МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____ к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: «СПОСОБИ ПОБУДОВИ ЗАХИСТУ КАНАЛУ НА ОСНОВІ ПРОТОКОЛУ IEEE 802.11 AC»

студент групи СЗД-42 Тромса Кирило Олегович _____
(підпис)

Науковий керівник: к.т.н., доцент Пепа Юрій Володимирович _____
(підпис)

Нормоконтроль: Гребенніков Асаді Болдхоядович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н. Г.В. Шуклін

(підпис)

«_____»_____ 2022 р.

ЗАВДАННЯ

на атестаційну роботу

студенту: Тромсі Кирилу Олеговичу

1. Тема роботи: «Способи побудови захисту каналу на основі протоколу IEEE 802.11 ac», затверджена наказом по університету від « » 2022 р. за № .

2. Термін здачі студентом оформленої роботи « 2 » червня 2022 р.

3. Об'єкт дослідження: є побудування захисту каналу бездротової мережі по протоколу IEEE 802.11 ac.

4. Предмет дослідження: є методи та засоби побудування захисту каналу бездротової мережі по протоколу IEEE 802.11 ac.

5. Мета роботи: побудування захисту каналу на основі протоколу IEEE 802.11 ac.

6. Перелік питань, які мають бути розроблені:

1) Аналіз мережевих стандартів бездротового доступу; 2) Розгляд принципів роботи Wi-Fi мереж; 3) Аналіз можливих видів загроз та протоколів інформаційної безпеки, котрі боряться з ними в мережах Wi-Fi; 4) Методи захисту каналу по протоколу.

7. Перелік публікацій:

8. Перелік ілюстративного матеріалу: Презентація виконана на слайдах для подання за допомогою світлопроектору та комп'ютерних засобів.

9. Дата видачі завдання «____» _____ 2022 р.

Науковий керівник _____ Пепа Ю.В.

(підпис)

Завдання прийняв до виконання _____ Тромса К.О.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «16» лютого 2022 р.

№ з/п	Назва етапів атестаційної роботи	Строк виконання етапів роботи	Примітка
1	Огляд літератури	до 29.03.22 р.	виконано
2	Написання першого розділу роботи	до 10.04.22 р.	виконано
3	Написання другого розділу роботи	до 27.04.22 р.	виконано
4	Написання третього розділу роботи	до 08.05.22 р.	виконано
5	Оформлення атестаційної роботи	до 16.05.22 р.	виконано
6	Підготовка демонстраційних матеріалів	до 20.05.22 р.	виконано

Студент: СЗД-42 Тромса К.О. _____
(підпис)

Науковий керівник: к.т.н., доц. Пепа Ю.В. _____
(підпис)

Нормоконтроль: Гребенніков А.Б. _____
(підпис)

РЕФЕРАТ

Текстова частина бакалаврської роботи містить: 52 сторінки, 23 рисунки, 8 таблиць та 22 джерела.

В даній роботі було розглянуто безпровідні мережі та передачі даних по ним. Детальніше розглянуто безпровідні локальні мережі, принципи її роботи та захист для уникнення атак і забезпечення цілісності персональних даних в майбутньому.

Об'єкт дослідження – побудова захисту каналу по протоколу IEEE 802.11 ac.

Предмет дослідження – методи та засоби побудови захисту безпровідних мереж по протоколу IEEE 802.11 ac.

Мета роботи – покращення захисту та надійності безпровідних мереж.

Галузь використання – інформаційна безпека.

Ключові слова: WI-FI, БЕЗПРОВІДНІ ЛОКАЛЬНІ МЕРЕЖІ, АВТЕНТИФІКАЦІЯ, ЗАХИСТ, ПРОТОКОЛ, СТАНДАРТ, ЗЛОМ, WEP, WPA, WPA2.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Wi-Fi – Wireless Fidelity

DCF (Discounted cash flow) – розподілений режим доступу

PCF (Point coordination function) – централізований метод доступу

DSSS (Direct Sequence Spread Spectrum) – широкополосна модуляція з прямим розширенням спектра

P2P – мережа Peer-to-Peer

MIMO – Multiple Input Multiple Output

WLAN (Wireless Local Area Network) – бездротова локальна мережа

SSID (Service Set Identifier) – ідентифікатор бездротової мережі

WEP – Wired Equivalent Privacy

WPA – Wi-Fi Protected Access

IEEE – Institute of Electrical and Electronic Engineers

TKIP – Temporal Key Integrity Protocol

AES – Advanced Encryption Standard

ВСТУП

В наш час безпровідні технології набувають швидкої популярності. Незабаром, якщо вже не так, кількість безпровідних, працюючих пристроїв досягне числа рівного кількості людей на планеті, адже на кожну особу приблизно 3-4 пристрої: телефон, планшет, ноутбук і т.д. Ми всі залежні від цих гаджетів, бо в собі вони тримають як і розважальний контент так і всі наші важливі документи:

- ситуацію в світі;
- ігри та відео контент;
- водійське посвідчення, студентський квиток і т.ін.

Працюють всі пристрої за допомогою безпровідних мереж на основі протоколу IEEE 802.11, часто називають також – Wi-Fi. Використовується для побудування мереж в публічних місцях, та для організацій з безпровідним локальним підключенням. Завдяки цій технології ми можем обмінювати, скачувати, передавати різну інформацію, тому її захист повинен бути на першому місці.

Метою роботи є різні способи побудування захисту каналу на онові протоколу IEEE, а саме 802.11ac.

Об’єктом дослідження є безпровідні (локальні) мережі.

Предмет дослідження – методи захисту в мережах безпровідного доступу.

1 ФУНКЦІОНУВАННЯ БЕЗПРОВІДНИХ МЕРЕЖ СТАНДАРТІВ IEEE 802.11

Розвиток не стоїть на місці, особливо в технічній сфері, тому люди виготовляють і впроваджують нові технології, котрі суттєво відлічаються від свої попередників: продуктивніші, ефективніші та більш захищені. Так само розвиваються і бездротові мережі, з самого початку безпровідні пристрої могли підтримувати швидкість не більше 1-2 Мбіт/с. В теперішній час це здається занадто мало. Наразі технології досягли швидкості до 1 Гбіт/с передачі даних по безпровідній мережі, що вже являється претендентом для конкуренції з кабельними мережам. Класифікувати безпровідні мережі можна за декількома параметрами:

- швидкість передачі даних;
- радіус дії;
- тип кодування інформації.

1.1 Класифікація безпровідних мереж передачі інформації

На ринку можна знайти чималий асортимент обладнання безпровідного доступу:

- обладнання для побудови Wi-Fi мереж;
- GSM;
- WiMAX;

Відомо три основні види використання таких мереж:

- офіси, зали і т.ін.;
- підключення віддалених локальних мереж одна з одною;
- побудова територіально розподілених безпровідних мереж.

Для підключення мереж на великих відстанях, або великих самих по собі мереж можуть бути використанні обладнання з спрямованими антенами або підсилювачі і розміщення антен на великій висоті.

Більш детальний розгляд безпровідних мереж передачі інформації, то можемо виділити чотири типи (рис. 1.1).

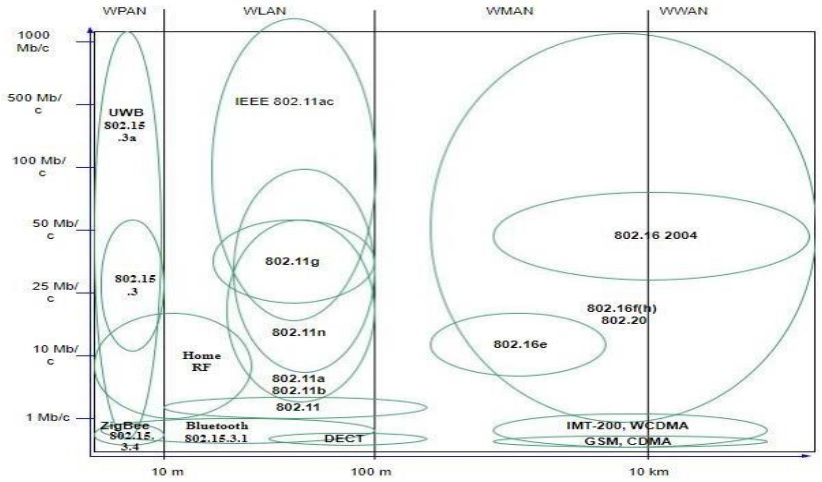

Рис. 1.1 – Класифікація технологій БМПІ

Безпровідні персональні мережі (WPAN - wireless personal area network) – мережа, радіус дії якої орієнтовно сягає від декількох сантиметрів і до 15 м. Призначені для з’єднання обладнання в межах робочого місця, наприклад, зв'язку стільникового телефону і ноутбука або комп'ютера і принтера. Найбільш поширеною технологією з цієї категорії – Bluetooth.

Безпровідні локальні мережі (WLAN – wireless local area network) – радіус до 100 метрів, якщо розгорнути підсилювачі і антени дальність дії може зростати понад кількох сотень метрів. В простонародді їх називають Wi-Fi мережами. Основне призначення - розгортання безпровідних мереж в приміщеннях, хоча є випадки коли їх використовують на відкритих майданчиках. Базова послуга – доступ в Internet або до корпоративної мережі.

Безпровідні міські мережі (WMAN – Wireless Metropolitan Area Network) – радіус дії звичайної станції до 10 км. За допомогою обладнання, що є класом фіксованого широкосмугового безпровідного доступу (Fixed Broadband Wireless Access (FBWA)). За допомогою них будується розподілена безпровідна операторська мережа масштабу міста або великих корпоративних мереж.

Безпровідні глобальні мережі WWAN. Глобальні бездротові мережі

представлені в основному супутниковими системами зв'язку.

Щоб розгледіти потенціал і функціональну спроможність вище згаданих видів безпровідних мереж передачі інформації наведено таблицю, в якій описуються основні характеристики такі як, швидкість передачі даних в кожній технології і дальність зв'язку (табл. 1.1).

Таблиця 1.1

Характеристика технологій БМПІ

WPAN		
IEEE 802.15.1 (Bluetooth)	64 Кб/с-1 Мб/с	10-100 м
Home RF	1(2) Мб/с – 10(20) Мб/с	До 50 м
IEEE 802.15.3	11, 22, 33, 44, 55 Мб/с	До 10 м
IEEE 802.15.4 (ZigBee)	20, 40, 250 Кб/с	До 10 м
IEEE 802.15.3a (UWB)	100 Мб/с – 1,3 Гб/с	5-10 м
WLAN		
IEEE 802.11	1-2 Мб/с	300 м
IEEE 802.11a	6, 12, 24 (9, 18, 36, 48, 54) Мб/с	100 м
IEEE 802.11b	2, 5 – 11 Мб/с (до 33 Мб/с)	100 м
IEEE 802.11g	11 – 54 Мб/с	100 м
IEEE 802.11n	Понад 160 Мб/с	100 м
IEEE 802.11ac	Понад 1 Гбіт/с	100 м
DECT	70 Кб/с	30-70 м (в приміщені), 100-400 м (ззовні)

Продовження табл. 1.1

WMAN		
IEEE 802.11.16 2004 (WiMAX)	30-40 Мб/с (до 70Мб/с)	2,5-5 км (рухомі абоненти (до 15 км/год)) 40-50 км (Стаціонарні абоненти)
IEEE 802.11.16e (WiMAX)	до 15 Мб/с	2-7 км
IEEE802.11.16f(h) (WiMAX) – перспективні	до 10 Тб/с	Підтримка мобільності (до 300 км/год)
WWAN		
IEEE 802.20 (WiMAX)	Понад 1 Мб/с	Підтримка мобільності і мобільної структури
GSM	9,6 Кб/с	Сота до 35 км
CDMA	14,4 Кб/с	Сота до 20 км
IMT-2000	2 Мб/с (для малорухомих абонентів) 384 Кб/с (для рухомих абонентів)	Сота 20-40 км

В теперішньому світі всі мережі мають широке застосування, але найбільшого поширення зазнала технологія Wi-Fi. ЇЇ використовують як і провідні мережі, так і безпровідні. В основному її використовують для забезпечення території покриттям.

