасовими сесійними ключами, які будуть використовуватися для шифрування та дешифрування даних. Ці ключі є унікальними для кожного сеансу та кожного клієнта, що забезпечує форвардну секретність.

Фаза 4 - Protected Data Transfer (Захищена передача даних)

Коли ключі встановлено, STA може безпечно передавати та приймати дані через AP. Весь трафік між STA та AP тепер шифрується та захищається за допомогою узгоджених ключів, використовуючи протоколи, такі як CCMP (на основі AES). Дані, що передаються через AP, можуть потім направлятися до End Station у дротовій мережі, або навпаки, зашифровано до STA.

Фаза 5 - Connection Termination (Завершення з'єднання)

Коли STA або AP бажають завершити з'єднання, відбувається процес деасоціації. З'єднання розривається, і сесійні ключі, що використовувалися, анулюються. Це завершує життєвий цикл захищеного бездротового з'єднання за стандартом IEEE 802.11i.

Ця схема наочно демонструє, що безпека 802.11i — це не єдиний крок, а послідовність ретельно визначених фаз, що включають виявлення, складні процеси автентифікації та управління ключами, щоб забезпечити конфіденційність та цілісність даних протягом всього періоду з'єднання.

1.5. Методологія дослідження та умови проведення моделювання

Для практичної демонстрації вразливостей WEP та WPA2 було розгорнуто експериментальну ad-hoc мережу.

Обладнання: Три ноутбуки, оснащені Wi-Fi адаптерами, що підтримують режим моніторингу (monitor mode) та ін'єкції пакетів.

Конфігурація мережі: Були створені дві тестові мережі: одна з використанням шифрування WEP, інша – WPA2-PSK.

Програмне забезпечення:

CommView for Wi-Fi використовувався для перехоплення та аналізу бездротового трафіку. Цей інструмент дозволяв збирати пакети даних, включаючи вектори ініціалізації та частини рукостискання.

Aircrack-ng 1.2 RC 1 - набір інструментів для аудиту безпеки бездротових мереж. Він використовувався для:

`airmon-ng` - переведення Wi-Fi адаптера в режим моніторингу.

`airodump-ng` - збір пакетів даних (зокрема, IVs для WEP та рукостискань для WPA/WPA2).

`aireplay-ng` - ін'єкція пакетів для прискорення генерації IVs або деавтентифікації клієнтів.

`aircrack-ng` - безпосереднє відновлення ключів WEP та WPA/WPA2.

1.6. Опис імітаційних процесів атаки

1.6.1. Атака на WEP

Атака на WEP експлуатувала слабкості алгоритму RC4 та повторне використання IV.

1. Переведення адаптера в режим моніторингу: За допомогою `airmon-ng` Wi-Fi адаптер було переведено в режим, який дозволяє перехоплювати всі бездротові пакети в радіусі дії.

2. Збір IVs: За допомогою `airodump-ng` здійснювався безперервний збір пакетів даних, що містять унікальні IV. Оскільки IVs є короткими (24 біти) та передаються у відкритому вигляді, їхнє повторення є неминучим при достатньому обсязі трафіку.

3. Прискорення збору IVs (опційно): Для прискорення процесу `aireplay-ng` використовувався для ін'єкції ARP-реквестів, що стимулювало точку доступу генерувати більше пакетів з новими IVs.

4. Відновлення ключа: Після збору достатньої кількості IVs (зазвичай десятки тисяч), `aircrack-ng` застосовував статистичний аналіз для відновлення WEP-ключа. Час відновлення ключа варіювався від декількох хвилин до десятків хвилин, залежно від кількості зібраних IVs та обчислювальної потужності.

1.6.2. Атака на WPA2-PSK

Атака на WPA2-PSK була спрямована на перехоплення 4-стороннього рукостискання та подальшу офлайн-атаку.

1. Переведення адаптера в режим моніторингу: Аналогічно WEP, адаптер було переведено в режим моніторингу.

2. Збір 4-стороннього рукостискання: За допомогою `airodump-ng` здійснювався моніторинг трафіку з метою захоплення повного 4-стороннього рукостискання між клієнтом та точкою доступу. Цей процес відбувається, коли клієнт вперше підключається до мережі.

3. Деавтентифікація клієнта (опціонально): Для прискорення захоплення рукостискання, `aireplay-ng` використовувався для надсилання пакетів деавтентифікації до підключеного клієнта. Це змушувало клієнта повторно підключатися до мережі, що призводило до повторного виконання 4-стороннього рукостискання.

4. Офлайн-атака: Захоплений файл з рукостисканням (формату `.cap`) був переданий в `aircrack-ng`. Для відновлення PSK використовувалися

словникові атаки. `aircrack-ng` порівнював хеші, згенеровані зі слів у наданому словнику, з перехопленим хешем рукостискання. Успіх атаки залежав від наявності пароля у словнику.

1.7. Передумови та завдання дипломної роботи

Бездротові локальні мережі (WLAN) набули повсюдного поширення в численних секторах завдяки своїй простоті інсталяції, гнучкості розгортання, мобільності, зниженню загальної вартості володіння та високій масштабованості. Їхня значущість у сучасних мережевих технологіях є беззаперечною. Поряд з технологіями Bluetooth та стільниковими мережами, WLAN трансформували обчислювальну та бізнес-індустрії, що, в свою чергу, спричинило численні наслідки для безпеки. Зокрема, системи WLAN, такі як мережі стандарту IEEE 802.11, стали домінуючими мережами доступу як у приватних, так і в громадських середовищах [3]. Вони пропонують значні переваги, включаючи покращену мобільність та гнучкість, що дозволяє користувачам значно більшу свободу доступу до мережі порівняно з традиційними дротовими локальними мережами.

Однак, ці переваги супроводжуються додатковими міркуваннями щодо безпеки. Ризики безпеки у бездротових середовищах охоплюють як ризики, притаманні дротовим мережам, так і нові загрози, що виникають внаслідок мобільності та використання відкритого радіоефіру. Для мінімізації цих ризиків та захисту користувачів від несанкціонованого прослуховування, організації впровадили низку механізмів безпеки.

Традиційним механізмом безпеки WLAN був WEP. Розроблений у 1999 році разом зі стандартом 802.11b, WEP мав на меті забезпечити базовий рівень бездротової безпеки, використовуючи алгоритм шифрування RC4 (Rivest Cipher 4) від RSA Data Security. Проте, згодом криптоаналітиками було виявлено декілька серйозних криптографічних недоліків, що призвело

до його заміни на Wi-Fi Protected Access (WPA) у 2003 році, а згодом на повний стандарт IEEE 802.11i (WPA2) у 2004 році. Незважаючи на ці значні вади безпеки, WEP все ще може забезпечувати мінімальний рівень конфіденційності даних [6]. У цьому дослідженні ми прагнемо виявити вразливості протоколів безпеки WLAN шляхом їх практичного зламу. Нашою метою є демонстрація можливості зловмисника легко скомпрометувати паролі мереж, що використовують цей тип захисту, що зазвичай виконується під час оцінок безпеки для виявлення слабких облікових записів.

Основною метою є комплексний аналіз наявних механізмів безпеки WLAN, а також виявлення їхніх реальних вразливостей та методів їхньої експлуатації.

Конкретні завдання роботи включають:

- Аналіз та характеристика різних протоколів безпеки WLAN.

- Ідентифікація та документування вразливостей, притаманних протоколам безпеки WLAN, зокрема WEP, WPA та WPA2.

- Проведення експериментального дослідження (імітаційного моделювання) з метою демонстрації практичної експлуатації виявлених вразливостей протоколів безпеки WLAN.

РОЗДІЛ 2. ПРИНЦИПИ БЕЗПЕКИ І ТЕХНІКИ ШИФРУВАННЯ БЕЗДРОТОВИХ МЕРЕЖ

Цей розділ охоплює базову теорію, яка стане основою для решти роботи в цій дипломній роботі. Спочатку ми визначимо деякі загальні принципи безпеки. Далі ми надамо вступ до бездротових мереж та безпеки бездротових мереж. Ми також надамо деякий опис техніки шифрування WEP, WPA, TKIP та відомих атак на них. Ці техніки використовуються для цілей безпеки. Але ці техніки мають деякі проблеми. Через ці проблеми ми можемо зламати пароль і побачити дані. Ми зламуємо пароль, використовуючи Aircrack-ng та Commview у нашій роботі.

2.1. Принципи безпеки

Комп'ютери та комп'ютерні мережі, особливо Інтернет, стали життєво важливою частиною сучасного суспільства. Отже, безпека цих систем дуже важлива. Аспекти, починаючи від конфіденційності користувачів до збереження важливої інфраструктури та громадських послуг, всі залежать від безпеки комп'ютерних систем та мереж.

Інформаційну безпеку розділяють на три основні принципи: конфіденційність, цілісність та доступність. Ці принципи виходять за межі технічних реалізацій безпеки та включають соціальні та організаційні аспекти. Цей розділ зосередиться на загальних технічних принципах безпеки.

RFC4949 визначає конфіденційність як: властивість, що дані не розголошуються системним об'єктам, якщо вони не були уповноважені знати дані.

Наприклад, якщо користувач входить в комп'ютерну систему, пароль повинен бути збережений в таємниці для підтримки конфіденційності. Це

означає, що пароль ніколи не повинен надсилатися по мережі в відкритому вигляді. Користувач ніколи не повинен зберігати його незахищеним або розголошувати іншим особам.

Інший аспект конфіденційності при обговоренні мереж - це конфіденційність потоку трафіку. Це захист інформації. Він міг бути отриманий шляхом спостереження за мережевим трафіком. Конфіденційність є ключовим аспектом у підтримці конфіденційності користувачів.

Цілісність визначається як гарантія того, що отримані дані точно такі ж, як і ті, що були надіслані уповноваженим об'єктом [10]. (тобто не містять модифікацій, вставок, видалень або повторів.) Цілісність інформації може бути скомпрометована як навмисно, так і ненавмисно. Для виявлення модифікації даних часто обчислюється код цілісності повідомлення (MIC - Message Integrity Code) з даних. Будь-яка модифікація даних призведе до іншого MIC. Він вкаже, що дані були модифіковані. Існує багато різних засобів забезпечення цілісності, починаючи від простих циклічних надлишкових перевірок (CRC) до MIC на основі складних криптографічних хеш-функцій, таких як MD5 або SHA [11]. Щоб мати можливість повністю захистити цілісність даних, MIC і/або дані потрібно зашифрувати. В іншому випадку, зловмисник міг би просто модифікувати дані та переобчислити MIC відповідно. Якщо використовується шифрування, потрібна якась форма спільного секрету, тобто ключа.

Прості MIC можуть виявляти лише незначні модифікації, такі як, наприклад, помилки передачі, і не надають захисту від навмисного підроблення даних. Криптографічні хеш-функції призначені для виявлення будь-яких змін у даних. Має бути обчислювально неможливо модифікувати дані без зміни хеш-значення. Також має бути неможливо для зловмисника повторно відправити або ретранслювати раніше надіслані дані без активації якоїсь схеми захисту від повторів, це найчастіше досягається за допомогою послідовних номерів і/або часових міток.

Доступність визначається в RFC4949 як властивість системи або системного ресурсу бути доступним, або придатним для використання, або оперативним за запитом, уповноваженим системним об'єктом, відповідно до специфікацій продуктивності для системи [8].

Інформаційна система повинна бути доступною для своїх користувачів, коли це необхідно. В іншому випадку вона не відповідає своїм вимогам. Ця властивість особливо важлива в комп'ютерних мережах та серверах, які обслуговують велику кількість користувачів і є життєво важливою частиною сучасного суспільства, наприклад, банківські системи. Найбільшою навмисною загрозою для доступності є атаки типу "відмова в обслуговуванні" (DoS). Атаки DoS зазвичай виконуються шляхом генерації надмірної кількості запитів або трафіку. Це зробить легітимне використання послуги неможливим [13]. Використання вразливостей протоколів також могло б скомпрометувати доступність системи. Доступність досягається за допомогою фізичної надлишковості та безпеки, а також належного управління та контролю.

2.2 Огляд бездротових локальних мереж

IEEE 802.11 посилається на сімейство специфікацій, розроблених IEEE для інтерфейсу "повітря" між бездротовим клієнтом та точкою доступу (AP) або між двома бездротовими клієнтами. Щоб називатися пристроями 802.11, вони повинні відповідати специфікаціям рівня управління доступом до середовища (MAC) та фізичного рівня. Стандарт IEEE 802.11 охоплює фізичний (рівень 1) та рівень передачі даних (рівень 2) моделі OSI. У цій статті ми в основному зосереджуємося на рівні MAC, а не на варіаціях фізичного рівня, відомих як 802.11a/b/g.

Бездротова мережева інтерфейсна карта (адаптер) - це пристрій, який називається станцією, що надає мережевий фізичний рівень через

радіозв'язок з іншою станцією. Точка доступу (AP) - це станція, яка надає послугу розподілу кадрів станціям, пов'язаним з нею. Сама AP зазвичай підключена дротом до LAN.

Станція та AP містять мережевий інтерфейс, який має адресу управління доступом до середовища (MAC), як і дротові мережеві карти. Ця адреса - це унікальний у всьому світі 48-бітний номер, присвоєний йому на момент виготовлення. 48-бітну адресу часто представляють як рядок з шести октетів, розділених двокрапками (наприклад, 00:02:2D:17:B9:E8) або дефісами (наприклад, 00-02-2D-17-B9-E8). Хоча MAC-адреса, присвоєна виробником, надрукована на пристрої, адресу можна змінити програмно [16].