Безпровідні локальні мережі (Wireless Fidelity (Wi-Fi)), створені на основі стандартів IEEE 802.11. На початку свого існування визначення “Wi-Fi” використовували щоб позначити технологію, котра надає зв’язок в діапазоні 2,4 ГГц (частот), но в наш час цей термін використовують для безпровідних мереж. Wi-Fi використовується для обміну даними між вузлами, та вважається

гнучкою системою для обміну інформації до подібної їй провідній мережі, яка знаходиться в приміщені чи на певній території.

1.2 Режим роботи стандарту IEEE 802.11

В 1990 році IEEE 802 вирішили створити групу для роботи по стандартам для безпровідних мереж. За основу завдання вони взяли створення загального стандарту мереж, які б працювали в діапазоні 2.4 ГГц з швидкістю 1-2 Мбіт/с. В 1997 році вони завершили розробку і випустили в світ першу сертифікацію 802.11.

Цей стандарт вважається першим для пристроїв WLAN, але швидкість передачі інформації не була задовільною для користувачів. Для того, щоб задовільнити користувачів, розробники почали роботу над новим стандартом, та вже восени 1999 року схвалили удосконалення існуючого стандарту, та назвали його 802.11 High rate (802.11b). Після випуску нового стандарту пристрої могли обмінюватись даними на швидкості 11 Мбіт/с та більше.

Стандарт IEEE 802.11 використовується в більшості галузей, тому було вирішено використовувати різні топології, які були б більш підходящими в різних ситуаціях. Стандарт IEEE 802.11 використовують декілька мережевих топологій:

- режим інфраструктури;
- режим Ad Hoc;
- топологія бездротової сітки;
- P2P мережева топологія.

1.3 Огляд існуючих стандартів сімейств IEEE 802.11

В наш час є безліч стандартів групи IEEE 802.11, але є найбільш вживані та розповсюджені:

- базовий IEEE 802.11;
- 802.11 a;

- 802.11 b;
- 802.11 g;
- 802.11 n;
- 802.11 s;
- 802.11 p;
- 802.11 ac.

Всі стандарти працюють на двох нижніх рівнях моделі OSI (фізичному та канальному).

1.3.1 Базовий стандарт IEEE 802.11

Влітку 1997 року оприлюднили стандарт IEEE 802.11 під назвою “Специфікація фізичного рівня і рівня контролю доступу до каналу передачі бездротових локальних мереж”. Протокол (рис. 1.2) визначав архітектуру мереж, формати пакетів, захист даних та автентифікацію.

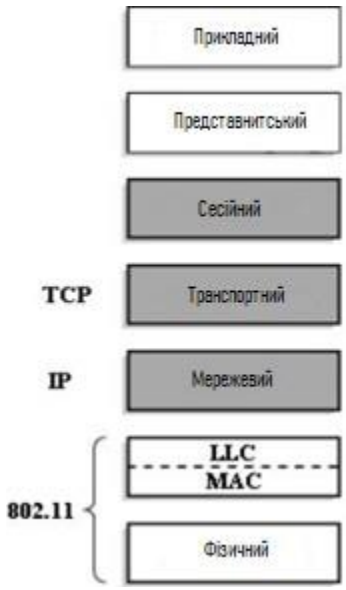

Рисунок 1.2 – Рівні моделі OSI та їх відповідність до стандарту IEEE 802.11

Як і було казано раніше, стандарт 802.11 працював з обладнанням 2.4 ГГц та швидкістю до 2 Мбіт/с. Базовий протокол на своєму фізичному рівні застосовує 2 методи передачі даних: FHSS (Frequency Hopping Spread Spectrum) та DSSS (Direct Sequence Spread Spectrum).

FHSS – технологія передачі в котрій сигнал модулюється за допомогою вузькосмугового сигналу носія, що стрибає у рандомній або ж передбачуваній послідовності від частоти до частоти, технологія забезпечує менший рівень перешкод, адже сигнал з вузькомугової системи буде мати вплив на сингал розповсюдженого спектру лише в тому випадку, коли обидва сигнали мають однакову частоту.

DSSS – техніка поширення спектру, за допомогою якої вихідний сигнал даних множиться а псевдо-випадковий код розповсюдження шуму. Цей код має більш високу швидкість чіпа. DSSS (рис. 1.3) значно покращує захист від непотрібних (заклинюючих) сигналів, особливо вузькомугових і робить сигнал менш помітним.

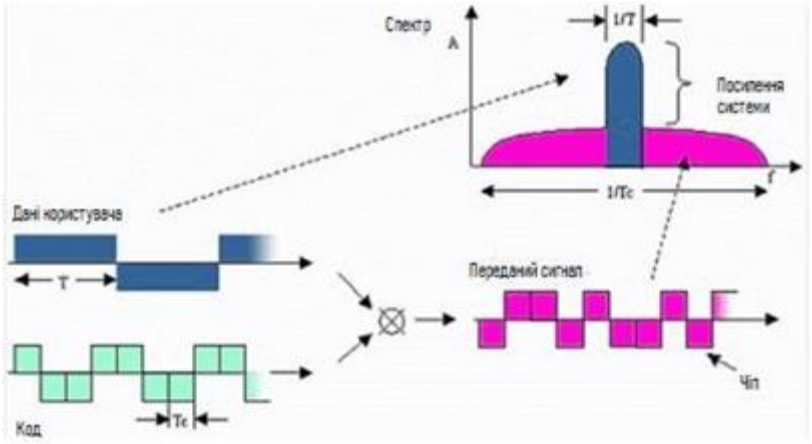

Рисунок 1.3 – Метод прямої послідовності DSSS

FHSS схожий до методу перескоку частоти, але в мережах GSM і EDGE. Пристрої цього методу працюють в частотному діапазоні від 2.402 до 2.480 ГГц і ділять його на 79 рівних неперервних каналів, шириною 1МГц. DSSS в багатьох аспектах нагадує метод в системі кодового розділення CDMA. Ці дві технології забезпечують в мережі максимально можливу для них, але мізерну по теперішнім міркам, швидкість понад 2 Мбіт/с.

1.3.2 802.11 a

IEEE 802.11 a був впроваджений в 1999 році. Основою даного протоколу була робота в діапазоні 5 ГГц з швидкістю передачі 54 Мбіт/с. Стандарт використовує технологію побудови радіоканалу на основі мультиплексування з ортогональним поділом частот (OFDM). Якщо простіше, передача даних виконується за допомогою ряду незалежних радіосигналів. Даний метод призводить до зниження швидкості передачі, що безпосередньо забезпечує захист від завад зв’язку при досягненні високої пропускної здатності. Модулюється за допомогою BPSK, QPSK, 16- і 64-позиційної квадратурної амплітудної модуляції (QAM). Стандарт має вісім швидкостей передачі, три з яких є обов’язковими, ті шо залишились - додатковими. В табл. 1.2 наведені всі види швидкостей.

Таблиця 1.2

Швидкість передачі для різних видів модуляції стандарту 802.11 a

Модуляція	Швидкість кодування	Швидкість передачі Мбіт/с
BPSK (Обов'язкова)	1/2	6
BPSK (Додаткова)	3/4	9
QPSK (Обов'язкова)	1/2	12
QPSK (Додаткова)	3/4	18
QAM-16 (Обов'язкова)	1/2	24
QAM-16 (Додаткова)	3/4	36
QAM-64 (Додаткова)	2/3	48
QAM-64 (Додаткова)	3/4	54

Стандарт 802.11 a поділений на 3 підвиди, які не схожі між собою по максимальній потужності випромінювання:

- нижній діапазон – потужність до 100 мВт;

- середній діапазон – потужність до 250 мВт;

- верхній діапазон – потужність до 1 Вт.

Недоліки цього стандарту – високе споживання потужності та малий радіус, на відміну з обладнанням котрі працюють на діапазоні 2.4 ГГц (радіус приблизно в тричі більший).

1.3.3 802.11 b

IEEE 802.11 b – вдосконалений попередник IEEE 802.11. Максимальна швидкість – 11 Мбіт/с, але не забуває про втрати протоколу CSMA/CA, та на виході отримуємо по TCP – 5,9 Мбіт/с, UDP – 7,1 Мбіт/с.

802.11 b працює в частоті 2.4 ГГц з каналом 83.5 МГц. Діапазон розділено на 14 каналів з інтервалом в 5 МГц, але в останнього 10 МГц (рис. 1.4).

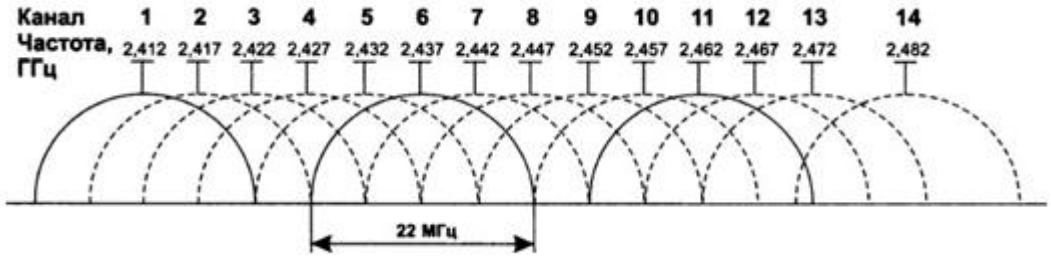

Рисунок 1.4 – Розділення діапазону на 14 каналів

Канал в 5 МГц є замалим, тому використовується ширина каналу в 22 МГц. Тобто, відбувається об'єднання декількох каналів щоб збільшити ширину та забезпечити безперешкодну передачу даних.

1.3.4 802.11 g

IEEE 802.11 g є модернізацією стандарту IEEE 802.11 b. Використовуючи ефективніші технології модуляції, швидкість було збільшено до 54 Мбіт/с (табл. 1.3).

Таблиця 1.3

Швидкість передачі даних стандарту IEEE 802.11 g

Стандарт передачі	Швидкість передачі	Вид модуляції
IEEE 802.11g (обов'язковий)	5,5/11 Мбіт/с	CCK
IEEE 802.11g (обов'язковий)	до 54 Мбіт/с	OFDM
IEEE 802.11g (опціональний)	до 33 Мбіт/с	PBCC
IEEE 802.11g (опціональний)	до 54 Мбіт/с	CCK-OFDM

По аналізу чутливості стандарту 802.11 g можна дійти до висновку, що стандарт масштабується вниз до відповідної межі, тому в перехідному діапазоні швидкість змінюється плавно.

1.3.5 802.11 n

802.11 n вдосконалена варіація стандарту 802.11 g, порівняно з пристроями. З'являється можливість працювати на вибраному з двох діапазонів (2.4 ГГц та 5 ГГц).

В канбальному рівні реалізували ефективніше застосування допустимої пропускної здатності. На виході максимальну швидкість можна було отримати в 10 разів більшу ніж в попередніх стандартів – 600Мбіт/с; створення багатоканального входу/виходу, або ж MIMO; збільшення ширини смуги пропускної здатності від 20 МГц до 40 МГц.

Багатоканальний вхід/вихід (MIMO).

Стандарт 802.11 n запровадив в мережу MIMO. Розшифровується воно як Multi-Input і Multiple-output. У 80-х та на початку 90-х років було проведено значні дослідження у галузі багатоканальної техніки передачі з метою використання багатоканального розповсюдження для передачі декількох потоків інформації через декілька антен одночасно (рис. 1.5).

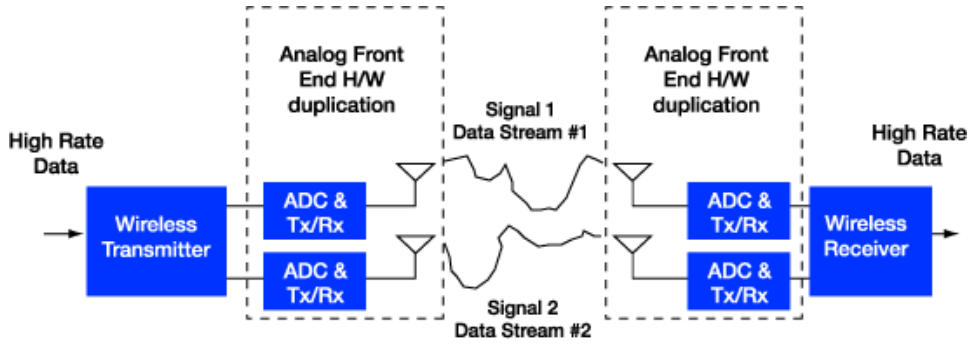

Рисунок 1.5 – Найпростіша система MIMO 2x2

В її основі лежала концепція багато шляхового поширення, кожен сигнал, який передається від антени, стикається і відскакує від непрозорих твердих предметів на шляху до приймача. Отриманий сигнал буде сумішшю переданого сигналу, що надходить на різні проміжки часу, а також під різними кутами прибуття. Теорія полягала в тому, що якщо кілька потоків були налаштовані таким чином, що передані ними сигнали були достатньо відокремленими, так що кожен з прийнятих сигналів може бути незалежно декодований на приймачі - це призвело б до збільшення пропускної здатності системи.

Кількість антен під час одночасної роботи прямо пропорційно відноситься величині максимальної швидкості передачі даних. Чим більше антен – тим більша швидкість передачі. Але нарахування тільки великої кількості антен не збільшує максимальну швидкість передачі і розширення діапазону, це буде працювати тільки з пристроями які підтримують стандарт IEEE 802.11 n. Саме в цих пристроях застосовується метод обробки сигналу, який визначає алгоритм роботи MIMO – пристроїв при застосуванні певної кількості антен.

Ширина смуги пропускання каналу 40 МГц.

Другим удосконаленням стандарту являється збільшення ширини каналу з 20 МГц до 40 МГц. В табл. 1.4 наведено швидкості передачі і швидкості кодування видів модуляції для каналів зі смугами в 20 МГц і 40 МГц.

Таблиця 1.4

Швидкість передачі і кодування в смугах частот 20 МГц і 40 МГц

MCS Index	Type	Coding Rate	Spatial Streams	Data Rate (Mbps) with 20 MHz CH		Data Rate (Mbps) with 40 MHz CH	
				800 ns	400 ns	800 ns	400 ns
0	BPSK	1/2	1	6.50	7.20	13.50	15.00
1	QPSK	1/2	1	13.00	14.40	27.00	30.00
2	QPSK	3/4	1	19.50	21.70	40.50	45.00
3	16-QAM	1/2	1	26.00	28.90	54.00	60.00
4	16-QAM	3/4	1	39.00	43.30	81.00	90.00
5	64-QAM	2/3	1	52.00	57.80	108.00	120.00
6	64-QAM	3/4	1	58.50	65.00	121.50	135.00
7	64-QAM	5/6	1	65.00	72.20	135.00	150.00
8	BPSK	1/2	2	13.00	14.40	27.00	30.00
9	QPSK	1/2	2	26.00	28.90	54.00	60.00
10	QPSK	3/4	2	39.00	43.30	81.00	90.00
…	…	…	…	…	…	…	…
31	64-QAM	5/6	4	260.00	288.90	540.00	600.00

Пристрої стандарту 802.11n можуть використовувати будь-яку ширину каналу 20 або 40 МГц в будь-якому частотному діапазоні (2.4 або 5 ГГц). При використанні ширини каналу 40 МГц відбувається подвоєння пропускної здатності в порівнянні з шириною каналу 20 МГц.

1.3.6 802.11 s

IEEE 802.11 s розроблявся більше для комірчастих мереж, так звані mesh-мережі WMN (Wireless mesh network). Мають властивості самоконфігурування, відновлення і організаційність побудови мережі, надійні та масштабні (рис. 1.6).

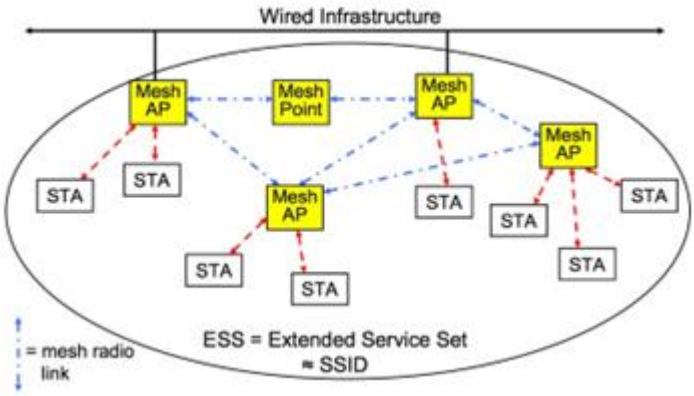

Рисунок 1.6 – Архітектура 802.11 s

WMN гарантує працездатність мережі при виході з ладу певних елементів, розширення покриття мережі, рухому маршрутизацію трафіку, а також ретрансляцію кадрів між пристроями без прямої видимості. Всі нововведення введені тільки на MAC-рівні. Мережа стандарту визначена для невеликих розмірів з максимальною кількістю вузлів до 64.

1.3.7 IEEE 802.11 p

IEEE 802.11p є одним з останніх затверджених поправок до стандарту IEEE 802.11 для додавання бездротового доступу в автомобільних умовах (WAVE). Він доклав деякі покращення в останню версію стандарту 802.11, який потрібно для підтримки додатків інтелектуальних транспортних систем (ITC). Це включає в себе обмін даних між високошвидкісними транспортними засобами, а також між транспортними засобами та придорожньої інфраструктурою в ліцензованому діапазоні. IEEE Система радіочастотної 802.11 p LAN націлена на 5.15-5.25, 5,25- 5,35 ГГц і 5,725-5,825 ГГц U-NII групою.

Система використовує 52 піднесучі, які модулюються з використанням двійкових або квадратурних фазових маніпуляцій (BPSK/QPSK), 16 квадратурно-амплітудної модуляції (16 QAM), або 64-КАМ. Пряме виправлення помилок кодування використовується з швидкістю кодування 1/2, 2/3, 3/4. IEEE 1609 є більш високим стандартом шару на основі IEEE 802.11 p для підтримки

мережевих проблем безпеки в стандарті хвилі. Стандарт IEEE 802.11p працює на 7 каналів, кожен з яких має відповідну смугу частот, як описано на рис. 1.7.

Рисунок 1.7 – Частотний діапазон каналів IEEE 802.11 p

Поправка дозволяє використання 5.9 GHz група (5,850 - 5,925) ГГц з відстанню між рівним 20 МГц, 10 МГц і 5 МГц каналу, які наведено в табл. 1.5, і встановлює вимоги до використання цієї групи в Європі і США.

Таблиця 1.5

Основні параметри IEEE 802.11 p на основі IEEE 802.11 a

Параметр	IEEE 802.11a 20 МГц	IEEE 802.11p 20 МГц	IEEE 802.11p 10 МГц	IEEE 802.11p 5 МГц
Кількість піднесучих	52	52	52	52
Розміщення піднесучої	312,5 кГц	312,5 кГц	156,25 кГц	78,125 кГц
Тривалість символу	4 мкс	4 мкс	8 мкс	16 мкс
Час охорони	0,8 мкс	0,8 мкс	1,6 мкс	3,2 мкс
ПДВ період	3,2 мкс	3,2 мкс	6,4 мкс	12,8 мкс
Тривалість парамбули	16 мкс	16 мкс	32 мкс	64 мкс
Режими модуляції	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM

Він пропонує обмін даних між транспортними засобами (V2V) і між транспортними засобами та придорожньої інфраструктурою (V2i) в межах 1 км з використанням швидкості передачі 3 Mbps до 27 Mbps і швидкості транспортного засобу до 260 км/год.

1.3.8 802.11 ac

IEEE 802.11 ac – отримав назву Wi-Fi 5. Пристрої з 802.11 ac зазвичай також реалізують стандарт 802.11 n в діапазоні 2.4 ГГц. Переваги даного стандарту:

- робота бездротового трафіку відбувається у діапазоні частот 5 ГГц;
- збільшення швидкості та потужності бездротової мережі передачі даних;
- збільшення ширини каналів;
- збільшення числа просторових потоків;
- використання нової і більш ефективної модуляції сигналу;
- використання технології багатокористувацького MIMO (Multi-User MIMO);
- підтримка технології формування спрямованого сигналу Beamforming.

Використовується даний стандарт тільки в діапазоні 5ГГц, що забезпечує вільний радіоефір та призводить до стабільності та кращої швидкості.

Підтримує, даний стандарт, гігабітні швидкості. Як було заявлено, що максимальна швидкість підключення – 7 Гбіт/с. На ринку, наразі, немає пристроїв, які б підтримували такі швидкості, але на тих що маємо отримували максимум в 1,3 Гбіт/с.

Для отримання такої швидкості було рішення збільшити канал до 80 МГц, та збільшення кількості потоків та підтримка модуляції 256-QAM. Це на відміну від стандарту 802.11 n збільшення каналу вдвічі, що призвело до поліпшення та збільшення пропускної здатності.

Також було покращено технологію MIMO, де в стандарті 802.11n тільки один пристрій міг отримувати та відправляти інформацію, коли інші були в черзі. В стандарті 802.11 ac ситуацію було покращено, та реалізовано технологію MU-MIMO, котра створює багатоканальний канал передачі.

Опціонально було реалізовано можливість підтримки технології формування спрямованого сигналу Beamforming, тобто була вирішена проблема пониження потужності сигналу, викликана відбиттям сигналу від стін та перешкод.

Застосування в стандарті 802.11 ac нової і більш продуктивної системи модуляції сигналу 256-QAM забезпечує приріст пропускної здатності.