Кожна AP має ідентифікатор набору послуг (SSID) довжиною від 0 до 32 байтів, який також часто називають мережевим ім'ям. SSID використовується для сегментації ефіру для використання. Якщо дві бездротові мережі фізично близькі, SSID позначають відповідні мережі та дозволяють компонентам однієї мережі ігнорувати компоненти іншої. SSID можуть бути відображені на віртуальні LAN; таким чином, деякі AP підтримують кілька SSID. На відміну від повністю кваліфікованих імен хостів (наприклад, gamma.cs.wright.edu), SSID не реєструються, і можливо, що дві не пов'язані мережі використовують один і той же SSID [15].

Станції спілкуються одна з одною, використовуючи радіочастоти між 2,4 ГГц і 2,5 ГГц [15]. Сусідні канали віддалені один від одного лише на 5 МГц. Дві бездротові мережі, що використовують сусідні канали, можуть заважати одна одній.

2.2.1. Інфраструктурний та ad-hoc режими

Бездротова мережа працює в одному з двох режимів. У ad-hoc режимі кожна станція є рівноправною з іншими станціями та спілкується безпосередньо з іншими станціями в мережі. AP не бере участі. Всі станції

можуть надсилати кадри Beacon та Probe. Станції ad-hoc режиму утворюють незалежний базовий набір послуг (IBSS).

Станція в інфраструктурному режимі спілкується лише з AP. Базовий набір послуг (BSS) - це набір станцій, які логічно пов'язані одна з одною та керуються однією AP. Разом вони працюють як повністю підключена бездротова мережа. BSSID - це 48-бітне число того ж формату, що і MAC-адреса. Це поле унікально ідентифікує кожен BSS. Значення цього поля - це MAC-адреса AP.

Станція та AP випромінюють та збирають кадри 802.11 за необхідності. Формат кадрів показано нижче. Більшість кадрів містять IP-пакети. Інші кадри призначені для управління та контролю бездротового з'єднання.

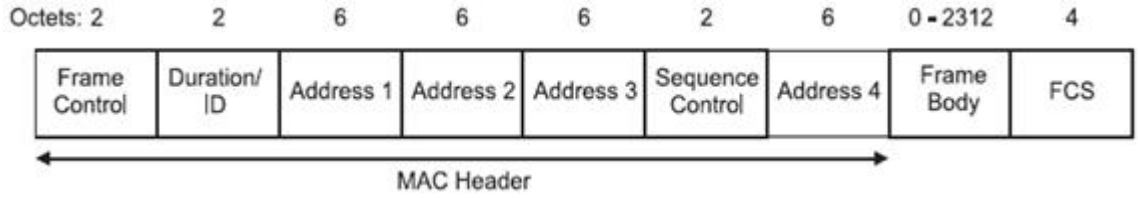

Рисунок 2.1 - Кадр IEEE 802.11

Існує три класи кадрів. Кадри управління встановлюють та підтримують зв'язок. Це кадри типу Запит на асоціацію, Відповідь на асоціацію, Запит на повторну асоціацію, Відповідь на повторну асоціацію, Запит на зондування, Відповідь на зондування, Beacon, Повідомлення про індикацію трафіку, Роз'єднання, Аутентифікація, Деаутентифікація. SSID є частиною кількох кадрів управління. Повідомлення управління завжди надсилаються у відкритому вигляді, навіть коли використовується шифрування зв'язку (WEP або WPA), тому SSID видимий для будь-якого, хто може перехопити ці кадри. Кадри керування допомагають у доставці даних [15].

Кадри даних інкапсулюють пакети мережевого рівня OSI. Вони містять MAC-адреси джерела та призначення, BSSID та датаграму TCP/IP. Частина корисного навантаження датаграми шифрується за допомогою WEP.

2.2.2. Процес аутентифікації

Аутентифікація - це процес доведення ідентичності станції іншій станції або AP. При аутентифікації з відкритою системою всі станції аутентифікуються без будь-якої перевірки. Станція A надсилає кадр управління аутентифікацією, який містить ідентифікатор A, станції B. Станція B відповідає кадром, який вказує на визнання, адресованим A. При аутентифікації з використанням спільного ключа станції повинні знати SSID AP, щоб підключитися до AP. Аутентифікація з використанням спільного ключа використовує стандартний виклик та відповідь разом із спільним секретним ключем.

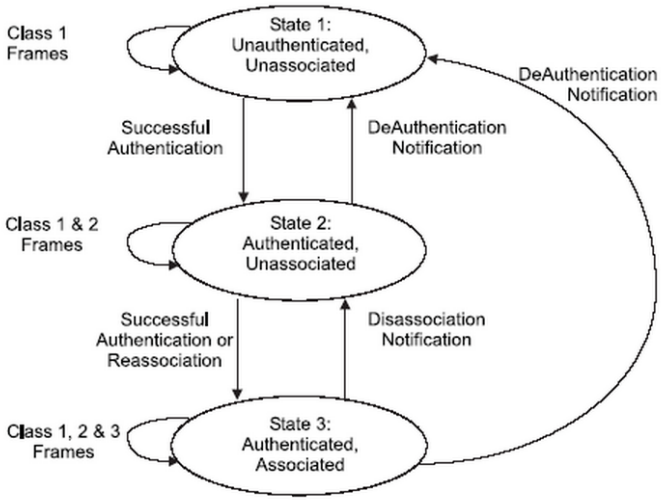

Рисунок 2.2 - Стани та послуги

2.3. Безпека бездротових мереж

Розгортання бездротових мереж збільшується як у домашніх, так і в ділових середовищах завдяки постійному збільшенню як надійності, так і

продуктивності. Зручність уникнення фізичної інфраструктури дротової мережі часто робить бездротову мережу переважною над дротовою мережею. Бездротові мережі більш схильні до загроз безпеки, ніж дротові мережі, через їх природу. У дротовій мережі комп'ютери підключені через дроти. Адміністратору легко контролювати цю довірену зону.

У бездротових мережах трафік поширюється в будь-якому напрямку по повітрю. Він може бути легко захоплений бездротовим інтерфейсом у межах досяжності на правильному каналі. З цієї причини, якщо бездротова мережа не захищена, слід припустити, що все, що надсилається, може бути прочитано будь-ким. Щоб захистити інформацію, необхідно застосувати шифрування. Якщо хтось може бачити передані дані, необхідно переконатися, що вони марні для них, якщо вони не володіють якимсь спільним секретом; а саме ключем.

2.3.1. Протоколи безпеки IEEE 802.11

Існує багато плутанини та неправильного тлумачення скорочень протоколів безпеки, доступних у бездротових мережах. У цьому розділі буде надано історичний огляд протоколів безпеки IEEE 802.11, щоб розвіяти частину плутанини. Протягом років розвиток протоколів безпеки бездротових мереж був гонкою між IEEE (комітетом зі стандартизації) та WiFi Alliance (індустрією). У 1997 році Wired Equivalent Privacy (WEP) (далі пояснюється в розділі 2.4) став частиною стандарту IEEE 802.11. Він мав на меті надати безпеку, еквівалентну тій, яку ми повинні отримати в дротовій мережі. У 2001 році WEP вже не міг вважатися безпечним після того, як було доведено, що він повністю зламаний.

Щоб впоратися зі слабкостями WEP, IEEE створив робочу групу 802.11i. WiFi Alliance став неспокійним у тривалому процесі IEEE щодо встановлення стандарту 802.11i. В результаті був розроблений WiFi Protected Access (WPA). Він був випущений WiFi Alliance у 2003 році. Стандарт WPA

має два режими. Один з них - Temporal Key Integrity Protocol (TKIP). Інший необов'язковий режим - Advanced Encryption Standard (AES). Обидва ці режими були розроблені на основі поточної роботи, виконаної робочою групою 802.11i.

У 2004 році робоча група 802.11i завершила свою роботу над стандартом безпеки 802.11i. Стандарт був названий Robust Security Network (RSN) IEEE. RSN включав два режими: TKIP (покращене розширення WEP) та Counter Mode CBC-MAC Protocol (CCMP3) з шифруванням AES. До того часу бренд WPA (від WiFi Alliance) був добре встановлений у точках доступу та маршрутизаторах. WiFi Alliance назвав стандарт RSN WPA2. Хронологія розвитку протоколів безпеки.

2.4. Система шифрування WEP (Wired Equivalent Privacy)

WEP - це система шифрування з спільним ключем, яка використовується для шифрування пакетів, що передаються між станцією та AP (точкою доступу). Основна функція протоколу WEP - забезпечити безпеку даних у бездротових мережах так само, як і в дротових мережах. Алгоритм, що використовується в WEP, призначений для захисту бездротової комунікації від підслуховування. WEP шифрує корисне навантаження пакетів даних. WEP використовує алгоритм RC4. Спільний секретний ключ має довжину 40 або 104 біти. Ключ вибирається системним адміністратором. Цей розділ надасть огляд історії, передумов та технічних деталей WEP, а також його слабкостей. Наступний розділ пояснить різні атаки на WEP, деякі з яких можуть бути адаптовані для атаки на TKIP.

WEP був призначений лише для забезпечення безпеки, еквівалентної дротовій мережі. Звичайна дротова мережа не забезпечує конфіденційності на рівні каналу передачі даних, і весь трафік надсилається незашифрованим, поки не використовується шифрування вищого рівня. Єдиний захист на

цьому рівні - фізичний захист від підключення мережевого кабелю до мережевого обладнання. Бездротові мережі є більш вразливими, ніж їх дротові аналоги. Будь-хто з радіоантеною та бездротовою мережевою картою може підслуховувати дані та потенційно отримати доступ до мережі.

Очевидно, що бездротові мережі потребують додаткового захисту. Він повинен бути від втрати конфіденційності та несанкціонованого доступу до мережі. IEEE представив WEP у стандарті 802.11 1997 року. Оскільки популярність бездротових мереж зростала, вона привернула увагу криптографічного співтовариства. Вже у 2001 році було виявлено кілька слабкостей, і інструменти для злому WEP за короткий час з особистим комп'ютером стали вільно доступними в Інтернеті [20].

2.4.1. Конструкція протоколу

Конструкція MPDU (MAC Protocol Data Unit) WEP може бути побачена на рисунку 2.3.

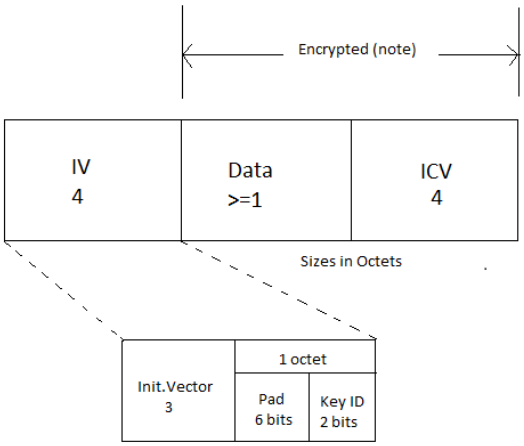

Рисунок 2.3 - Конструкція розширеного MPDU WEP

MPDU складається з трьох основних частин: фактичне повідомлення або дані, значення перевірки цілісності (ICV) та вектор ініціалізації (IV). Цей MPDU подальше інкапсулюється в заголовок 802.11. У WEP лише фактичні дані повідомлення та ICV шифруються. IV та заголовки 802.11 надсилаються

у відкритому вигляді. ICV складається з 32-бітного значення CRC-32. Він додається для перевірки цілісності пакету. Поле IV також має довжину 32 біти. Воно складається з 24-бітного IV, 2-бітного підполя ідентифікатора ключа та 6 бітів заповнення. 24-бітний IV використовується в поєднанні з спільним секретним ключем як вхід для алгоритму шифрування RC4. Підполе ідентифікатора ключа вказує, який секретний ключ, з чотирьох можливих, був використаний для шифрування пакету.

WEP був розроблений для забезпечення безпеки дротової LAN шляхом шифрування за допомогою алгоритму RC4 з двома сторонами передачі даних [21].

Сценарій А, на стороні відправника: WEP намагається використовувати чотири операції для шифрування даних (відкритий текст). По-перше, секретний ключ, що використовується в алгоритмі WEP, має довжину 40 біт з 24-бітним вектором ініціалізації (IV), який конкатенується з ним для дії як ключ шифрування/дешифрування. По-друге, отриманий ключ діє як насіння для генератора псевдовипадкових чисел (PRNG). По-третє, відкритий текст проходить через алгоритм цілісності та конкатенується з відкритим текстом знову. По-четверте, результат послідовності ключів та ICV піде в алгоритм RC4. Остаточне зашифроване повідомлення створюється шляхом приєднання IV перед шифротекстом. Тепер на рисунку 2.4 визначені об'єкти та пояснюються деталі операцій [18].

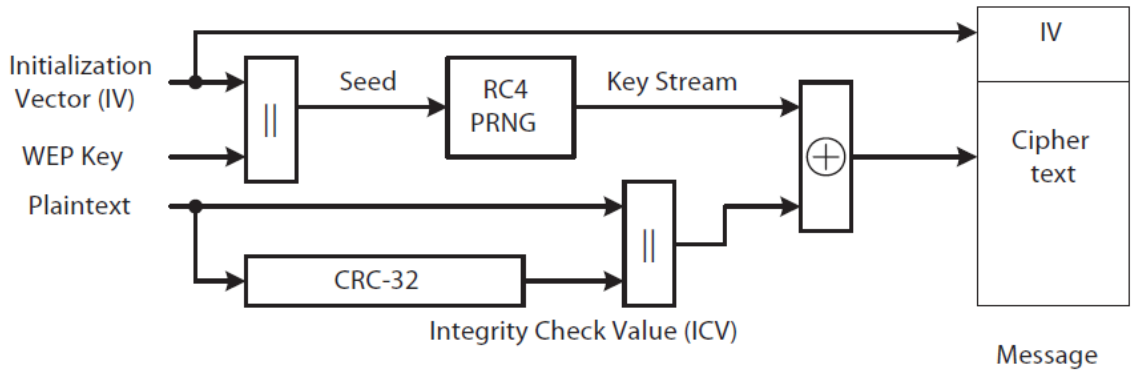

Рисунок 2.4 - Блок-схема інкапсуляції WEP

Сценарій В, на стороні отримувача: WEP намагається використовувати п'ять операцій для дешифрування отриманої сторони (IV + шифротекст). По-перше, попередньо спільний ключ та IV конкатенується для створення секретного ключа. По-друге, шифротекст та секретний ключ йдуть в алгоритм CR4, і відкритий текст виходить як результат. По-третє, ICV та відкритий текст будуть розділені. По-четверте, відкритий текст йде в алгоритм цілісності для створення нового ICV (ICV), і, нарешті, новий ICV (ICV) порівнюється з оригінальним ICV. На рисунку 2.5 можна побачити об'єкти та деталі операцій схематично [21].

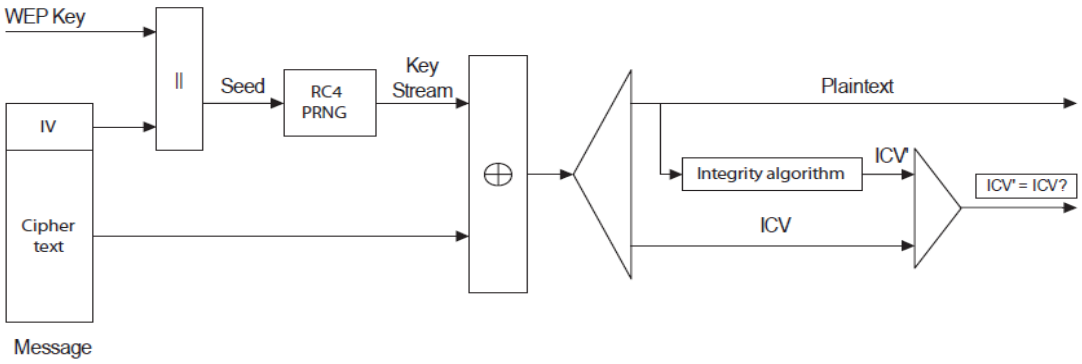

Рисунок 2.5 - Блок-схема декапсуляції WEP

2.4.2. Аутентифікація

Перед тим, як може відбутися будь-яке спілкування між станцією та мережею, станція повинна аутентифікуватися, щоб стати асоційованою з мережею. WEP підтримує два типи аутентифікації: аутентифікацію відкритої системи та аутентифікацію за допомогою спільного ключа [4]. Аутентифікація відкритої системи насправді є нульовим алгоритмом аутентифікації [3]. Це означає, що будь-яка станція може аутентифікуватися, якщо AP встановлений на аутентифікацію відкритої системи [22]. Цей протокол просто складається з запиту та повідомлення про успіх, і насправді не відбувається жодної аутентифікації.

Аутентифікація за допомогою спільного ключа пропонує односторонню аутентифікацію, на відміну від взаємної аутентифікації. Станція аутентифікується з AP, але AP ніколи не аутентифікується зі станцією. Тільки станції, які знають секретний ключ, можуть успішно аутентифікуватися з AP. Цей протокол складається з чотиристороннього рукостискання та ініціюється станцією, яка надсилає запит на аутентифікацію. AP відповідає викликом, який містить 128-октетне повідомлення, згенероване PRNG WEP. Коли станція отримує цей виклик, 128-октетний блок шифрується за допомогою WEP з секретним спільним ключем та надсилається назад до AP. Коли AP отримує це повідомлення, воно декапсулюється, і перевіряється ICV. Якщо ця перевірка успішна, розшифровані дані порівнюються з викликом, раніше надісланим. Якщо вони збігаються, AP знає, що станція знає спільний ключ, і надсилає повідомлення про успішну аутентифікацію [9].

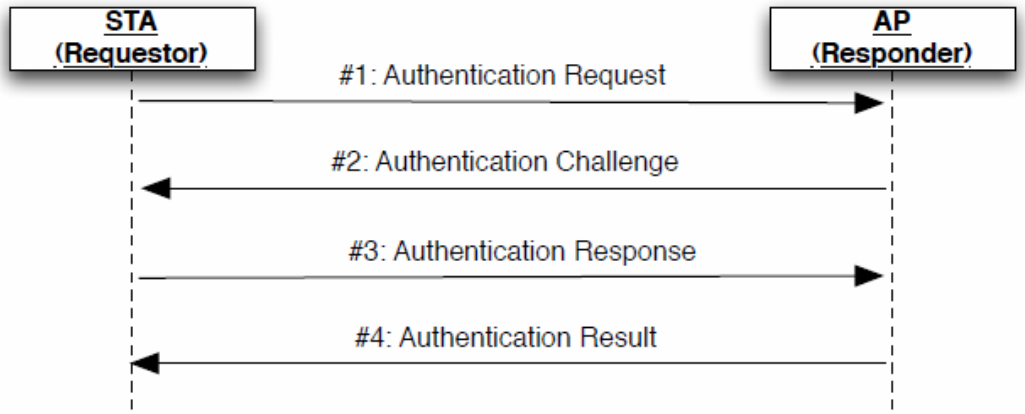

Рисунок 2.6 - Діаграма послідовності аутентифікації за допомогою спільного ключа

Незважаючи на те, що цей метод аутентифікації може здатися більш безпечним, ніж аутентифікація відкритої системи, він має деякі серйозні слабкості. Аутентифікація за допомогою спільного ключа застаріла, і якщо

використовується WEP (який також застарів), слід увімкнути лише аутентифікацію відкритої системи.

2.4.3. Генератор псевдовипадкових чисел - RC4

WEP використовує генератор псевдовипадкових чисел RC4 для шифрування. Алгоритм насправді називається ARC4 (Alleged RC4) у стандарті IEEE 802.11, тому що власник алгоритму, RSA Security, ніколи не опублікував його деталі. Вихідний код RC4 був анонімно опублікований в Інтернеті в 1994 році [23]. RC4 - це потіковий шифр, що означає, що він працює на рівні байтів, на відміну від блочного шифру, який працює на блоках з кількох байтів. RC4 приймає ключ змінного розміру (від 1 до 256 байтів) як вхід і генерує псевдовипадковий потік байтів. У WEP цей ключ має довжину 64 або 128 біт, 24-бітний IV конкатенується з 40 або 104-бітним спільним ключем. Для шифрування даних згенерований потік псевдовипадкових байтів XOR-ється з відкритим текстом для створення шифротексту. Дешифрування працює так само, оскільки XOR - це симетрична операція. Шифротекст XOR-ється з потоком псевдовипадкових байтів для отримання відкритого тексту. Алгоритм RC4 дивно простий і може бути легко пояснений. RC4 працює з 256-байтовим вектором стану S, який містить всі 256 перестановок 8 біт. Цей вектор стану спочатку ініціалізується для міщення всіх значень у порядку зростання. Також створюється 256-байтовий тимчасовий вектор, який містить ключ K. Якщо ключ менший за 256 байтів, ключ просто повторюється, поки вектор не заповнений. Ця ініціалізація описана в алгоритмі 2.1.

Алгоритм 2.1. Ініціалізація вектора стану RC4

```
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
end for
```

Наступний крок - використання тимчасового вектора T для створення початкової перестановки вектора стану S. Це робиться шляхом обміну двома байтами в S відповідно до процедурою, заданою T. Оскільки єдина операція, яка виконується над S, - це обмін байтів, S все ще містить всі перестановки восьми біт. Алгоритм для початкової перестановки S наведений в алгоритмі 2.2.

Алгоритм 2.2. Початкова перестановка вектора стану RC4

```
j = 0;
for i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
end for
```

Коли початкова перестановка завершена, ключ і тимчасовий вектор більше не використовуються. Потік ключів генерується по одному байту за раз шляхом обміну кожним байтом S, на основі власного стану. Далі вибирається байт k для потоку ключів. Ця процедура наведена в алгоритмі 2.3.

Алгоритм 2.3. Генерація потоку S-Box RC4 [10]

```
i, j = 0;
while true do
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
k = S[t];
end while
```

RC4, і особливо спосіб, яким його використовує WEP, має деякі недоліки, які будуть описані нижче.

WEP спочатку був створений для забезпечення безпеки, еквівалентної тій, яку ми могли б очікувати від дротових мереж. Навіть якщо назва протоколу не передбачає найвищого рівня безпеки, вона передбачає бути досить безпечною.

У протоколі WEP ключ розширюється потоком IV для отримання різних потоків ключів для шифрування кожного з передаваних кадрів. Але є деякі недоліки у використанні потоків ключів. Під час обчислення XOR з аргументами, які представляють два повідомлення, зашифровані тим самим потоком ключів. Якщо повідомлення зашифровані за допомогою того самого потоку ключів, то ми можемо розшифрувати не тільки одне повідомлення, але й інші повідомлення за допомогою ідентичного потоку ключів. Проблема виникає через повторюваний послідовність IV, оскільки ключ змінюється рідко, тому, коли той самий IV генерується разом з тим самим ключем, який не був змінений, ми отримуємо повторюваний потік ключів. Зловмисники можуть дуже легко отримати доступ до IV, оскільки він не шифрується під час передачі пакету.

Модифікація повідомлення означає модифікацію повідомлень у процесі передачі. Отримувач не помітить, що повідомлення було модифіковано. Через лінійні характеристики контрольної суми існує можливість контролювати модифікації в зашифрованому повідомленні без зміни контрольної суми. Таким чином, можна зробити будь-які модифікації в зашифрованому повідомленні без страху, що отримувач помітить ці модифікації [9].

Дві характеристики протоколу WEP:

$\rightarrow$ Контрольна сума WEP є незаблокованою функцією,

$\rightarrow$ Можна застосовувати старі функції IV без виявлення отримувачем.

Через першу характеристику, будь-хто, хто знає повідомлення, може обчислити поле контрольної суми. Це дозволяє уникнути заходів контролю

доступу. Друга характеристика допомагає зловмисникам впроваджувати своє повідомлення у випадку, якщо вони знають послідовність IV та потік ключів. Зловмисник шифрує своє власне повідомлення, знаючи потік ключів, і надсилає його отримувачу.

2.4.4. Атаки на WEP

WEP був створений з метою забезпечення безпеки, еквівалентної дротовим мережам. WEP містив так багато очевидних слабкостей, що повне відновлення ключа було майже неминучим. Атака з відновленням ключа - це остаточна атака, в результаті якої зловмисник отримує головний ключ, який може бути використаний для отримання повного доступу до мережі. Цей розділ пояснить історію та деталі найбільш серйозних та відомих атак на протокол WEP. Більшість цих атак - атаки, спрямовані проти алгоритму RC4 та способу його використання в WEP. Однак також існують атаки, які дозволяють зловмиснику дешифрувати окремі пакети, ніколи не знаючи ключа шифрування. Ці некриптографічні атаки використовують слабкості самого протоколу WEP, а не статистичну атаку проти RC4. Всі ці атаки доступні через такі інструменти, як набір aircrack-ng. Це компіляція кількох інструментів та алгоритмів, що атакують безпеку бездротових мереж.

У 2004 році особа під псевдонімом KoreK опублікувала дві атаки на інтернет-форумі. Пізніше їх назвали атакою KoreK та атакою Chopchop. Атака KoreK описує сімнадцять різних атак на WEP, які можна класифікувати наступним чином:

- Відновлення ключа на основі першого байта потоку ключів PRNG.

- Відновлення ключа на основі першого та другого байтів потоку ключів PRNG.

- Зворотні методи для зменшення простору пошуку.

Приблизно в той же час, коли атаки KoreK на RC4 були опубліковані на інтернет-форумі, той самий анонімний хакер опублікував нову атаку, яку

назвали атакою Chopchop. Атака Chopchop належить до нової групи атак, які, порівняно з усіма попередніми атаками, можуть вважатися некриптографічною атакою. Замість того, щоб використовувати вразливості в алгоритмі RC4, Chopchop атакує сам протокол WEP та дві його конструктивні вади, а саме відсутність захисту від повторів та слабкість ICV. Атака Chopchop - це помітна та відмінна атака на WEP, ніж попередньо пояснена. Хоча вона не дуже ефективна, вона має практичний інтерес з пакетами, які мають велику кількість відомих даних, наприклад, пакет ARP. Атака Chopchop дозволяє зловмиснику дешифрувати пакет, ніколи не знаючи ключа. У реальних умовах атака Chopchop може бути використана для дешифрування пакету, його модифікації та повторного впровадження в мережу для генерації трафіку. Функція CRC-32 була розроблена для виявлення помилок і не призначена для функціонування лінійності CRC-32 та операції XOR, що використовується для шифрування WEP, можливо перевернути біт у шифротексті, а потім обчислити, який біт у зашифрованому значенні CRC-32, який, у свою чергу, повинен бути перевернутий, щоб контрольна сума була вірною. Цей факт у поєднанні з відсутністю захисту від повторів у WEP є найважливішими компонентами атаки Chopchop.

2.5. Технологія безпеки WPA

WPA - це технологія безпеки для бездротових комп'ютерних мереж Wi-Fi. WPA покращує функції аутентифікації та шифрування WEP (Wired Equivalent Privacy). Насправді WPA був розроблений галузевим співтовариством у відповідь на слабкості WEP.