Модуляція 256-QAM в порівнянні з 64-QAM (в стандарті 802.11 n) збільшив швидкість передачі даних приблизно на 25 %.

Знаючи ширину каналу, кількість просторових потоків і тип модуляції, можна взнати максимально можливу теоретичну швидкість передачі даних.

Нижче приведена табл.1.6 швидкостей передачі даних стандарту 802.11 ac.

Таблиця 1.6

Швидкості передачі даних стандарту 802.11 ac

MCS index	Spatial Streams	Modulation type	Coding rate	Data rate (in Mbit/s)							
				20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
				800 ns	400 ns	800 ns	400 ns	800 ns	400 ns	800 ns	400 ns
0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	1	64-QAM	2/3	52	57.8	108	120	234	260	468	520
6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780
9	1	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7
0	2	BPSK	1/2	13	14.4	27	30	58.5	65	117	130
1	2	QPSK	1/2	26	28.9	54	60	117	130	234	260
2	2	QPSK	3/4	39	57.8	108	90	175.5	195	351	390

3	2	16-QAM	1/2	52	57.8	108	120	234	260	468	520
4	2	16-QAM	3/4	78	86.7	162	180	351	390	702	780
5	2	64-QAM	2/3	104	115.6	216	240	468	520	936	1040
6	2	64-QAM	3/4	117	130.3	243	270	526.5	585	1053	1170
7	2	64-QAM	5/6	130	144.4	270	300	585	650	1170	1300
8	2	256-QAM	3/4	156	173.3	324	360	702	780	1404	1560
9	2	256-QAM	5/6	N/A	N/A	360	400	780	866.7	1560	1733.4
0	3	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195
1	3	QPSK	1/2	39	43.3	81	90	175.5	195	351	390
2	3	QPSK	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
3	3	16-QAM	1/2	78	86.7	162	180	351	390	702	780
4	3	16-QAM	3/4	117	130	243	270	526.5	585	1053	1170
5	3	64-QAM	2/3	156	173.3	324	360	702	780	1404	1560
6	3	64-QAM	3/4	175.5	195	364.5	405	N/A	N/A	1579.5	1755
7	3	64-QAM	5/6	195	216.7	405	450	877.5	975	1755	1950
8	3	256-QAM	3/4	234	260	486	540	1053	1170	2106	2340
9	3	256-QAM	5/6	260	288.9	540	600	1170	1300	2340	2600
0	4	BPSK	1/2	26	28.8	54	60	117.2	130	234	260
1	4	QPSK	1/2	52	57.6	108	120	234	260	468	520
2	4	QPSK	3/4	78	86.8	162	180	351.2	390	702	780
3	4	16-QAM	1/2	104	115.6	216	240	468	520	936	1040
4	4	16-QAM	3/4	156	173.2	324	360	702	780	1404	1560
5	4	64-QAM	2/3	208	231.2	432	480	936	1040	1872	2080
6	4	64-QAM	3/4	234	260	486	540	1053.2	1170	2106	2340
7	4	64-QAM	5/6	260	288.8	540	600	1170	1300	2340	2600
8	4	256-QAM	3/4	312	346.8	648	720	1404	1560	2808	3120
9	4	256-QAM	5/6	N/A	N/A	720	800	1560	1733.2	3120	3466.8

Було зменшено споживання енергії при передачі даних за рахунок нових чіпів.

1.4 Фізичний рівень (Physycal layer) та MAC-рівень стандарту IEEE 802.11

Фізичний рівень стандарту IEEE 802.11 використовує пакетні передачі чи пакети. Кожен з цих пакетів складається з парамбули, заголовку і даними корисного навантаження (рис. 1.8).

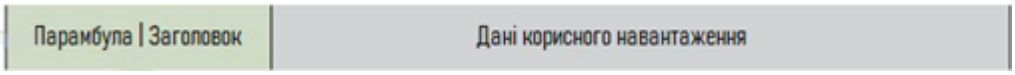

Рисунок 1.8 – Структура пакету фізичного рівня

Парамбула дозволяє приймачу отримати синхронізації часу і частоти і оцінити характеристики каналу для вирівнювання. Заголовок надає інформацію про конфігурацію пакета, таку як формат, швидкість передачі даних і т.ін.

На фізичному рівні стандарт 802.11 охоплює дві альтернативи DSSS і FHSS. Обидва різновиди передачі по радіо з використанням розширення спектра методом прямої послідовності (DS) і методом частотних стрибків (FH) використовують частотний діапазон 2,400 -2,4835 ГГц . Смуга пропускання 2,4 ГГц була обрана тому, що в усьому світі цей діапазон виділений для неліцензованого використання, а також в даному діапазоні можливе створення і виробництво приймально-передавального радіообладнання, що володіє низькою вартістю, невеликим випромінюванням потужності і праці на швидкостях, близьких до швидкостей в звичайних дротових Ethernet мережах.

Рівень MAC відповідає за розподіл каналу, тобто обирає станцію яка буде передавати інформацію наступною. На MAC рівні обрано принцип, що визначає як пристрій буде ділити загальний канал, механізм шифрування і автентифікації даних. Оскільки стандарт 802.11 розроблявся як «бездротовий Ethernet», він передбачає пакетну передачу з 48-бітовими адресами пакетів, як і будь-яка

мережа Ethernet. Рівень MAC отримує блок даних від рівня LLC і відповідає за виконання функцій, пов'язаних з доступом до середовища, і за передачу даних.

Стандарт IEEE 802.11 передбачає два режими управління мережами: PCF і DCF (розділяється ще на два підтипи).

2 ІСНУЮЧІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ

2.1 Способи взлому та вразливості Wi-Fi мереж

З кожною новою введеною технологією з’являються люди які бажають використовувати потенціал технології по призначенню, але бувають користувачі які намагаються наражати на небезпеку дані інших користувачів. Іншими словами в мережах бувають звичайні користувачі і зловмисники, проти яких і застосовуються методи забезпечення безпеки. Методи забезпечення безпеки використовуються для захисту від загроз порушення інформаційної безпеки, ці загрози умовно можна розділити на два класи:

1. Прямі – загрози інформаційної безпеки, які виникають при інформаційному обміні через безпровідну мережу Wi-Fi;

2. Непрямі - загрози, пов'язані з великою кількістю точок доступу Wi-FI.

Радіоканал в межах доступності Wi-FI роутера, схильний до легкого втручання з метою отримання несанкціонованого доступу до ресурсів та інформації. У стандартах IEEE 802.11, що регламентують роботу Wi-Fi, передбачені, як автентифікація, так і шифрування, але дані елементи захисту мають свої вади і слабкі місця. На даний час відомі такі прямі атаки.

Чужинці – це периферійні пристрої і комп'ютери, що надають можливість несанкціонованого доступу до корпоративної мережі, зазвичай в обхід захисних механізмів, визначених політикою безпеки. У ролі пристрою чужака може виступати все що завгодно, у чого є дротової і бездротової інтерфейси: роутери (включаючи програмні), проектори, сканери, ноутбуки з обома включеними інтерфейсами.

Нефіксована природа зв'язку – безпровідні Wi-Fi пристрої можуть легко змінювати точки підключення до мережі прямо в процесі роботи і навіть непомітно для користувача. Зловмисник може перемикати на свою підставну точку доступу користувача для подальшого сканування вразливостей, фішингу або атак KRACK. А якщо для користувача пристрій при цьому підключено і до

дротової локальної мережі, то він стає точкою входу, так званим чужаком.

Уразливості мереж і пристроїв – некоректно налаштовані мережеві пристрої, пристрої зі слабкими і недостатньо довгими ключами шифрування, які використовують скомпрометовані методи автентифікації – саме ці пристрої піддаються атакам в першу чергу.

Некоректно сконфігуровані точки доступу – варто підключити некоректно сконфігуровані точку доступу до мережі для злому останньої. Заводські настройки, так звані «за замовчуванням», зазвичай не включають шифрування і автентифікацію, або використовують ключі, прописані в інструкціях користувача, і тому вони є всім відомими навіть на офіційних форумах виробника.

Некоректно сконфігуровані бездротові клієнти – загроза куди небезпечніше, ніж некоректне налаштування точки доступу. Це клієнтські пристрої, і вони зазвичай не конфігуруються спеціально для безпеки внутрішньої мережі підприємства. До того ж зазвичай вони знаходяться за межами периметра контрольованої зони або всередині периметра, що може дозволити зловмиснику проводити всілякі атаки, наприклад, поширювати вірусне програмне забезпечення або просто забезпечити легкодоступну і зручну точку входу.

Імперсонації і крадіжка особистих даних – імперсонації (видача себе за іншу людину) авторизованого користувача - серйозна загроза для будь-якої комп'ютерної мережі, це стосується не тільки бездротової.

Відмови в обслуговуванні – DoS атаки спрямовані на порушення якості функціонування сервісу бездротової мережі або на абсолютне припинення доступу користувачів і відмова обладнання до перезавантаження. У разі Wi-Fi мережі відстежити джерело, котрий завалює мережу, специфічним для цього типу атаки, «сміттєвими» пакетами, дуже складно - його місце розташування обмежується тільки зоною покриття. До того ж є апаратний варіант цієї атаки - установка досить сильного джерела перешкод в частотному діапазоні працює точки доступу, так звані "глушилки".

Очевидно, що ці загрози не були виявлені одразу після введення нового протоколу захисту. Їх наявність ставала явною тільки після деякого часу, протягом якого система працювала. На теперішній час, можна з впевненістю стверджувати, що на кожну з цих загроз є захист, але на момент впровадження нових протоколів було зовсім навпаки. Це була нова технологія, і ніхто не міг подумати, що вона може бути вразливою до якихось «Атак». Однак з часом люди зрозуміли, що захист безпровідних мереж потрібно розвивати теж, адже за цим майбутнє.

2.2 Протоколи захисту безпровідних мереж

Існує безліч технологій безпеки, і всі вони пропонують рішення для найважливіших компонентів політики в області захисту даних: автентифікації, підтримки цілісності даних і активної перевірки. Ми визначаємо автентифікацію як автентифікацію користувача або кінцевого пристрою і його місця розташування з подальшою авторизацією користувачів і кінцевих пристроїв. Цілісність даних включає такі області, як безпека мережевої інфраструктури, безпеку периметра і конфіденційність даних. Активна перевірка допомагає впевнитися в тому, що встановлена політика в області безпеки витримується на практиці, і відстежити всі аномальні випадки і спроби несанкціонованого доступу.

2.2.1 WEP

В той самий час, коли було представлено базовий стандарт IEEE 802.11, в IEEE також був затверджений механізм захисту Wired Equivalent Privacy (WEP). WEP (Wired Equivalent Privacy) – технологія стандарту 802.11, яка забезпечувала безпеку передачі інформації. Шифрування даних здійснювалося з використанням алгоритму RC4 на ключі зі статичною складовою від 40 до 104 біт і з додатковим вектором ініціювання розміром 24 біт. Тобто в сумі шифрування даних проводилося на ключі розміром від 64 до 128 біт. У WEP не було мети повністю

захистити інформацію від зловмисників, а просто зробити її недоступною для читання. Основним завданням цієї технології було шифрування потоку даних, що передавались в межах безпровідної мережі.