WPA забезпечує більш сильне шифрування, ніж WEP, завдяки використанню однієї з двох стандартних технологій: Temporal Key Integrity Protocol (TKIP) та Advanced Encryption Standard (AES). WPA також включає

вбудовану підтримку аутентифікації, якої не надає WEP. Загалом WPA забезпечує безпеку, порівнянну з тунелюванням VPN з WEP, з перевагою простішого адміністрування та використання.

Wi-Fi Protected Access (WPA) - це протоколи безпеки та програми сертифікації безпеки, розроблені Wi-Fi Alliance для захисту бездротових комп'ютерних мереж. Альянс визначив його у відповідь на серйозні слабкості, які дослідники виявили в попередній системі, WEP (Wired Equivalent Privacy).

WPA (іноді називають проектом стандарту IEEE 802.11i) став доступним у 2003 році. Альянс Wi-Fi мав на меті його як тимчасовий захід у очікуванні доступності більш безпечного та складного WPA2. WPA2 став доступним у 2004 році та є поширеним скороченням для повного стандарту IEEE 802.11i (або IEEE 802.11i-2004).

Wi-Fi Alliance мав на меті WPA як тимчасовий захід для заміни WEP до доступності повного стандарту IEEE 802.11i. WPA міг бути реалізований через оновлення мікропрограм на бездротових мережевих інтерфейсних картах, розроблених для WEP, які почали поставлятися ще в 1999 році. Однак, оскільки зміни, необхідні в бездротових точках доступу (AP), були більш значними, ніж ті, які були потрібні на мережевих картах, більшість AP, випущених до 2003 року, не могли бути оновлені для підтримки WPA [18].

2.5.1. Огляд протоколу

Протокол WPA реалізує більшу частину стандарту IEEE 802.11i. Зокрема, для WPA був прийнятий протокол Temporal Key Integrity Protocol (TKIP). WEP використовував 40-бітний або 104-бітний ключ шифрування, який повинен бути вручну введений на бездротових точках доступу та пристроях і не змінюється. TKIP використовує ключ на пакет, що означає, що він динамічно генерує новий 128-бітний ключ для кожного пакету і таким чином запобігає типам атак, які скомпрометували WEP.

WPA також включає перевірку цілісності повідомлення. Це призначено для запобігання зловмиснику захопленню, зміні та/або повторному відправленню пакетів даних. Це замінює циклічну перевірку надлишковості (CRC), яка використовувалася стандартом WEP. Основною вадою CRC було те, що він не надавав достатньо сильної гарантії цілісності даних для пакетів, які він обробляв. Існували добре перевірені коди аутентифікації повідомлень для вирішення цих проблем, але вони вимагали занадто багато обчислень для використання на старих мережевих картах. WPA використовує алгоритм перевірки цілісності повідомлення, який називається Michael, для перевірки цілісності пакетів. Michael набагато сильніший, ніж CRC, але не такий сильний, як алгоритм, який використовується в WPA2. Дослідники з тих пір виявили ваду в WPA, яка спиралася на старіші слабкості в WEP та обмеження Michael для отримання потоку ключів з коротких пакетів для повторного впровадження та підробки.

Не минуло багато часу, як з'явилася нова технологія під назвою WPA, або Wi-Fi Protected Access, щоб вирішити багато недоліків WEP. WPA має на меті забезпечити більш сильне шифрування бездротових даних, ніж WEP, але не всі мають або змогли перейти на нову технологію шифрування бездротових даних. Для того щоб використовувати WPA, всі пристрої в мережі повинні бути налаштовані для WPA.

Якщо пристрій не налаштований для WPA, він зазвичай повертається до менш безпечного методу шифрування WEP, дозволяючи бездротовим пристроям спілкуватися в мережі. Технологія була розроблена для роботи з існуючими продуктами Wi-Fi, які були увімкнені з WEP (т. е., як оновлення програмного забезпечення до існуючого апаратного забезпечення), але технологія включає два покращення над WEP:

- Покращене шифрування даних за допомогою протоколу цілісності тимчасового ключа (TKIP). TKIP перемішує ключі за допомогою алгоритму

хешування та, додаючи функцію перевірки цілісності, забезпечує, що ключі не були підроблені.

- Аутентифікація користувача, яка зазвичай відсутня в WEP, за допомогою протоколу розширеної аутентифікації (EAP). WEP регулює доступ до бездротової мережі на основі апаратної MAC-адреси комп'ютера, яка відносно просто може бути перехоплена та викрадена. EAP заснований на більш безпечній системі шифрування з відкритим ключем, щоб забезпечити, що тільки авторизовані користувачі мережі можуть отримати доступ до мережі.

WPA є основною технологією вже багато років, але WEP залишається стандартною функцією на практично кожному бездротовому маршрутизаторі на полицях магазинів сьогодні. Хоча він в основному там для зворотної сумісності з найстарішим апаратним забезпеченням, якщо звіти та дослідження точні, значний відсоток WLAN, що працюють сьогодні (особливо ті, що використовуються вдома), все ще використовують застарілий та небезпечний WEP для свого шифрування.

2.5.2. Схожість між WPA та WEP

WPA був створений з метою вирішення проблем у криптографічному методі WEP, без необхідності користувачів змінювати апаратне забезпечення. Стандарт WPA, подібний до WEP, визначає два режими роботи:

1. Персональний WPA або WPA-PSK (попередньо спільний ключ), який використовується для малого офісу та домашнього використання для аутентифікації, яка не використовує сервер аутентифікації, і ключ шифрування даних може досягати 256 біт. На відміну від WEP, це може бути будь-який алфанумеричний рядок і використовується лише для узгодження початкової сесії з AP. Оскільки як клієнт, так і AP вже володіють цим

ключем, WPA забезпечує взаємну аутентифікацію, і ключ ніколи не передається по повітрю.

2. Підприємницький WPA або Комерційний, де аутентифікація здійснюється сервером аутентифікації 802.1x, що забезпечує відмінний контроль та безпеку в трафіку користувачів бездротової мережі. Цей WPA використовує 802.1X+EAP для аутентифікації, але знову замінює WEP на більш просунуте шифрування TKIP. Попередньо спільний ключ не використовується тут, але нам знадобиться сервер RADIUS. І ми отримуємо всі інші переваги, які надає 802.1X+EAP, включаючи інтеграцію з процесом входу в Windows та підтримку методів аутентифікації EAP-TLS та PEAP.

Основною причиною появи WPA після WEP є те, що WPA дозволяє більш складне шифрування даних на основі протоколу TKIP (Temporal Key Integrity Protocol) та допомоги MIC (Message Integrity Check), функція якого полягає в запобіганні атак типу bit-flipping, які легко застосовуються до WEP за допомогою техніки хешування.

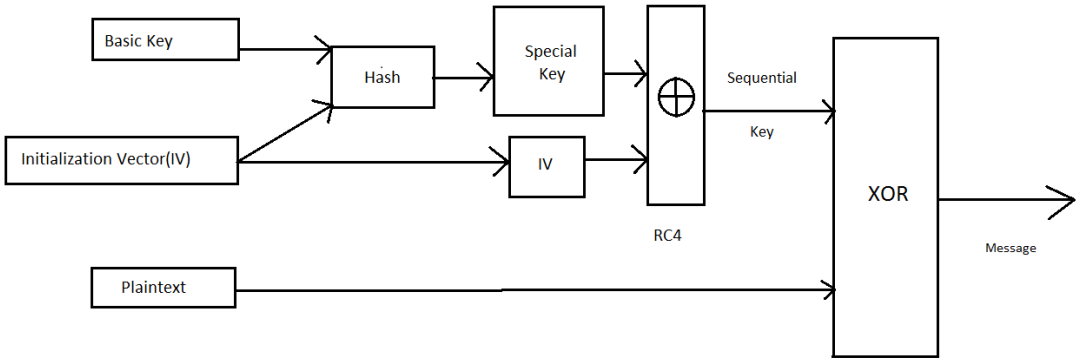

Рисунок 2.7 - Алгоритм шифрування WPA (TKIP)

На рисунку 2.7 TKIP використовує ту ж техніку RC4, що і WEP, але робить хешування перед збільшенням алгоритму RC4. Створюється дублікат вектора ініціалізації. Одна копія надсилається на наступний крок, а інша хешується (змішується) з базовим ключем. Після виконання хешування

результат генерує ключ для пакету, який приєднується до першої копії вектора ініціалізації, відбувається збільшення алгоритму RC4. Після цього відбувається генерація послідовного ключа за допомогою XOR з текстом, який ми бажаємо зашифрувати, генеруючи таким чином зашифрований текст. Нарешті, повідомлення готове до відправки. Це шифрування та дешифрування буде виконано шляхом інвертування процесу.

У листопаді 2003 року було опубліковано "Слабкість у виборі пароля в інтерфейсі WPA". Тоді було пояснено формулу, яка розкриває пароль шляхом виконання атаки за словником проти мереж WPA-PSK (попередньо спільний ключ). Ця слабкість базувалася на попередньому ключі (PMK), який походить від конкатенації пароля, SSID, довжини SSID та nonce (число або бітовий рядок, який використовується лише один раз у кожній сесії). Отриманий рядок хешується 4096 разів для генерації 256-бітного значення, а потім комбінується з nonce значеннями. Необхідна інформація для генерації та перевірки цього ключа (на сесію) передається з звичайним трафіком і є легко доступною; завдання полягає в відновленні початкових значень. Він пояснює, що попередній тимчасовий ключ (PTK) є функцією HMAC з ключем на основі PMK; шляхом захоплення чотиристороннього рукостискання аутентифікації WPA, зловмисник має дані, необхідні для піддання пароля атаці за словником. Нарешті він виявив, що ключ, згенерований з пароля довжиною менше приблизно 20 символів, малоймовірно зупинить атаки.

Для підтвердження, наприкінці 2004 року випустили WPA Cracker і cowpatty. Обидва інструменти написані для систем Linux і виконують атаку за словником проти мереж WPA-PSK у спробі визначити спільний пароль. Обидва вимагають від користувача надати файл словника та файл дампу, який містить чотиристоронє рукостискання аутентифікації WPA-PSK. Обидва функціонують подібним чином; однак, cowpatty містить автоматичний парсер, тоді як WPA Cracker вимагає від користувача

виконання ручного витягування рядків. Крім того, cowpatty оптимізував функцію HMAC-SHA1 і є дещо швидшим. Кожен інструмент використовує алгоритм PBKDF2, який керує хешуванням PSK для атаки та визначення пароля. Жоден з них не є дуже швидким або ефективним проти більших паролів, хоча, оскільки кожен повинен виконувати 4096 HMAC-SHA1.

2.5.3. WPA2-PSK

Скорочено від Wi-Fi Protected Access 2-Pre-Shared Key, і також називається WPA або WPA2 Personal, це метод захисту вашої мережі за допомогою WPA2 з використанням необов'язкового попередньо спільного ключа (PSK) аутентифікації, який був розроблений для домашніх користувачів без сервера аутентифікації підприємства.

Щоб зашифрувати мережу за допомогою WPA2-PSK, ми надаємо нашому маршрутизатору не ключ шифрування, а скоріше пароль англійською мовою довжиною від 8 до 63 символів. Використовуючи технологію, яка називається TKIP (Temporal Key Integrity Protocol), цей пароль, разом з мережевим SSID, використовується для генерації унікальних ключів шифрування для кожного бездротового клієнта. І ці ключі шифрування постійно змінюються. Хоча WEP також підтримує паролі, він робить це лише як спосіб легшого створення статичних ключів, які зазвичай складаються з шістнадцяткових символів 0-9 та A-F [36].

2.6. Протокол безпеки Access-Temporal Key Integrity Protocol (WPA-TKIP)

Коли WEP був доведений як повністю зламаний, для бездротових мереж терміново потрібен був новий схем безпеки. Протокол Temporal Key Integrity Protocol (TKIP) був розроблений на основі WEP для виправлення

всіх його відомих слабкостей. У цьому розділі буде надано короткий історичний огляд TKIP, а потім детальний технічний огляд протоколу [19].

Попередник TKIP, WEP, має кілька серйозних слабкостей і вважається повністю зламаним. Зловмисник може отримати секретний ключ, що використовується в WEP, протягом хвилини, або навіть дешифрувати пакети без знання ключа.

У 2001 році була створена робоча група IEEE 802.11i для розробки нових протоколів безпеки для сімейства WLAN 802.11.

Процес стандартизації зайняв досить багато часу, і WiFi Alliance хотів мати можливість надавати своїм клієнтам безпечне обладнання. В результаті WiFi Alliance створив власний стандарт безпеки на основі проектної версії 802.11i, який вони назвали WPA (WiFi Protected Access). Хоча TKIP забезпечує значно покращену безпеку порівняно зі старим стандартом WEP, він все ще побудований з використанням деяких тих же будівельних блоків, що і WEP. TKIP має деякі слабкості, найбільш значущою з яких є код цілісності повідомлення (MIC). Це використовується в новій атаці на TKIP. TKIP буде застарілим у наступній версії стандарту 802.11.

2.6.1. Огляд протоколу

TKIP мав одну важливу мету проектування; він повинен бути реалізований на старому апаратному забезпеченні WEP. З цієї причини були деякі серйозні обмеження щодо того, як міг бути спроектований TKIP. Через це обмеження протокол все ще використовує інкапсуляцію WEP, але був спроектований для надання додаткового захисту від усіх відомих атак на WEP. Стандарт 802.11-2007 визначає чотири модифікації WEP, зроблені TKIP.