Для посилення захисту застосовується так званий вектор ініціалізації Initialization Vector (IV), який призначений для рандомізації додаткової частини ключа, що забезпечує різні варіації шифру для різних пакетів даних. Даний вектор є 24-бітовим. Таким чином, в результаті ми отримуємо загальне шифрування з розрядністю від 64 (40 + 24) до 128 (104 + 24) біт.

Зламати подібний захист можна за допомогою утиліти (наприклад, AirSnort, WEP crack). Основне її слабке місце - це як раз-таки вектор ініціалізації. Оскільки ми говоримо про 24 біти, це має на увазі близько 16 мільйонів комбінацій (2 в 24 ступені) - після використання цієї кількості ключ починає повторюватися. Хакеру необхідно знайти ці повтори (від 15 хвилин до години для ключа 40 біт) і за секунди зламати решту ключа. Після цього він може входити в мережу як звичайний зареєстрований користувач.

Процес шифрування WEP виконується в два етапи:

1. Спочатку підраховується контрольна сума (Integrity Checksum Value – ICV) із застосуванням алгоритму Cyclic Redundancy Check (CRC-32), що додається в кінець незашифрованого повідомлення і служить для перевірки його цілісності прийнятої стороною;

2. На другому етапі здійснюється безпосередньо шифрування.

Ключ для WEP-шифрування – загальний секретний ключ, який повинні знати пристрої на обох сторонах бездротового каналу передачі даних. Цей секретний 40-бітний ключ разом з випадковим 24-бітовим IV є вхідний послідовністю для генератора псевдовипадкових чисел, що базується на шифрі Вернама для генерації рядка випадкових символів, званої ключовим потоком (key stream). Дана операція виконується з метою уникнення методів злому, заснованих на статистичних властивостях відкритого тексту. IV використовується, щоб забезпечити для кожного повідомлення свій унікальний ключовий потік.

Зашифроване повідомлення (рис. 2.1) утворюється в результаті виконання операції XOR над незашифрованим повідомленням з ICV і ключовим потоком.

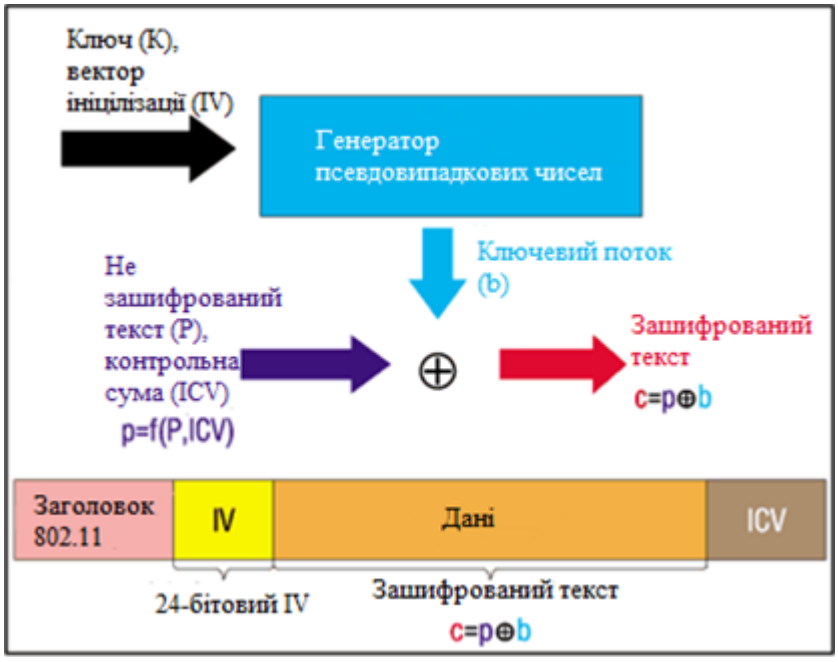

Рисунок 2.1 – Схема роботи шифрування по протоколу WEP

Коли інформація приймається на іншій стороні, проводиться зворотний процес (p = c + b). Значення b одержувач обчислює, застосувавши код Вернама до вхідної послідовності, що складається з ключа K (який він знає заздалегідь) і IV, який прийшов цим же повідомленням у відкритому вигляді. Для кожного чергового пакета процес повторюється з новим обраним значенням IV. До числа відомих властивостей алгоритму RC4 відноситься те, що при використанні одного і того ж значення ключа і вектори ініціалізації ми завжди будемо отримувати однакове значення b, отже, застосування операції XOR до двох текстів, зашифрованим RC4 за допомогою того ж значення b, являє собою не що інше, як операцію XOR до двох початковим текстам.

$$c_1 = p_1 + b; \qquad c_2 = p_2 + b;$$

$$c_1 + c_2 = (p_1 + b) + (p_2 + b) = p_1 + p_2.$$

Таким чином, ми можемо отримати незашифрований текст, який є результатом операції XOR між двома іншими оригінальними текстами.

Процедура їх вилучення не складає великих труднощів. Наявність оригінального тексту і IV дозволяє обчислити ключ, що в подальшому дасть можливість читати всі повідомлення даної бездротової мережі. Після нескладного аналізу можна легко розрахувати, коли повториться b. Так як ключ K постійний, а кількість варіантів IV складає 224 = 16 777 216, то при достатній завантаженні точки доступу, середній розмір пакета в бездротової мережі, що дорівнює 1500 байт (12 000 біт), і середньої швидкості передачі даних, наприклад 5 Mbps (при максимальній 11 Mbps), ми отримаємо, що точкою доступу буде передаватися 416 повідомлень в секунду, або ж саме 1 497 600 повідомлень на годину, тобто повторення відбудеться через 11 год 12 хв (224/1 497 600 = 11,2 год). Дана проблема носить назву "колізія векторів". Існує велика кількість способів, що дозволяють прискорити цей процес. Крім того, можуть застосовуватися атаки "з відомим простим текстом", коли одному з користувачів мережі надсилається повідомлення із заздалегідь відомим змістом і прослуховується зашифрований трафік. В цьому випадку, маючи три складові з чотирьох (незашифрований текст, вектор ініціалізації і зашифрований текст), можна обчислити ключ.

З ICV, використовуваним в WEP-алгоритмі, справи йдуть аналогічно. Значення CRC-32 підраховується на основі поля даних повідомлення. Це хороший метод для визначення помилок, що виникають при передачі інформації, але він не забезпечує цілісність даних, тобто не гарантує, що вони не були підмінені в процесі передачі. Контрольна сума CRC-32 має лінійне властивість: CRC (A XOR B) = CRC (A) XOR CRC (B), що надає зловмиснику можливість легко модифікувати зашифрований пакет без знання WEP-ключа і перерахувати для нього нове значення ICV.

WEP інкапсуляція.

Ключ WEP і вектор ініціалізації об'єднуються для створення початкового числа WEP, яке подається в PRNG ARC4 для створення потоку ключів. Процес створення для двох довжин описано нижче:

- WEP-64 - біти 0–39 ключа WEP відповідають бітам 24–63 WEP, а біти

0–23 IV відповідають бітам 0–23;

- WEP-128 - біти 0–103 ключа WEP відповідають бітам 24–127 WEP, а біти 0–23 від IV відповідають бітам 0–23;

ICV (цінність перевірки цілісності) обчислюється на даних простого тексту та додається до даних прямого тексту перед шифруванням.

Інкапсуляція (рис .2.2) даних проходить наступним чином:

1. Контрольна сума від поля «дані» обчислюється за алгоритмом CRC32 і додається в кінець кадру;

2. Дані з контрольною сумою шифруються алгоритмом RC4, які використовують в якості ключа криптоалгоритму;

3. Проводиться операція XOR над вихідним текстом і шифротекстом;

4. На початок кадру додається вектор ініціалізації і ідентифікатор ключа.

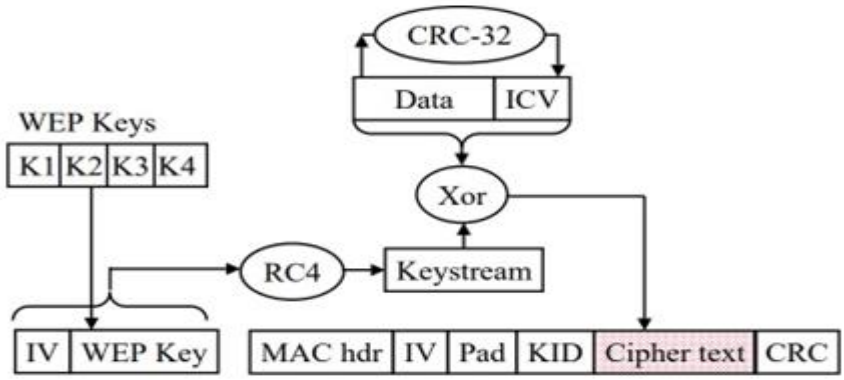

Рисунок 2.2 – WEP інкапсуляція

WEP декапсуляція.

WEP дотримується наведеної нижче процедури для декапсуляції (рис. 2.3) отриманого зашифрованого кадру 802.11 WEP:

- WEP витягує вектор ініціалізації (IV) та ідентифікатор ключа з отриманого пакету для отримання відповідного ключа WEP. Якщо використовуються ключі зіставлення клавіш, то буде використовуватись ключ

зіставлення клавіш, а ідентифікатор ключа ігнорується;

- Система розшифрування WEP створює потік ключів і застосовує потік ключів на зашифрованому пакеті для отримання простого тексту MPDU;

- ICV перераховується та порівнюється з ICV, з'єднаним у MPDU. Якщо невідповідність ICV – кадр опускається, а верхньому шару надається вказівка як помилка дешифрування.

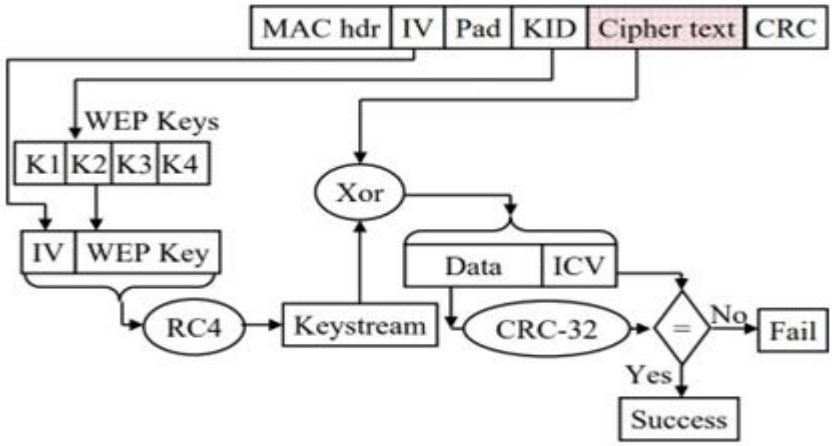

Рисунок 2.3 – WEP декапсуляція

Проблеми в шифруванні WEP.

У проводовій мережі - через те, що станції підключаються за допомогою кабелів, дані досить безпечні самі по собі. Однак, коли середовище передачі є повітряним, усі передачі даних чуються кожною станцією в мережі. Дані також можуть обнюхуватися хакерськими станціями, які можуть спробувати і розшифрувати пакети.