- Використання нового коду цілісності повідомлення (MIC), який генерується ключовим криптографічним алгоритмом Michael.

- MIC, через обмеження проектування, не дуже безпечний. Тому TKIP реалізує контрзаходи для обробки цього.

- Захист від повторів за допомогою лічильника послідовності TKIP (TSC) на MPDU.

- TKIP використовує криптографічну функцію змішування ключів на пакет для подолання атак на слабкі ключі проти ключа WEP.

2.6.2. Інкапсуляція TKIP

На рисунку 2.8 128-бітний сеансовий ключ, TK, отримується через рукостискання EAPOL і пояснюється пізніше в цьому розділі. Як видно з малюнка, перший крок Temporal Key Integrity Protocol - це генерація ключа на пакет. Це робиться у двох фазах, позначених як фаза 1 та фаза 2 змішування ключів на рисунку 2.8.

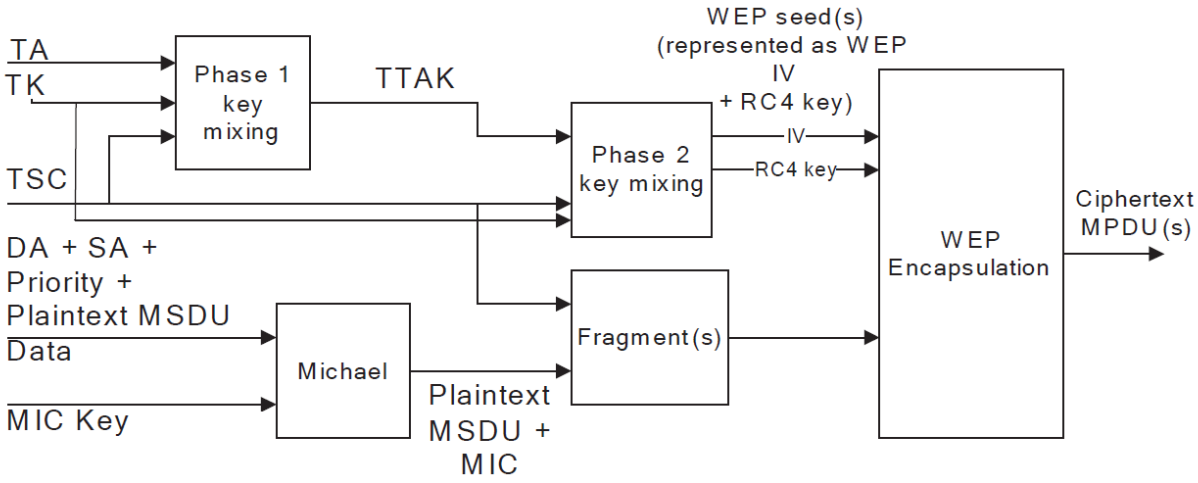

Рисунок 2.8 - Блок-схема інкапсуляції TKIP

Фаза 1 змішування ключів приймає три вхідні дані: TA, TK та 32 найстарші біти (MSB) TSC. Вихідною даними цієї функції є 80-бітний TTAK. Далі, друга функція змішування ключів використовує TTAK разом з TK та 16 найменших значущих бітів (LSB) TSC. Це призводить до насіння WEP, яке

представлене як 24-бітний IV WEP та 104-бітний ключ RC4. Причина змішування ключа у двох фазах полягає в тому, щоб зробити обчислення ключа менш інтенсивним, і таким чином полегшити навантаження для старого апаратного забезпечення WEP. Перша фаза повинна обчислюватися для кожного $216=65536$ пакету, оскільки вона використовує 32 MSB TSC. Обчислення другої фази змінюється для кожного пакету. TSC збільшується монотонно, і тому обчислення могло бути виконано заздалегідь.

Крім ICV, TKIP представив нову перевірку цілісності, яка називається MIC. MIC генерується алгоритмом Michael, який обчислює 8-байтовий код цілісності повідомлення (MIC) на основі MSDU у відкритому тексті. Крім MSDU, алгоритм Michael приймає три вхідні дані: DA, SA та однобайтове поле пріоритету. MSDU, TSC та обчислений MIC фрагментуються на два або більше MPDU, якщо це необхідно. MPDU потім вводиться в інкапсуляцію WEP як відкритий текст WEP.

2.6.3. Декапсуляція TKIP

При отриманні пакету, інкапсульованого Temporal Key Integrity Protocol, виконується процес декапсуляції, як показано на рисунку 2.9. Спочатку виконується витяг номера послідовності TSC та ідентифікатора ключа з WEP IV та розширеного IV TKIP. Пакети, які порушують послідовність, будуть відкинуті, тобто пакети, які не мають вищий TSC, ніж попередній пакет, відкидаються.

Конструкція насіння WEP виконується з тим самим двома фазами змішування ключів, що і в інкапсуляції. MPDU, виведений з декапсуляції WEP, потім збирається, якщо він був частиною фрагментованого MSDU. Далі, зібраний відкритий текст MSDU, DA, SA та поле пріоритету надсилаються до алгоритму Michael для створення MIC. Якщо MIC збігається з розшифрованим MIC, пакет приймається. Якщо ні, будуть активовані контрзаходи TKIP.

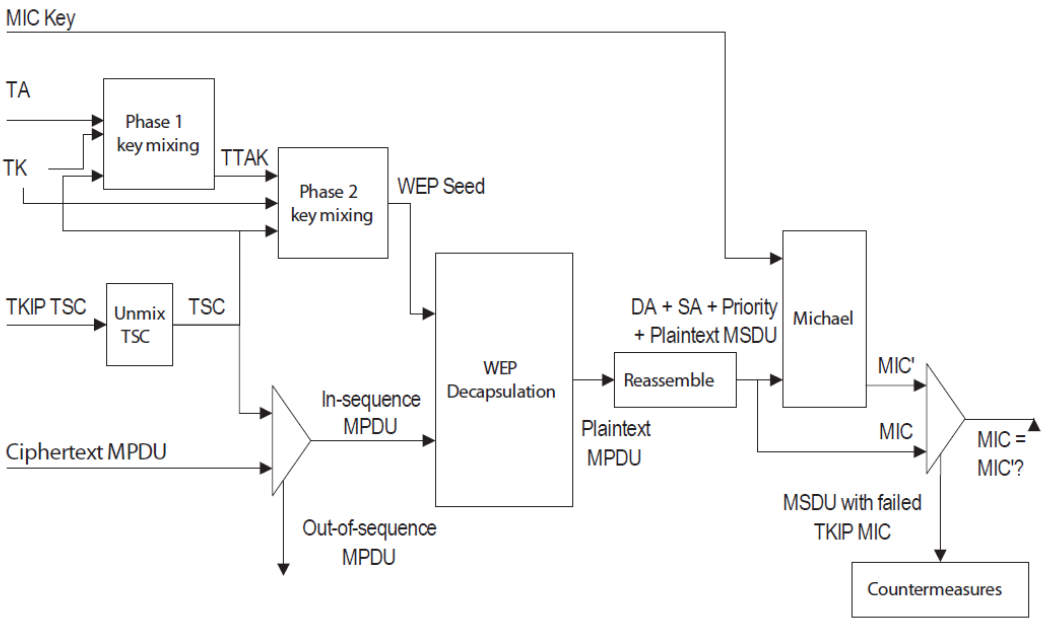

Рисунок 2.9 - Блок-схема декапсуляції TKIP

Однією з найбільших недоліків WEP було те, що він не захищав від підробки повідомлень. Це було через те, що ICV, заснований на CRC-32, не був достатньо безпечним. Для захисту від модифікації повідомлень та інших активних атак, TKIP включає MIC. MIC обчислюється на основі MSDU, який може бути фрагментований на кілька MPDU. MIC заснований на алгоритмі Michael, який є простим алгоритмом, але з значно покращеною безпекою порівняно з CRC32. Michael - це ключовий MIC, що означає, що він приймає секретний ключ як вхід, крім відкритого тексту. Ключ та вихід алгоритму мають довжину 64 біти. Ключ Michael походить від головного ключа. Хоча Michael безпечніший, ніж CRC-32, алгоритм Michael є слабким кодом цілісності повідомлення порівняно з ключовими криптографічними хеш-функціями, такими як SHA-1. Однак, розробники TKIP повинні були враховувати сумісність з устаткуванням при виборі алгоритму. Michael мав мету забезпечити лише 20 бітів безпеки. Це означає, що випадково обраний MIC має 1 шанс з $220=1,048,576$ бути прийнятим як дійсний. ICV WEP все ще обчислюється на основі відкритого тексту. Це призводить до того, що на даних обчислюються два коди цілісності повідомлення. Коли пакет

отримується, ICV WEP обчислюється так само, як і в WEP. Як і в WEP, пакет відкидається, якщо обчислений ICV не збігається з отриманим ICV. Якщо перевірка ICV успішна, MIC обчислюється та перевіряється з отриманим MIC, як описано раніше. Дуже малоймовірно, що ICV обчислюється правильно (пам'ятайте, що CRC-32 дуже добре виявляє помилки передачі), тоді як MIC не вдається, якщо не відбувається атака.

У дослідженні [18] автори показали процедуру злому WEP, злому WPA та злому WPA2. Було проведено багато досліджень щодо атак на протоколи безпеки. Більшість робіт було виконано в різних операційних системах, таких як Mac, Linux, Ubuntu та Windows XP.

Попередні роботи з WPA-TKIP в основному пов'язані з роботами [19], [21], що описують, як модифікована версія атаки Chopchop може бути виконана на мережі з підтримкою Quality of Service (QoS) або WiFi MultiMedia (WMM) для отримання потоку ключів для зв'язку від точки доступу до станції. Їхня атака, на відміну від попередніх атак на WEP, не є атакою на відновлення ключа. Вона дозволяє зловмиснику впроваджувати пакети в мережу і таким чином може призвести до атак на різні протоколи управління мережею. Нова атака на TKIP заснована на попередніх атаках на WEP, таких як атака Chopchop. Тут було виявлено спосіб отримання потоку ключів без знання ключа шифрування. Модифікована версія цієї атаки використовується для атаки на TKIP. Ми також вважаємо за доцільне віднестися до всіх попередніх атак на WEP і розглянути їх в еволюційній перспективі, які призвели до все більш витончених атак на протоколи безпеки бездротових мереж [19].

РОЗДІЛ 3. ІМПЛЕМЕНТАЦІЯ СТАНДАРТІВ ТА ПРОТОКОЛІВ БЕЗПЕКИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

3.1. Опис процесів імітаційного моделювання злому ключів безпеки

В цьому розділі буде проведено експеримент (імітаційне моделювання) з злому ключа безпеки типу WPA-TKIP. Тут ми будемо використовувати два програмні забезпечення: CommView та Aircrack-ng 1.2 RC 1.

У WEP статистичні методи можуть бути використані для прискорення процесу злому, зазвичай тільки прості методи перебору словника можуть бути використані проти WPA/WPA2 у спробі визначити спільний пароль. Це означає, що пароль повинен бути міститися у словнику, який ми використовуємо для злому WPA/WPA2. Тут ми застосовуємо атаку словника на захоплені зашифровані IV. Мета цього експерименту - показати, наскільки легко зламати бездротову мережу з шифруванням WPA-TKIP за допомогою машини Windows.

3.1.1 Програмне забезпечення, необхідне для моделювання

CommView для WiFi - це потужний монітор та аналізатор бездротових мереж для мереж 802.11 a/b/g/n/ac. Завантажений багатьма зручними функціями, CommView для WiFi поєднує продуктивність та гнучкість з простотою використання, незрівнянною в галузі.

CommView для WiFi захоплює кожен пакет в ефірі для відображення важливої інформації, такої як список точок доступу та станцій, статистика на вузол та на канал, сила сигналу, список пакетів та мережевих з'єднань, діаграми розподілу протоколів тощо. Надаючи цю інформацію, CommView для WiFi може допомогти вам переглядати та досліджувати пакети, виявляти мережеві проблеми та усувати несправності програмного та апаратного забезпечення.

Клацніть для отримання додаткових знімків екрана CommView для WiFi включає модуль VoIP для глибокого аналізу, запису та відтворення SIP та H.323 голосових комунікацій.

Пакети можуть бути дешифровані за допомогою користувацьких ключів WEP або WPA-PSK і дешифровані до найнижчого рівня. З понад 100 підтримуваними протоколами, цей аналізатор мережі дозволяє вам бачити кожну деталь захопленого пакету, використовуючи зручну структуру у вигляді дерева для відображення шарів протоколу та заголовків пакетів. Крім того, продукт надає відкритий інтерфейс для підключення користувацьких модулів дешифрування.

Кілька кейс-стадій описують реальні застосування CommView для WiFi в бізнесі, уряді та освітніх секторах.

CommView для WiFi - це комплексний та доступний інструмент для адміністраторів бездротових LAN, фахівців з безпеки, мережевих програмістів або будь-кого, хто хоче мати повну картину трафіку WLAN. Це додаток працює на Windows XP / Vista / 7 / 8 або Windows Server 2003 / 2008 / 2012 (як 32-, так і 64-бітні версії) і вимагає сумісного бездротового мережевого адаптера.

Aircrack-ng 1.2 RC 1 - це набір програмного забезпечення для мережі, що складається з детектора, аналізатора пакетів, зламника WEP та WPA/WPA2-PSK та інструменту аналізу для бездротових LAN 802.11. Він працює з будь-яким бездротовим мережевим інтерфейсним контролером, драйвер якого підтримує режим моніторингу в сирому вигляді, і може перехоплювати трафік 802.11 a, 802.11 b та 802.11 g. Програма працює під Linux та Windows; версія Linux упакована для OpenWrt та також була портована на платформи Zaurus та Maemo; і було створено концептуальний порт для iPhone.