WEP був розроблений, щоб забезпечити безпеку, еквівалентну дротовій мережі. Однак, WEP не вдалося забезпечити те саме, що реалізація безпеки WEP була серйозно хибною. Проблеми алгоритму WEP носять комплексний характер і криються в цілій серії слабких місць:

- механізм обміну ключами (а точніше, практично повну його відсутність);

- малих розрядних ключа і вектори ініціалізації;

- механізм перевірки цілісності переданих даних;

Вирішення проблем.

Проблеми WEP були усунені в ключі шифрування TKIP через збільшення довжини IV до 48 біт. Крім того, якщо поле IV номера вичерпано, новий ключ TKIP потрібно обміняти з Точкою доступу. Виснаження IV довжини зайняло б дуже велику кількість часу – завдяки 48-бітовій довжині та іншим параметрам (наприклад, тайм-аут клавіші PTK) потраплятиме до вичерпання IV довжини.

Перший стандарт шифрування Wired Equivalent Privacy був дискредитований знаходженням вразливостей в алгоритмірозподілу ключів RC4. Це трохи загальмувало розвиток ринку бездротових Wi-Fi мереж і викликало створення Інститут інженерів з електротехніки та електроніки (IEEE) групи 802.11i для розробки нового стандарту безпеки, що враховує відомі уразливості WEP, що забезпечує 128-бітове шифрування AES і автентифікацію для захисту переданих даних.

2.2.2 WPA

WPA означає бездротовий захищений доступ. Стандарт WPA був введений Альянсом Wi-Fi. Стандарт WPA запровадив TKIP як просування на WEP для забезпечення кращої безпеки. WPA також представила автентифікацію користувача верхнього рівня для пристроїв 802.11. Описано два способи автентифікації користувача:

1. Попередній ключ (рукостискання EAPOL);

2. 802.1 X рукостискання верхнього шару EAP/EAPOL для автентифікації користувача.

Обидва вищевказані механізми автентифікації (рис. 2.4) включають автентифікацію користувача, а також генерують набір ключів шифрування, які можуть бути використані для захисту даних. Асоціація WLAN та механізм автентифікації можуть бути розбиті на три фази:

1. Станція WLAN та точка доступу асоціюються одна з одною та визначають, чи використовується механізм автентифікації за допомогою

загальнодоступного ключа/802.1X;

2. Обраний механізм автентифікації створює "головний ключ" в кінці фази 2;

3. Головний ключ використовується в чотирьох сторонньому рукостисканні EAPOL, отриманому тимчасовими ключами для шифрування даних в кінці фази 3.

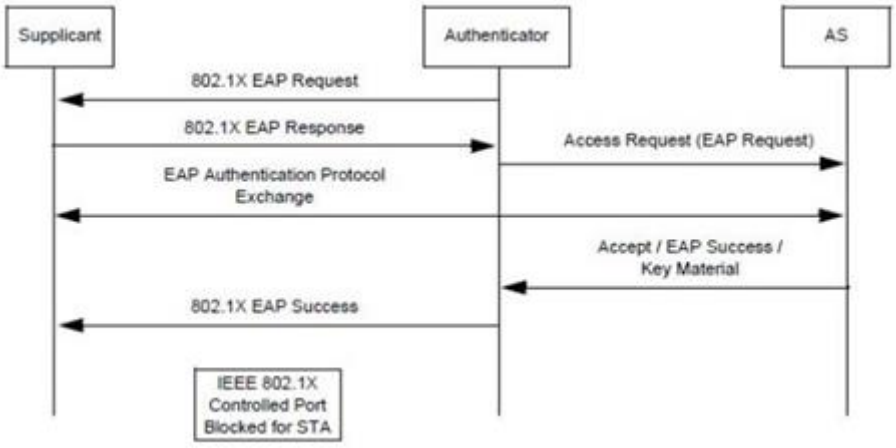

Рисунок 2.4 – Автентифікація EAP, яка забезпечує парний головний ключ для рукостискання EAPOL

Стандарт Wi-Fi/802.11 представив два нові інформаційні елементи для забезпечення нової схеми шифрування WPA (рис. 2.5):

- інформаційні елементи WPA (захищений бездротовий доступ);

- RSN (надійна мережа безпеки).

Будь-яка станція, що містить інформаційний елемент WPA/RSN у своєму запиті на асоціацію, повинна виконати рукостискання безпеки 802.11i/802.1X.

Рисунок 2.5 – Інформаційний елемент WPA

Ідентифікатор елемента WPA встановлений на 0x221. WPA є таким самим, як ідентифікатор елемента для постачальника. Отже, кожного разу, коли буде отримано специфічний для постачальника ідентифікатор елемента – OUI (табл. 2.1) потрібно перевірити AP/Station, щоб побачити, чи є інформаційний елемент WPA. Якщо це не WPA, то AP/Station може вирішити ігнорувати аналіз інформаційного елемента.

Таблиця 2.1

Деякі з різних списків шифрів, які підтримуються

OUI	Тип люкс	Значення
00-50-f2	0	Використовуйте груповий шифр-люкс
00-50-f2	1	WEP-40
00-50-f2	2	TKIP
00-50-f2	3	Зарезервований
00-50-f2	4	Зарезервований
00-50-f2	5	WEP-104

2.2.3 TKIP

TKIP – це набір шифрів за замовчуванням у WPA. WEP-40 і WEP-104 можна використовувати лише як групові шифрові пакети в мережі станції перехідних станцій (TSN).

Інформаційний елемент RSN був виведений групою IEEE 802.11i. RSN позначає надійну мережу безпеки, і вона зробила шифр AES обов'язковим при використанні надійної мережі безпеки.

Шифр TKIP може використовуватися як широкосмуговий / широкомовний шифр, а також WEP-40 / WEP104, але якщо метод автентифікації 802.1X, то WEP-40/WEP-104/TKIP також не дозволено використовувати як груповий шифр.

TKIP як парний шифр з WEP-40/WEP104 як груповий шифр також не підтримується інформаційний елемент RSN (рис. 2.6). Розмір IE RSN обмежений максимум 255 байтами.

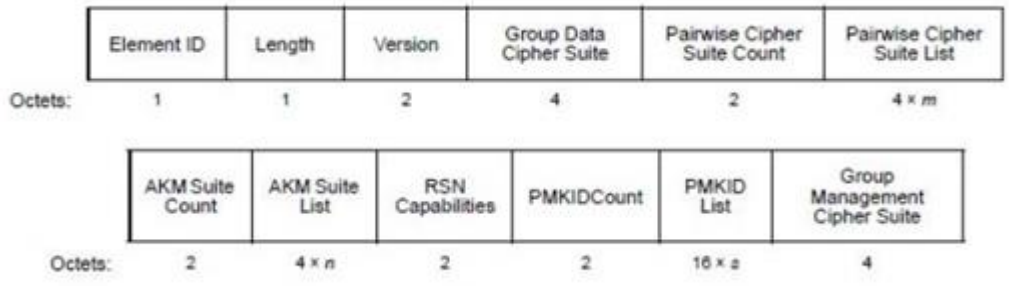

Рисунок 2.6 – RSN формат

Механізм шифрування TKIP.

Протокол шифрування TKIP був введений для виправлення помилок, виявлених при шифруванні WEP, до моменту, коли був розроблений більш безпечний механізм шифрування (AES). Отже, мережі, що підтримують TKIP, стали Стаціонарною мережею переходу. Алгоритм TKIP застосував модифікації до існуючого алгоритму WEP для вирішення вразливостей WEP і тим самим вирішив існуючі на той час проблеми.

Схема шифрування TKIP не вимагала додаткових вимог до апаратного забезпечення та могла бути реалізована над обладнанням WEP. Отже, схема шифрування TKIP широко застосовувалася протягом певного періоду часу до появи надійних мереж безпеки.

TKIP використовує той самий формат, що і формат кадру WEP Encryption з додатковим полем розширеної вектору ініціалізації (IV) (4 байти) та полем MIC (8 байт).(рис. 2.7).

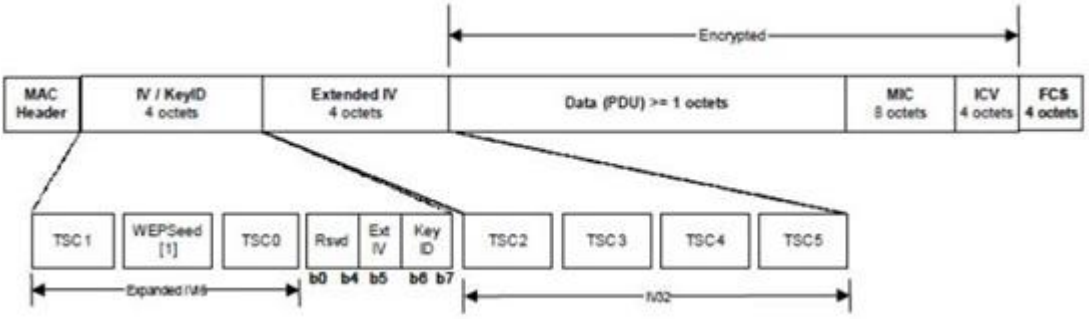

Рисунок 2.7 – Формат TKIP шифрування

TSC0- TSC5 – лічильник послідовностей TKIP (довжина 6 байтів) - TSC0 і TSC1 утворюють IV послідовний номер для змішування TKIP фази 2 та TSC2-TSC5 використовуються в хешуванні ключа фази 1.

Біт Ext IV включений, щоб вказати, чи є Extended IV чи ні. Для TKIP цей біт завжди встановлюється на 1.

Key ID – Ключовий індекс.

WEPSeed – встановлено на (TSC1 | 0x20) & 0x7f.

MIC – перевірка цілісності Майкла.

Лічильник послідовності TKIP використовується для запобігання атакам відтворення. Якщо TSC вичерпується до нуля, ключ TKIP потрібно оновити.

TKIP інкапсуляція.

Процес інкапсуляції TKIP показаний на рис. 2.8.

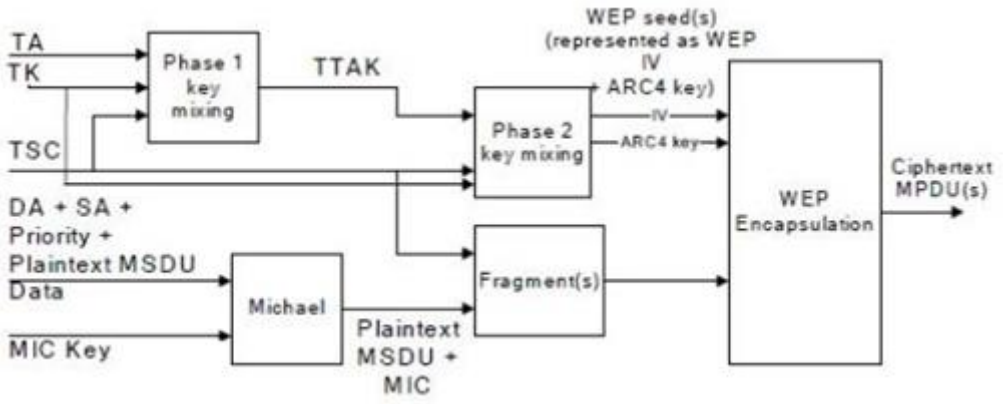

Рисунок 2.8 – Процес інкапсуляції TKIP

Обчислення TKIP MIC захищає поля даних MSDU та відповідні поля SA, DA та пріоритет. Обчислення MIC виконується на впорядкованому конкатенації полів даних SA, DA, Priority та MSDU. MIC додається до поля даних MSDU. TKIP відкидає будь-які прокладки MIC перед додаванням MIC.