У квітні 2007 року команда в Дармштадтському університеті технологій в Німеччині розробила новий метод атаки на основі статті,

опублікованої Аді Шаміром про шифр RC4. Ця нова атака, названа 'PTW', зменшує кількість векторів ініціалізації або IV, необхідних для дешифрування ключа WEP, і була включена в набір aircrack-ng з версії 0.9.

3.1.2 Процедура злому WPA-TKIP

Ми завантажуємо Aircrack-ng для Windows і потім ми завантажуємо CommView для WiFi. Потім ми встановлюємо CommView для WiFi.

Не має значення, чи встановлюєте ви його в режимі VoIP або стандартному режимі. Він автоматично встановлює необхідні драйвери. Дозвольте йому встановитися. Ми не зможемо підключитися до будь-якої мережі, використовуючи WiFi, коли використовуємо CommView.

Тепер відкриваємо CommView для WiFi і переходимо до опції файлу та натискаємо на захоплення файлу, як показано на рисунку 3.1.

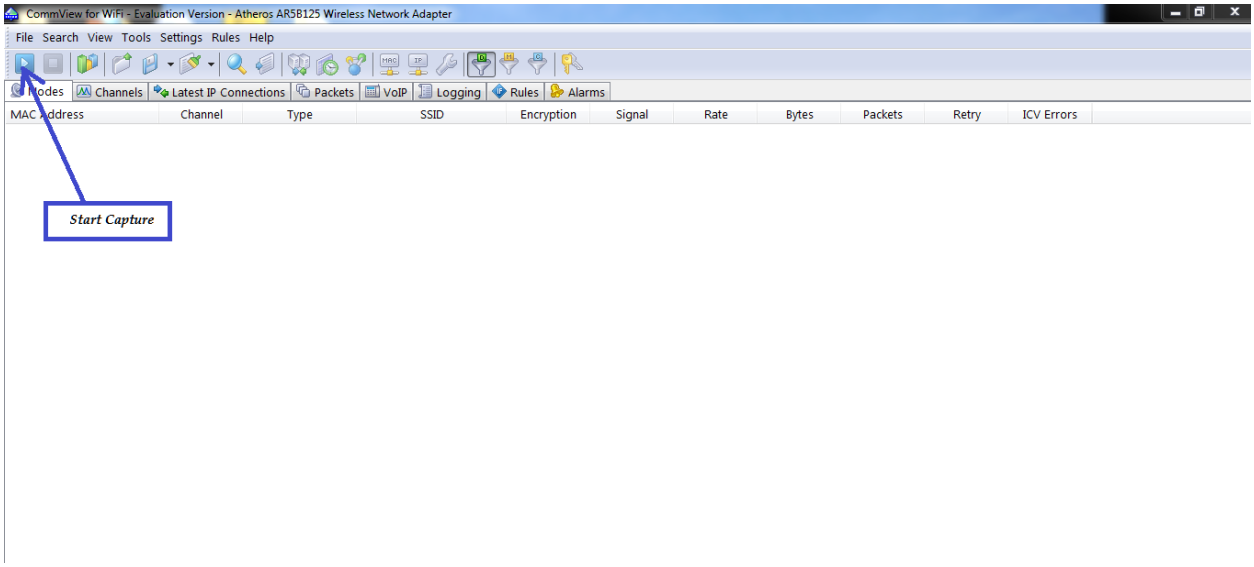

Рисунок 3.1 - Опція для захоплення

Повинно з'явитися нове вікно. Натисніть кнопку "РОЗПОЧАТИ СКАНУВАННЯ".

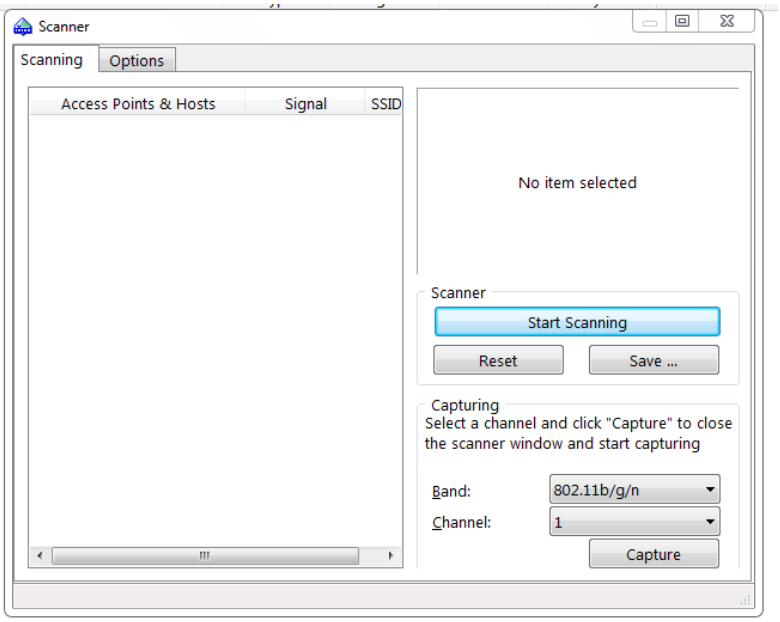

Рисунок 3.2 - Сканування

Після сканування відображається список усіх каналів та бездротових мереж, які працюють на зазначених каналах. Натисніть на бездротову мережу, яку ви хочете зламати, у правому стовпці та натисніть "ЗАХОПЛЕННЯ".

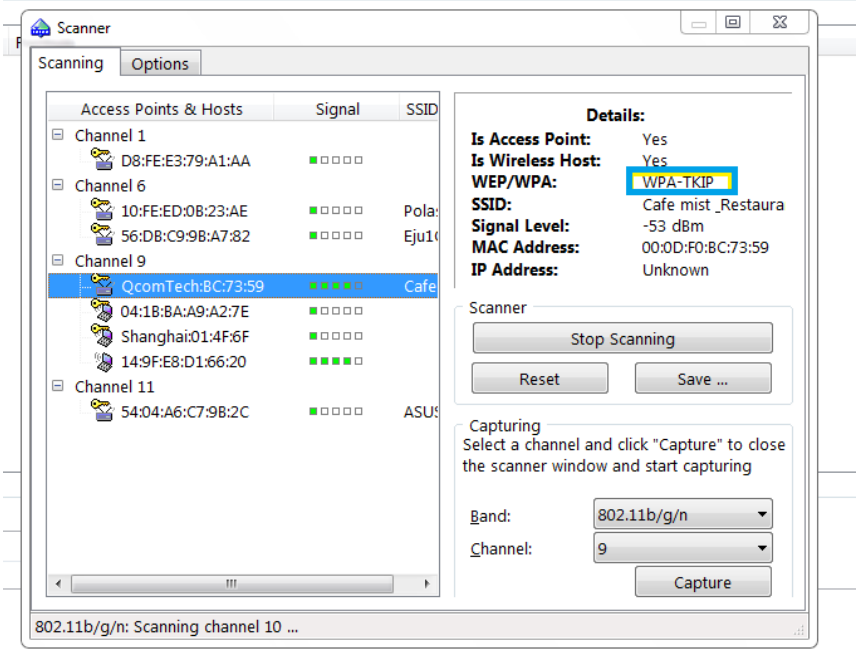

Рисунок 3.3 - Виявлення поблизу мережі

Вікно повинно закритися зараз, і ви повинні побачити, що CommView почав захоплювати пакети.

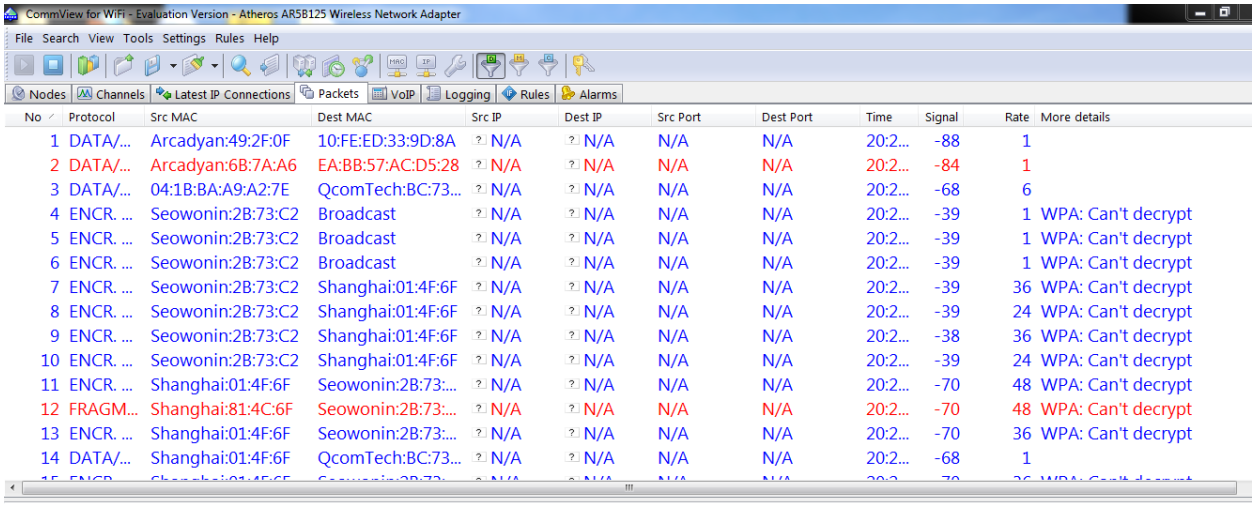

Рисунок 3.4 - Захоплення пакету

Тепер, коли пакети захоплюються, їх потрібно зберегти. Натисніть на Налаштування $\Longrightarrow$ Параметри $\Longrightarrow$ Використання пам'яті Змініть Максимальну кількість пакетів у буфері на 20000.

На вкладці "Пакети" є невелика панель інструментів, показана нижче:

Рисунок 3.5 - Нижня панель інструментів

Шоста кнопка дозволяє відкрити вміст поточного буфера пакетів у новому вікні. Для збереження натисніть Файл $\Longrightarrow$ Експорт журналів $\Longrightarrow$ Файли Wireshark/Tcpdump, введіть ім'я файлу та збережіть як файл .CAP. У нашому експерименті ім'я файлу - 'cafe-mist-3.CAP.

Відкрийте папку aircrack на робочому столі, потім перейдіть у папку bin і відкрийте aircrack-ng-gui, коли він з'явиться, просто натисніть відкрити/переглянути та знайдіть 'cafe-mist-3.CAP, який був збережений.

Виберіть опцію WPA та нам потрібно переглянути список слів. Тут ми використовуємо password.lst як список слів.

Перевірте розширену опцію та введіть ESSID та BSSID мережі, ключ якої ви хочете зламати.

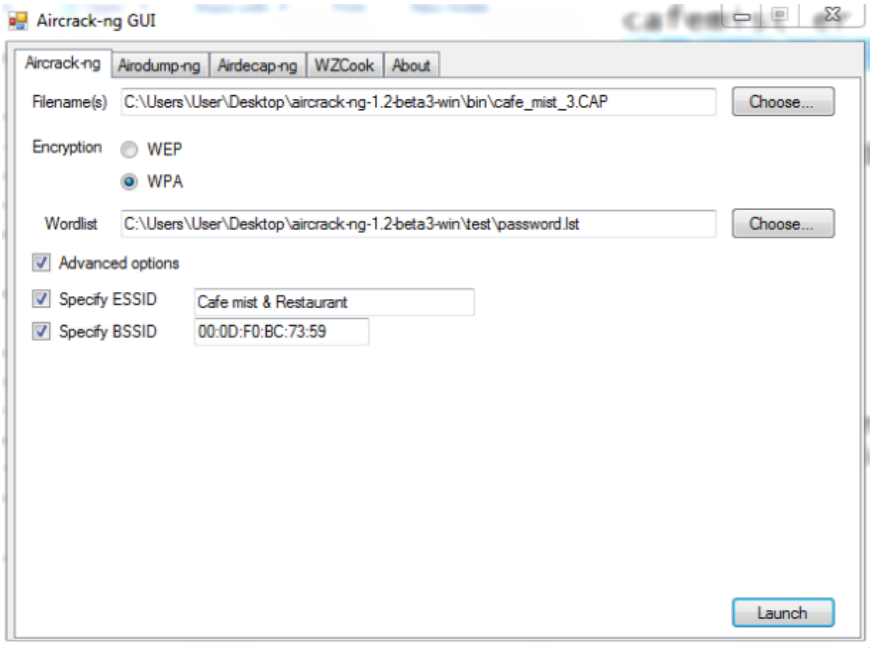

Рисунок 3.6 - Вибір файлу .CAP та списку слів

Потім натисніть Запуск.

Вище ми обговорили, як зламати пароль WPA-TKIP. У наступному розділі ми покажемо результати та проаналізуємо їх разом з обговоренням.

3.2. Результати проведення моделювання

3.2.1. Успішні спроби компрометації систем

В рамках проведеного дослідження було успішно здійснено компрометацію бездротової мережі з наступними параметрами:

- Протокол безпеки: WPA-TKIP

- Ідентифікатор ESSID: Cafemist та Restaurant

- Ідентифікатор BSSID: 00:0D:50:BC:73:59

- Тривалість атаки: 2 години

- Вектор атаки: Атака за словником

- Статус: Успішний

Рисунок 4.1 ілюструє результати успішної компрометації.

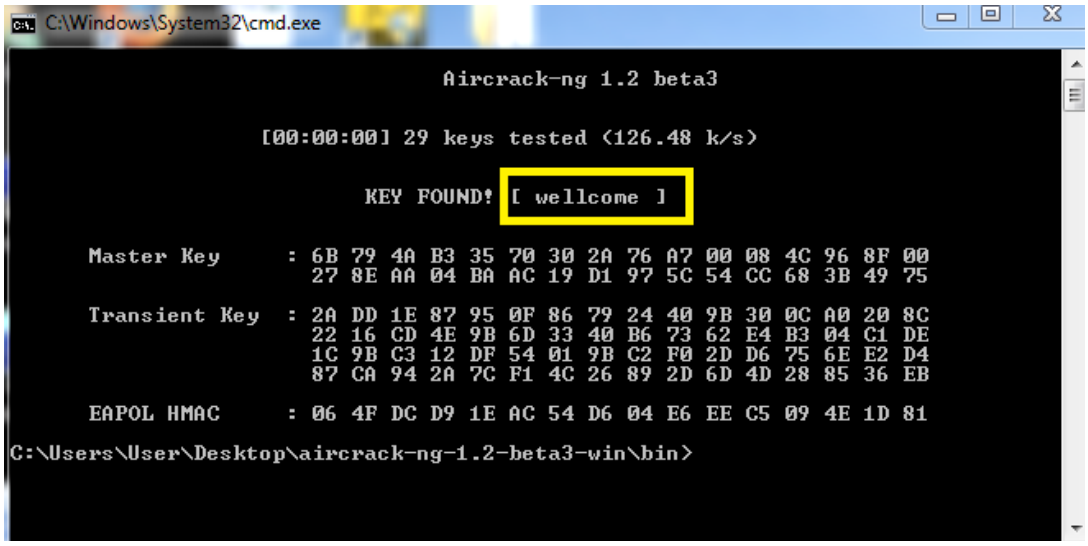

Рисунок 3.7 - Результат тесту 2

3.2.2. Неуспішні спроби компрометації систем

Деякі бездротові мережі не вдалося скомпрометувати протягом встановленого часу:

- Протокол безпеки: WPA-AES

- Ідентифікатор ESSID: Connectify-me

- Ідентифікатор BSSID: 5C:AC:4C:AA:4D:14

- Тривалість атаки: 2 години

- Вектор атаки: Атака за словником

- Статус: Неуспішний

Рисунок 3.8 демонструє візуалізацію результатів неуспішної спроби компрометації.

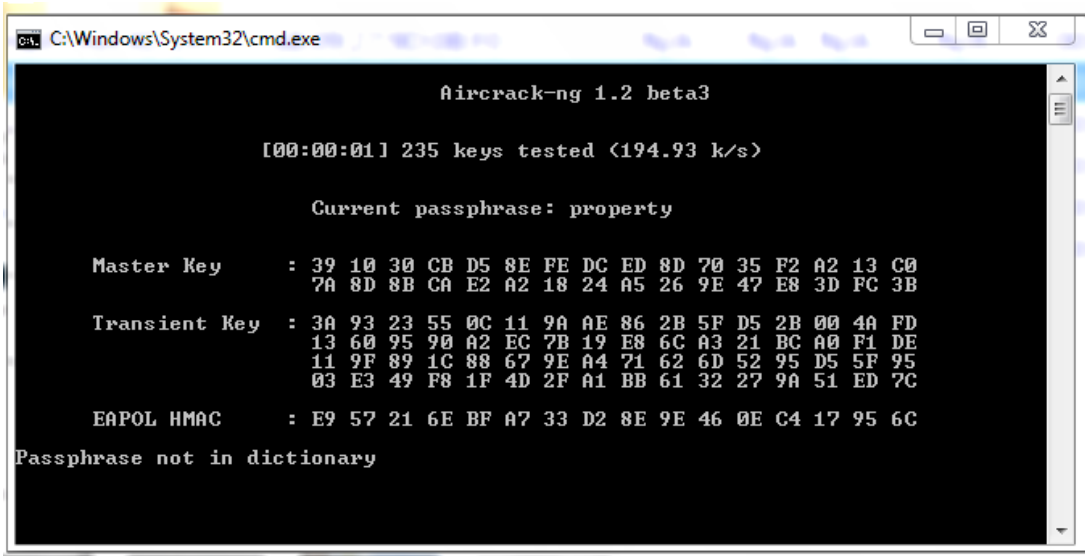

Рисунок 3.8 - Результат тесту 2

- Протокол безпеки: WPA-CCMP
- Ідентифікатор ESSID: jakia net Wifi
- Ідентифікатор BSSID: 5C:AC:4C:AA:4D:14
- Тривалість атаки: 2 години
- Вектор атаки: Атака за словником
- Статус: Неуспішний

3.2.3. Огляд статистики компрометації систем WPA, WPA2

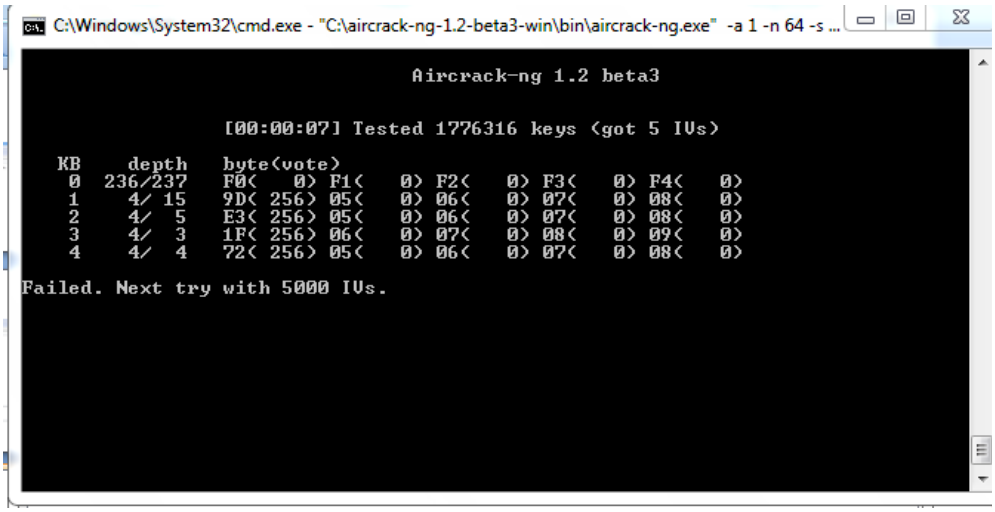

Рисунок 3.9 - Результат тесту 3

Таблиця 3.1 - Статистика огляду компрометації систем WPA, WPA2

	Статус злому	
Система, перевірена	Успішний	Неуспішний
Cafemist		
ESSID: Cafe mist & Restaurant	Так	-
BSSID: 00:0D:F0:BC:73:53		
Домашня мережа		
ESSID: jakia net Wifi	-	Так
BSSID: 00:0D:F0:BC:73:53		
Connectify me		
ESSID: Connectify-me	-	Так
BSSID: 5C:AC:4C:AA:4D:14		

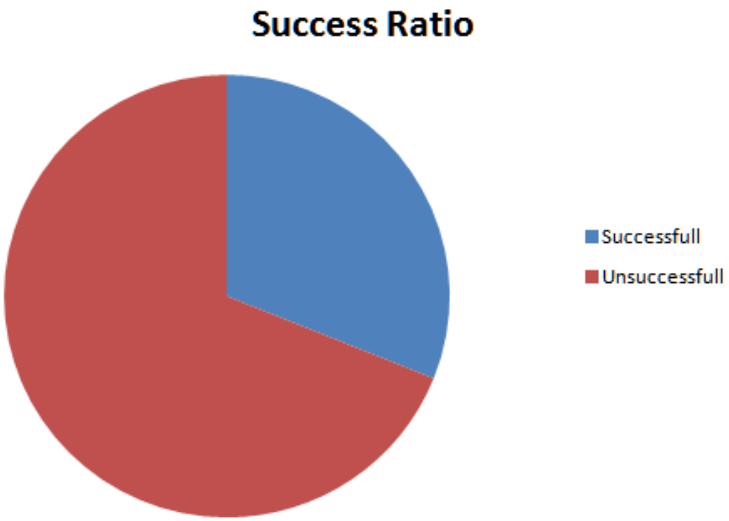

Рисунок 3.10 - Співвідношення успіху компрометації протоколів WLAN

3.3. Аналіз результатів

Компрометація ключа безпеки мережі "cafemist" (протокол безпеки WPA-TKIP) була успішною за допомогою атаки за словником. Цей результат свідчить про те, що цільовий пароль містився у використаному словнику, що

застосовувався для атаки на WPA/WPA2 мережі. У разі відсутності відповідності між захопленим хешем пароля та елементами словника, інструмент aircrack-ng не здатен визначити ключ. У даному випадку, завдяки присутності ключа безпеки в обраному словнику, Aircrack-ng успішно виявив збіг між словниковим терміном та захопленим хешем, що призвело до успішної компрометації. Якщо б ключ безпеки не був виявлений у поточному словнику, виникла б необхідність у виборі іншого словникового файлу.

Натомість, спроби компрометації мереж "Connectify-me" та "jakia net Wifi", які використовують протоколи безпеки WPA-AES та WPA-CCMP відповідно, виявилися невдалими. AES (Advanced Encryption Standard) є криптографічно стійким стандартом безпеки. Він пройшов ретельне криптографічне тестування, і наразі не виявлено ефективних методів його компрометації за умови належного вибору ключа. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), у свою чергу, ґрунтується на алгоритмах AES. З огляду на високу криптографічну стійкість AES, компрометація безпеки, що базується на ньому, є значно складнішою. Отже, спроби виявлення ключів безпеки цих двох мереж не принесли успіху.

Отже, у цьому розділі представлено обговорення отриманих результатів та зроблених висновків у ході виконання дипломної роботи. Розглянуто аспекти застосовності цих атак у реальних умовах, а також окреслені як позитивні, так і негативні уроки, здобуті під час дослідження. Варто зазначити, що TKIP (Temporal Key Integrity Protocol), що використовується у WPA1, сам по собі не є абсолютно вразливим у сенсі прямої криптографічної компрометації: для кожного пакета 48-бітний ініціалізаційний вектор (IV) комбінується зі 128-бітним тимчасовим ключем для генерації нового 104-бітного ключа RC4, що унеможливлює просту статистичну кореляцію. Крім того, WPA включає механізми захисту від активних атак (наприклад, повторного впровадження трафіку), посилений код цілісності повідомлення (Michael) та надійний протокол аутентифікації

(чотиристоронніє рукостискання). Наявна вразливість TKIP здебільшого пов'язана з атаками за словником, ефективність яких залежить від надійності обраного пароля.

TKIP використовує алгоритм потокового шифрування RC4 як свою основу. Натомість, AES є повністю окремою системою шифрування. Це 128-бітний, 192-бітний або 256-бітний блочний шифр, який наразі вважається золотим стандартом у системах шифрування, пропонуючи вищий рівень безпеки. CCMP базується на використанні AES, що робить його також високозахищеним. Наші експерименти підтверджують, що рівень успіху атаки значно варіюється залежно від використовуваного протоколу безпеки.

Вибір оптимального файлу словника виявився трудомістким процесом. Було проведено численні пошукові запити в мережі Інтернет для знаходження відповідних списків слів та словників. Проводився ітеративний підбір словникових файлів до тих пір, поки не було знайдено відповідність між словом зі словника та цільовим ключем безпеки, що зрештою дозволило досягти успішного результату.

Практичні експерименти продемонстрували значні відмінності у стійкості WEP та WPA2 до атак.

Атака на WEP була надзвичайно успішною та швидкою. В умовах тестової мережі, WEP-ключ був відновлений протягом декількох хвилин після збору необхідної кількості IVs. Це підтверджує, що WEP не забезпечує адекватного рівня безпеки і є вразливим до відносно простих та автоматизованих атак. Основні фактори, що сприяли успіху, – це обмежений простір IVs, повторне використання ключів та слабкість алгоритму RC4.

Атака на WPA2-PSK вимагала захоплення повного 4-стороннього рукостискання. Після його отримання, успіх відновлення PSK залежав виключно від міцності пароля та якості використовуваного словника. Якщо пароль був простим або був присутній у словнику, відновлення відбувалося досить швидко (від кількох секунд до декількох годин, залежно від

складності пароля та обчислювальної потужності). Проте, якщо пароль був складним (довгий, містив різні типи символів) і не був у словнику, атака методом грубої сили ставала надзвичайно трудомісткою, якщо не неможливою, для стандартних обчислювальних ресурсів. Це підкреслює, що основним слабким місцем WPA2-PSK є не сам криптографічний протокол, а вибір користувачами слабких паролів.

Бездротові мережі набувають широкого розповсюдження, проте їх архітектура безпеки все ще містить певні вразливості. Відповідно, ефективний захист цих мереж є критично важливим для запобігання несанкціонованому доступу до конфіденційних даних. Дана стаття містить стислий огляд ключових протоколів безпеки бездротових мереж: WEP, WPA та WPA2. Проблеми, притаманні WEP, були адресовані в WPA, який згодом еволюціонував до WPA2, стандартизованого як IEEE 802.11i. WPA інтегрує потоковий шифр RC4, тоді як 802.11i (WPA2) переважно використовує алгоритм AES. Зокрема, TKIP (Temporal Key Integrity Protocol) базується на RC4, тоді як CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) застосовує AES. У роботі представлено детальний аналіз та процес компрометації WPA-TKIP.