При необхідності IEEE Std 802.11 фрагментує MSDU з MIC на один або кілька MPDU. TKIP присвоює монотонно зростаюче значення TSC кожному MPDU, дбаючи про те, щоб усі MPDU, створені з одного і того ж MSDU, мали однакове значення розширеного IV.

Для кожного MPDU TKIP використовує функцію змішування ключів для обчислення насіння WEP.

TKIP представляє насіння WEP як ключ WEP IV і ARC4 і передає їх разом із кожним MPDU в WEP для генерації ICV та для шифрування MPDU простого тексту, включаючи весь або частину MIC, якщо він присутній. WEP використовує насіння WEP як ключ за замовчуванням WEP, ідентифікований ідентифікатором ключа, асоційованим з тимчасовим ключем.

Декапсуляція TKIP (рис. 2.9).

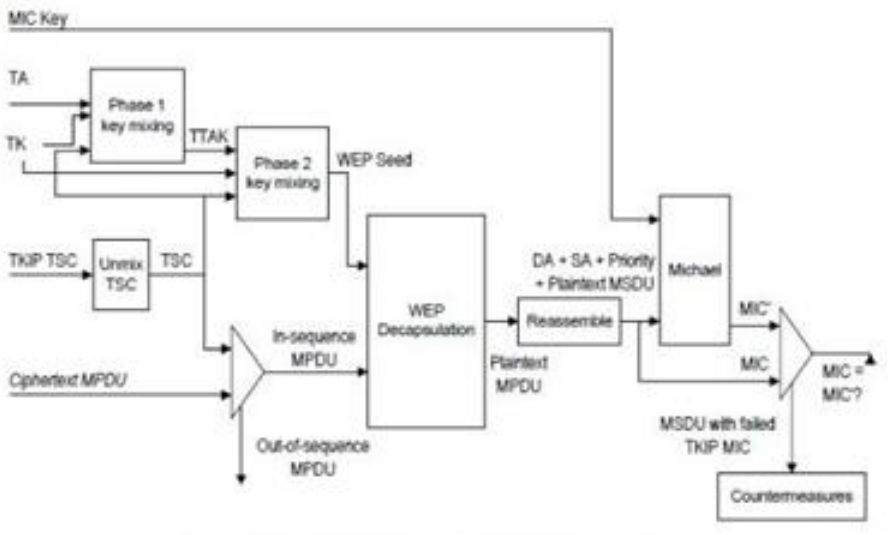

Рисунок 2.9 – Процес декапсуляції TKIP

Перед тим, як WEP декапсулює отриманий MPDU, TKIP витягує номер послідовності TSC та ідентифікатор ключа з WEP IV та розширеного IV. TKIP

відкидає отриманий MPDU, який порушує правила послідовності (тобто кадр, лічильник послідовностей TKIP не монотонно збільшує більш високе значення.

TKIP представляє насіння WEP як ключ WEP IV та ARC4 і передає їх разом з MPDU на декапсуляцію WEP.

Якщо WEP вказує, що перевірка ICV вдалася, реалізація повторно збирає MPDU в MSDU. Якщо дефрагментація MSDU проходить успішно, приймач перевіряє MIC TKIP. Якщо дефрагментація MSDU виходить з ладу, MSDU відкидається.

Крок підтвердження MIC повторно обчислює MIC над полями даних MSDU SA, DA, Priority та MSDU (але не поле MK TKIP). Потім обчислений результат TIC MIC порівнюється побіжно з отриманим MIC.

Якщо отримані та локально обчислені значення MIC однакові, перевірка проходить успішно, і TKIP доставляє MSDU до верхнього шару.

Якщо дві різняться, то перевірка не вдається; одержувач повинен відмовитися від MSDU та вжити відповідних заходів протидії.

TKIP використовує MIC (Michael Integrity Check) у надісланому пакеті, щоб перевірити, чи передається пакет справжньою WLAN-станцією, пов'язаною з мережею. Ми розберемося з потребою у TKIP MIC та форматі кадру та обчисленнях.

MIC TKIP запобігає нападам підробки. MIC – це 64-бітове (8 байт) значення. MIC сам по собі слабкий, а отже, шифрується та надсилається разом із MSDU. Оскільки ICV (Integrity Check Value) обчислюється на MPDU у шарі MAC, перевірка Цілісності забезпечує захист верхнього рівня для різних типів атак, які пройшли перевірку ICV.

Перелік атак, від яких MIC здатний захистити, наведено нижче:

- атаки біт-гортання;
- дані (корисне навантаження) усікання, з'єднання та сплайсинг;
- атаки фрагментації;
- ітеративні напади на відгадування проти ключа;

- перенаправлення шляхом зміни поля MPDU DA або RA;

- атаки видавання себе за допомогою модифікації поля MPDU SA або TA.

MIC (рис. 2.10) ускладнює успіх будь-якої з цих атак. MIC обчислюється за адресою призначення (DA), адресою джерела (SA), пріоритетом MSDU, трьома зарезервованими байтами та самою MSDU.

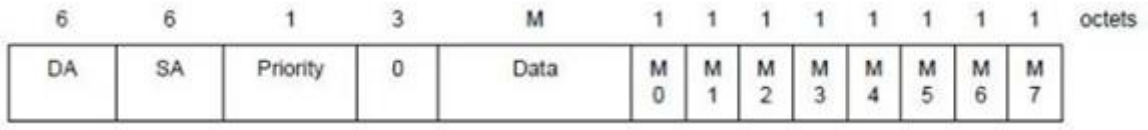

Рисунок 2.10 – Структура MIC

Він додається до MSDU в кінці MSDU і весь MSDU + MIC шифрується. Це дозволяє виявляти атаки шару MAC. Наведена нижче схема ілюструює вище сказане (рис. 2.11).

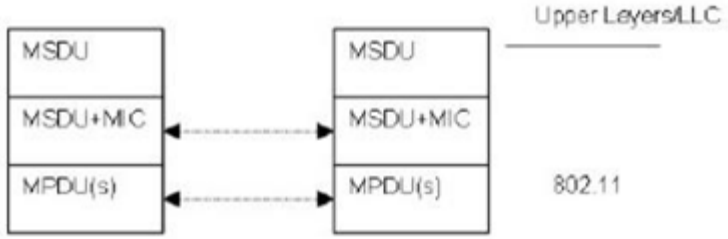

Рисунок 2.11 – Додавання до MSDU частини MIC

MSDU з приєднаним MIC може бути розділеним та надісланим у вигляді декількох MPDU. MIC сам не може забезпечити повний захист від підробок, тому TKIP також включає захист від повторного відтворення.

Захист від відтворення TKIP.

TKIP забезпечує 48-бітовий (6 байт) монотонно збільшуючи лічильник передачі послідовностей (TSC), який він додає до кожного пакету. Якщо приймається який-небудь пакет TKIP, у якому значення TSC менше або дорівнює поточному значенню лічильника відтворення - кадр мовчки відкидається.

Стандарт 802.11 визначає набір правил захисту від відтворення TKIP і надається (від стандарту) нижче:

1. Кожен MPDU повинен мати унікальне значення TKIP TSC;

2. Кожен передавач повинен підтримувати один TSC (48-бітний лічильник) для кожного PTKSA, GTKSA та STKSA;

3. TSC повинен бути реалізований як 48-бітний монотонно зростаючий лічильник, ініційований до 1, коли відповідний тимчасовий ключ TKIP ініціюється або оновляється;

4. Формат WEP IV містить 16 LSB 48-розрядних TSC, як визначено функцією змішування TKIP (Фаза 2, STEP3). Залишок TSC переноситься в розширене IV поле;

5. Одержувач повинен підтримувати окремий набір лічильників відтворення TKIP TSC для кожного PTKSA, GTKSA та STKSA;

6. Виявлення відтворення TKIP відбувається після перевірки MIC та будь-якого перевпорядкування, необхідного при обробці ACK. Таким чином, одержувач затримує просування лічильника відтворення TKIP TSC до тих пір, поки MSDU не пройде перевірку MIC, щоб запобігти зловмисникам вводити MPDU з дійсними ICV і TSC, але недійсними MIC;

7. Для кожного PTKSA, GTKSA та STKSA приймач повинен підтримувати окремий лічильник відтворення для кожного пріоритету кадру та використовувати TSC, відновлений з отриманого кадру, для виявлення відтворених кадрів. Повторний кадр виникає, коли TSC, вилучений з отриманого кадру, менший або рівний поточному лічильнику відтворення для пріоритету кадру. Передавач не повинен упорядковувати кадри з різними пріоритетами, не гарантуючи, що приймач підтримує необхідну кількіст лічильників повтору.

3 ЗАХИСТ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ WPA2 ENTERPRISE

Різниця між WPA2 Personal і WPA2 Enterprise (табл. 3.1) полягає в тому, звідки беруться ключі шифрування, які використовуються в механізмі алгоритму AES. Для приватних (домашніх, дрібних) застосувань використовується статичний ключ (пароль, кодове слово, PSK (Pre-Shared Key)) мінімальною довжиною 8 символів, яке задається в настройках точки доступу, і у всіх клієнтів даної бездротової мережі однаковим.

Таблиця 3.1

Всі можливі параметри безпеки протоколу WPA2 Enterprise

Властивість	WPA 2 (Enterprise)
Ідентифікація	Користувач, комп’ютер
Авторизація	EAP або загальний ключ
Цілісність	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code – CCM) Part of AES
Шифрування	CCMP (AES)
Розподілення ключів	Похідна від PMK
Вектор ініціалізації	48-біт номер пакету (PN)
Довжина ключа, біт	До 256
Інфраструктура	RADIUS

Компрометація такого ключа вимагає негайної зміни пароля у всіх, хто лишився користувачів, що реально тільки в разі невеликого їх числа. Для корпоративних застосувань, як випливає з назви, використовується динамічний ключ, індивідуальний для кожного працюючого клієнта в даний момент. Цей ключ може періодичний оновлюватися по ходу роботи без розриву з'єднання, і за

його генерацію відповідає додатковий компонент – сервер авторизації, і майже завжди це RADIUS-сервер.

Якщо говорити про безпеку персональних даних в персональній мережі і в корпоративній мережі, то перевагу отримає остання, так як ці мережі більш захищенні від зломів та перехоплень даних, що передаються. Але не потрібно розслаблятись, адже не кожна мережа надійна. Зловмисник, з метою викрадення ваших персональних даних зможе проникнути і в корпоративну мережу. В його арсеналі є не тільки хороший рівень кваліфікації, а й хороший набір спеціалізований інструментів, таких як:

- Wi-Fi адаптери для роботи на різних частотних діапазонах;
- мікрокомп'ютери для створення підробленої точки доступу;
- спрямовані антени;
- обладнання для аналізу мережі;
- різне ПЗ, що дозволяє проводити аналіз безпеки Wi-Fi мереж.