Бездротові мережі є вразливими до різноманітних кібератак. Ефективне протистояння цим загрозам вимагає глибокого розуміння технологій бездротової безпеки, розробки та суворого дотримання надійних політик безпеки, а також застосування посилених системних конфігурацій. Мотивацією даного дослідження стало загальне сприйняття WPA/WPA2 як стійких до компрометації протоколів, а також усвідомлення необхідності посилення безпеки бездротових мереж. Проте наші результати демонструють, що будь-яка бездротова мережа може бути схильною до успішних атак, якщо її налаштування та захист не відповідають високим стандартам безпеки.

У ході виконання даної роботи значний час було витрачено на підбір оптимального словникового файлу. Рекомендується розробка або впровадження більш ефективних інструментів та методологій для прискорення цього процесу в майбутніх дослідженнях. Отримані в даній роботі дані можуть бути використані для оптимізації інструментів компрометації паролів з метою підвищення їх ефективності.

Це дослідження емпірично підтвердило фундаментальні відмінності в рівнях безпеки, що надаються протоколами WEP, WPA та WPA2. WEP був продемонстрований як абсолютно ненадійний протокол, який не повинен використовуватися в жодній сучасній мережі. WPA представляв собою проміжне, але все ще вразливе рішення. WPA2 є значно більш стійким і забезпечує надійний захист, за умови використання надійних, складних паролів у режимі PSK та, де це можливо, розгортання WPA2-Enterprise для централізованої та міцнішої автентифікації.

Для забезпечення максимальної безпеки бездротових мереж, рекомендується:

1. Завжди використовувати WPA2 або новіший WPA3.
2. Для WPA2-PSK використовувати довгі, складні паролі, що містять комбінацію великих та малих літер, цифр та спеціальних символів.
3. Розглянути впровадження WPA2-Enterprise (802.1X/EAP) у великих організаціях.
4. Регулярно оновлювати програмне забезпечення маршрутизаторів та пристроїв для отримання патчів безпеки, що виправляють виявлені вразливості (наприклад, KRACK).

Майбутні дослідження можуть бути зосереджені на аналізі та практичній оцінці безпеки нового стандарту WPA3, який вводить додаткові механізми захисту, такі як SAE (Simultaneous Authentication of Equals) для посиленого 4-стороннього рукостискання.

Компрометація паролів типово вимагає значних обчислювальних ресурсів та обсягів пам'яті. Відповідно, доцільним є використання спеціалізованого сервера, призначеного виключно для таких операцій, що дозволить паралельно виконувати інші завдання тестування безпеки.

У подальших роботах та публікаціях планується представити детальний опис та аналіз процесу компрометації протоколів AES та CCMP, включаючи застосування ефективних методологій та інструментів для скорочення часу атаки, а також всебічне обговорення їхніх потенційних вразливостей та шляхів їх усунення.

ВИСНОВКИ

В дипломній роботі було здійснено аналіз концепцій, стандартів і протоколів безпеки локальних бездротових мереж (WLAN), що дозволило систематизувати наявні підходи до забезпечення конфіденційності, цілісності та доступності даних у таких мережах. Основною метою дослідження стало визначення ступеня захищеності локальної обчислювальної мережі залежно від застосованих протоколів безпеки, а також оцінка ефективності їх імплементації на практиці шляхом імітаційного моделювання атак.

Проведено критичний огляд основних вразливостей, притаманних бездротовим локальним мережам, зокрема слабких місць стандартів WEP, WPA та WPA2. Встановлено, що наявність криптографічних недоліків та обмежень у механізмах автентифікації й шифрування значною мірою впливає на загальний рівень безпеки мережі.

Проаналізовано алгоритмічні основи функціонування протоколів WEP, WPA, WPA2, а також механізмів, реалізованих у рамках стандарту IEEE 802.11i. Встановлено, що незважаючи на покращення у пізніших версіях стандартів (WPA2 порівняно з WEP і WPA), низька криптостійкість окремих компонентів (зокрема при використанні слабких паролів у режимі WPA2-PSK) зумовлює можливість успішного проведення атак із підбором ключа.

Описано та реалізовано методику моделювання атак на бездротові мережі з використанням спеціалізованого програмного забезпечення. Зокрема, здійснено моделювання атак на WEP та WPA2-PSK із застосуванням інструментів перехоплення трафіку, а також процедур дешифрування та підбору ключів доступу. Результати моделювання засвідчили низьку стійкість WEP до атак, що є підтвердженням його невідповідності сучасним вимогам інформаційної безпеки.

Представлено результати експериментального моделювання атак на мережі з різними типами захисту. На основі статистичного аналізу

результатів встановлено, що найменш стійким виявився протокол WEP, тоді як WPA2 при використанні складних ключів продемонстрував високу стійкість до компрометації. Водночас встановлено, що навіть сучасні протоколи залишаються вразливими у випадку нехтування принципами налаштування систем безпеки.

Здійснено порівняльний аналіз ефективності функціонування протоколів безпеки на основі кількісних показників, отриманих у результаті моделювання. Узагальнення отриманих результатів дозволило визначити переваги й недоліки кожного із протоколів, а також обґрунтувати доцільність використання WPA2 або новітніх рішень (зокрема WPA3) для забезпечення належного рівня захисту інформації в локальних бездротових мережах.

У ході дослідження підтверджено, що ефективна імплементація механізмів безпеки в локальних обчислювальних мережах вимагає не лише використання сучасних протоколів, але й дотримання принципів безпечної конфігурації, зокрема використання криптостійких ключів, автентифікації на основі сертифікатів та регулярного оновлення програмного забезпечення мережевого обладнання.

Отримані результати можуть бути використані як основа для вдосконалення політик інформаційної безпеки в організаціях, оптимізації процесів адміністрування бездротових мереж, а також для формування навчальних програм з кібербезпеки.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Lambert, P.A. (1989). Architectural considerations for LAN security protocols. Lecture Notes in Computer Science, 396, 5–11. https://doi.org/10.1007/3-540-51754-5_26
2. IEEE 802.11i Wireless LAN Security - https://www.brainkart.com/article/IEEE-802-11i-Wireless-LAN-Security_8486/
3. Toorani, M. (2016). Security Protocols in a Nutshell. arXiv preprint arXiv:1605.09771. https://arxiv.org/abs/1605.09771
4. What is WPA Authentication? - https://www.securew2.com/blog/what-is-wpa-authentication
5. Tobler, B. (2005). A Structured Approach to Network Security Protocol Implementation. Master's thesis, University of Cape Town. http://pubs.cs.uct.ac.za/archive/00000281/
6. T. I. of Electrical and E. Engineers, "Ieee standard for information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements," Amendment to IEEE Std 802.11TM, 1999 Edition (Reaff 2003), 2003.
7. Yang, M.-H. (2011). Security analysis of application layer protocols on wireless local area networks. Journal of Shanghai Jiaotong University (Science), 16, 586–592. https://doi.org/10.1007/s12204-011-1193-5
8. Baldi, M., Bianchi, M., Maturo, N., & Chiaraluce, F. (2012). A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks. arXiv preprint arXiv:1212.4991. https://arxiv.org/abs/1212.4991
9. F. M. Halvorsen, O. Haugen, M. Eian, and S. F. Mjølsnes, "An improved attack on TKIP," in Identity and Privacy in the Internet Age, 14th Nordic Conference on Secure IT Systems, NordSec 2009, Oslo, Norway, 14-16 October 2009. Proceedings, pp. 120-132, 2009.

10. Chakraborty, S., Khan, M., Amrita, Kaushik, P., & Nasseri, Z. (2021). An Extensive Review of Wireless Local Area Network Security Standards. In Applications of Artificial Intelligence and Machine Learning (pp. 591–604). Springer, Singapore. https://doi.org/10.1007/978-981-16-3067-5_44
11. Melnyk, V. (2018). Security Architecture Technical Investigation for IEEE 802.15.4 Low-Rate Wireless Personal Area Networks. Academic Journals and Conferences, 3(2), 92–111. https://doi.org/10.23939/acps2018.02.092
12. T. I. of Electrical and E. Engineers, “Ieee standard for information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements,” Amendment to IEEE Std 802.11TM, 1999 Edition (Reaff 2003), 2003.
13. Melnyk, V. (2019). Implementation Options of Key Retrieval Procedures for the IEEE 802.15.4 Wireless Personal Area Networks Security Subsystem. Academic Journals and Conferences, 4(1), 42–54. https://doi.org/10.23939/acps2019.01.042
14. Chiasserini, C.F., & Ganz, A. (2002). Security protocol for IEEE 802.11 wireless local area network. Mobile Networks and Applications, 7(3), 285–295. https://doi.org/10.1023/A:1019180916909
15. Shah, J.L. (2019). Secure Neighbor Discovery Protocol. International Journal of Business Data Communications and Networking, 15(1), 71–87. http://dx.doi.org/10.4018/ijbdcn.2019010105
16. Issac, B. (2014). Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks. arXiv preprint arXiv:1410.4398. https://arxiv.org/abs/1410.4398
17. Ogbu, H.N., & Agana, M.A. (2019). Intranet Security using a LAN Packet Sniffer to Monitor Traffic. arXiv preprint arXiv:1910.10827. https://arxiv.org/abs/1910.10827
18. Abdullahi, J., Abdulhamid, A.A., & Abbubakar, B. (2024). Implementation of a Secured Local Area Network (LAN): A Matter of Necessity in the

School of Engineering, Isa Mustapha Agwai I Polytechnic Lafia (IMAP), Nasarawa State. International Journal of Advanced Academic Research, 10(2), 1–9. https://www.openjournals.ijaar.org/index.php/ijaar/article/view/393

19. Boyanov, P., Stoyanov, S., Hristov, H., Fetfov, O., & Trifonov, T. (2023). Security Routing Simulation of the Local Area Network of Academic Departments Using a Link-State Routing Protocol - OSPF. Journal Scientific and Applied Research, 11(1), 47–58. https://doi.org/10.46687/jsar.v11i1.212
20. Verma, M., & Yadav, J. (2013). Comparative Analysis: Wi-Fi Security Protocols. International Journal of Engineering Research & Technology (IJERT), 2(12). https://www.ijert.org/comparative-analysis-wi-fi-security-protocols-3
21. Goldfisher, S., & Tanabe, S. (2010). IEEE 1901 access system: An overview of its uniqueness and motivation. IEEE Communications Magazine, 48(3), 150–157. https://doi.org/10.1109/MCOM.2010.5434372
22. Chung, M.Y., Jung, M.H., Lee, T.J., & Lee, Y. (2006). Performance analysis of HomePlug 1.0 MAC with CSMA/CA. IEEE Journal on Selected Areas in Communications, 24(7), 1411–1420. https://doi.org/10.1109/JSAC.2006.877219
23. N. Sklavos, "Book review: Samuelle, T.J. Mike Meyers' CompTIA Security + Certification Passport (Exam SY0-301) - 3rd ed. new york: Mcgraw-hill osborne media, 2011, 480p., \$30.00. ISBN: 13: 978-0071770385," Information Security Journal: A Global Perspective, vol. 23, no. 1-2, pp. 47-48, 2014.
24. Mohassel, R.R., Fung, A.S., Mohammadi, F., & Raahemifar, K. (2014). A survey on advanced metering infrastructure and its application in smart grids. In 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE) (pp. 1–8). IEEE. https://doi.org/10.1109/CCECE.2014.6901076

25. Cendrillon, R., Yu, W., Moonen, M., Verlinden, J., & Bostoen, T. (2006). Optimal multiuser spectrum balancing for digital subscriber lines. IEEE Transactions on Communications, 54(5), 922–933. https://doi.org/10.1109/TCOMM.2006.873415
26. A. H. Lashkari, S. Farmand, O. B. Zakaria, and R. Saleh, "Shoulder surfing attack in graphical password authentication," CoRR, vol. abs/0912.0951, 2009.
27. Ginis, G., & Cioffi, J.M. (2002). Vectored transmission for digital subscriber line systems. IEEE Journal on Selected Areas in Communications, 20(5), 1085–1104. https://doi.org/10.1109/JSAC.2002.1007407
28. Ahamed, S.V., Gruber, P.L., & Werner, J.J. (1995). Digital subscriber line (HDSL and ADSL) capacity of the outside loop plant. IEEE Journal on Selected Areas in Communications, 13(9), 1540–1549. https://doi.org/10.1109/49.464744
29. Christensen, K., Reviriego, P., Nordman, B., Bennett, M., Mostowfi, M., & Maestro, J.A. (2010). IEEE 802.3az: The road to energy efficient Ethernet. IEEE Communications Magazine, 48(11), 50–56. https://doi.org/10.1109/MCOM.2010.5621967
30. M. Ciampa, "A comparison of password feedback mechanisms and their impact on password entropy," Inf. Manag. Comput. Security, vol. 21, no. 5, pp. 344-359, 2013.
31. S. R. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," in Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001, Revised Papers, pp. 1-24, 2001.
32. S. Vaudenay and A. M. Youssef, eds., Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada,

August 16-17, 2001, Revised Papers, vol. 2259 of Lecture Notes in Computer Science, Springer, 2001.

33. Grafiati. (n.d.). Bibliographies: 'Security implementation'. Retrieved from https://www.grafiati.com/en/literature-selections/security-implementation/
34. Grafiati. (n.d.). Bibliographies: 'Network protocol implementation'. Retrieved from https://www.grafiati.com/en/literature-selections/network-protocol-implementation/

БІБЛІОГРАФІЧНА ДОВІДКА

Тема дипломної роботи: “ Імплементація концепцій та протоколів безпеки локальної обчислювальної мережі ”

Обсяг пояснювальної записки: 76 аркушів.

Дата закінчення роботи: 11 червня 2025 р.

Підпис студента _____