Спочатку зловмисника зацікавить інформація про механізми безпеки, що використовуються в механізмах автентифікації і алгоритмах шифрування корпоративної мережі. Вся зібрана ним інформація в майбутньому буде використана для проведення злому обраної ним мережі. Існує таке поняття як «контрольована зона», де використання Wi-Fi мереж буде безпечним і ця мережа буде доступна тільки для працівників компанії. Якщо «контрольованої зони» не має, то злом корпоративної мережі є можливим. Адже якщо обмеження по потужності сигналу на маршрутизаторах відсутні, то доступ до мережі може здійснюватися з прилеглих до будівлі територій. Багато великих компаній нехтують цим і наражають своїх співробітників і саму компанію на небезпеку.

Зловмисник не буде втрачати таку можливість для проведення різних атак на мережу за межами «контрольованої зони». Так як йому ніхто не заважатиме і він буде не помітним, то він може застосовувати не тільки швидкі атаки, а й довготривалі атаки – підбор ключа безпеки.

Зловмисник для взлому може використовувати різні типи атак, а саме такі:

- підроблена точка доступу;
- перехід з гостьової мережі в корпоративну;
- несанкціоновані точки доступу;
- словарні ключі безпеки;
- використання механізму WPS;
- не захищена автентифікація.

Всі ці атаки призводять до того, що зловмисник так чи інакше проникає в корпоративну мережу і може зловживати персональними даними користувачів, даними самої компанії та іншими ресурсами. Детальніше вплив кожної атаки на мережу і як з цим боротися розглянемо в наступних пунктах.

Всі ґаджети, що працюють в корпоративній мережі коли підключаються до безпровідної мережі автоматично запам’ятовують її назву (SSID мережі). Наші люди ліниві і вони не люблять кожного разу по новому підключатись до мережі, тому користуються небезпечним налаштуванням «Автоматичне підключення до мережі». Хоч ця функція і полегшує життя користувачів, але вона несе за собою деяку потенційну загрозу. Коли пристрій буде в межах доступу до корпоративної мережі, ґаджет автоматично підключиться. Саме в такий момент зловмисник створює підроблену ТД (рис. 3.1), після чого ґаджети співробітників, що знаходяться в зоні підробленої ТД,. будуть відправляти запити на автентифікацію автоматично.

Рисунок 3.1 – Атака із застосуванням підробленої ТД

І якщо в корпоративній мережі використовується протокол PEAPv0/EAP-MsCHAPv2, а в користувача не перевіряється сертифікат ТД, то зловмисник з легкістю може проводити атаку з підробленою ТД. Він акцентується на перехоплення пари «Challende + Response», які застосовуються коли проводиться запит на автентифікацію. Отримані дані можуть слугувати для захоплення хеш пароля методом підбору.

Отримавши значення пари «Challenge + Response», зловмисник буде застосовувати суперкомп'ютер для підбору ключів, що засновані на аглоритмах DES і SHA1, щоб отримати хеш пароля. В результаті в нього це вдасться.

Найбільш небезпечним є те, що користувачі можуть навіть не підозрювати, що їх намагаються зламати, адже зловмисник в цьому випадку зовсім непомітний. Він може розмістити підроблену ТД де завгодно – нижній поверх будівлі, кафе, парковка. Як тільки користувач буде в зоні роботи мережі, зловмисник почне діяти і спробує підключити пристрій зі збереженим раніше значенням SSID.

Найкраще рішення в цій ситуації, це не допускати виходу мережі за територію компанії. Але не завжди є можливість так зробити, тому для таких ситуацій рекомендується застосовувати в корпоративних мережах безпечні методи автентифікації, такі як EAP-TLS з використанням клієнтського сертифіката і перевіркою сертифіката сервера. Цей протокол вимагає встановлення клієнтських сертифікатів на кожен новий сеанс. І якщо зловмисник захоче атакувати з використанням підробленої ТД, то він потерпить невдачу.

WPS (Wi-Fi Protected Setup) – це механізм, який був призначений для спрощення процесу налаштування бездротової мережі. При використанні цього механізму в мережі ім'я і тип шифрування задаються автоматично, а для підключення до ТД застосовується деякий PIN-код. В більшості випадків він складається тільки з цифр і інколи цей код може бути написаний прямо на роутері. В багатьох роутерів цей механізм налаштування активований з самого початку. Тому зловмисник може підібрати PIN-код і отримати доступ до мережі.

Для цього підбору є спеціальне ПО, що допомагає знайти такі точки доступу і проводити на них атаки. Таке ПО є у вільному доступі, тому кожен бажаючий зловмисник може скачати його собі і займатись зломами мереж.

Рішенням даної проблеми є відключення механізму WPS в налаштуваннях точки доступу.

У корпоративних мережах можливі два сценарії установки підробленої ТД (рис. 3.2):

- підроблена ТД функціонує як незалежна від мережі точка;

- підроблена ТД підключається прямо до комутатора/контролера у локальної мережі.

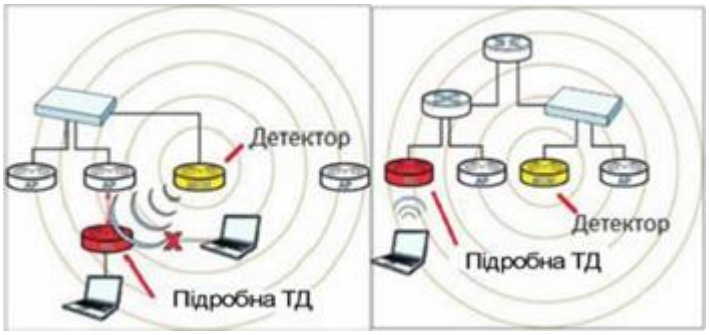

Рисунок 3.2 – Підроблена ТД є незалежною (ліворуч);
підроблена ТД підключена до внутрішньої мережі (праворуч)

На контролері безпровідної мережі налаштовуються списки довірених ТД на основі їх MAC-адрес. Ті адреси, які не входять до цього списку, для безпеки відкидаються. Більш ефективним рішенням є настроювання однієї із ТД у режим моніторингу. ТД сканує радіоефір і шукає підозрілі точки. Якщо ідентифікована ТД не підключена до локальної мережі, то детектор заважає їй працювати, а саме розсилає широкомовні пакети, щоб клієнти не могли підключитися до підробленої ТД (рис. 3.3).

Рисунок 3.3 – Заходи захисту від підроблених ТД,
яка не підключена до провідної мережі

Якщо підключена провідним з'єднанням, то з'являється можливість заблокувати її роботу через порт комутатора (рис. 3.4).

Рисунок 3.4 – Заходи захисту від підроблених ТД,
яка підключена до провідної мережі

На теперішній час найкращими технологіями для захисту безпровідних мереж володіє компанія Cisco. Вона підтримує технологію WIPS (Wireless Intrusion Prevention System), що виявляє підроблені ТД . Діагностування підозрілої ТД проводиться на основі SSID. Процес керування такими точками доступу здійснюється в 3 етапи:

1. Виявлення. Спеціальна ТД переводиться в режим моніторингу й сканує ефір, збираючи такі дані, як SSID, MAC-адреси точки і її клієнтів, IP-адреси. Отримані дані заносяться на контролер.

2. Класифікація. Точки-детектори порівнюють дані про підроблену ТД, отримані по бездротовому каналу, з тими, що отримані по провідному каналу. Якщо MAC-адреса підробленої точки був виявлений у провідній мережі, то така підроблена точка розглядається як критична. Cisco має спеціальний протокол RLDP, який допомагає визначити, чи підключена підроблена ТД до провідної мережі, підключаючись до неї прямо в якості клієнта й посилаючи її дані по протоколу RLDP на CPI.

3. Усунення. Визначається місце розташування ТД та створюються перешкоди. Проходить процес відключення портів цієї ТД.

ВИСНОВКИ

У моїй роботі розглянуто різні види захистів мереж безпровідного доступу на базі стандарту 802.11ac з протоколом безпеки WPA2 Enterprise.

Для досягнення мети були зроблені такі дії.

У першому розділі було розглянуто безпровідні мережі передачі інформації. Визначено, що безпровідна локальна мережа WLAN має найбільший масштаб розгортання, саме тому її було обрано для подальшого розгляду. Детальним аналізом цієї мережі були опрацьовані такі пункти:

- ознайомлено з чотирма топологіями розгортання мережі безпровідного доступу;

- були опрацьовані стандарти мережі Wi-Fi;

- розглянуто основний механізм доступу та рівні мережі;

Завдяки своїй простоті, дешевизни послуг і зручністю користування, безпровідні локальні мережі Wi-Fi мають широке застосування у різноманітних сферах. Завдяки цій технології працюють як і домашні мережі, так і великі корпоративні.

У другому розділі були розглянуті типи атак на мережі безпровідного доступу. Особливу увагу було приділено протоколам безпеки, що протидіють цим вразливостям.

Було виявлено, що протокол WPA3 є найбільш придатним для забезпечення безпеки та надійності персональних даних користувачів мережі. Переваги наведені у висновку до другого розділу. Але протокол ввійде в роботу лише тоді, коли більшість пристроїв будуть підтримувати цей протокол. На жаль цього зараз немає і основним протоколом для захисту мережі є протокол WPA2. Він розділяється на персональний і корпоративний.

У третьому розділі було розглянуто відмінність між протоколом WPA2 та WPA2 Enterprise. Були наведені можливі типи атак на корпоративну мережу, їх розгортання та застосування при зломі. Також після кожної з атак було наведено

рішення, що сприяло б уникненню або виправленню існуючої вразливості.

Також було надано рекомендації для подальшого захисту від атак на корпоративну мережу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Щербаков В.Б. Безопасность беспроводных сетей: стандарт IEEE 802.11. – Москва: РадиоСофт, 2010. – 255 с.

2. Берлин А.Н. Телекоммуникационные сети и устройства [учеб. пособ.]. – М.: Интернет-Университет Информационных Технологий, 2008. – 319 с.

3. Mathy Vanhoef and Frank Piessens. Predicting, decrypting, and abusing WPA2/802.11 group keys / In 25th USENIX Security Symposium, USENIX Security 16, 2016. – 673 p.

4. Олифер В. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2016. – 992 с.

5. Tanenbaum A. Computer Networks. – New Jersey: Pearson, 2012. – 959 p.

6. Колисниченко Д. Беспроводная сеть дома и в офисе. – СПб.: БХВ Петербург, 2009. – 479 с.

7. Mathy Vanhoef and Frank Piessens. Release the kraken: new KRACKs in the 802.11 standard / In Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS). – ACM, 2018. – 210 p.

8. Підпалий О.І. Романов М.О. Використання протоколу WPA2 Enterprise для підвищення захищеності Wi-Fi мережі / V Міжнародна науково-практична конференція "SCIENTIFIC ACHIEVEMENTS OF MODERN SOCIETY". Зб. матер. конф. 8-10 січня 2020 року. – Ліверпуль, 2020. – 803 с.

9. Підпалий О.І. Використання гібридних безплатних мереж доступу на основі технологій Wi-Fi для розвитку ефективності обслуговування / IV Міжнародна науково-практична конференція "SCIENCE, SOCIETY, EDUCATION: TOPICAL ISSUES AND DEVELOPMENT PROSPECTS". Зб. матер. конф. 16-17 березня 2020 року. – Харків, 2020. – 180 с.

10. Підпалий О.І. Аналіз роботи протоколу захисту безпроводових мереж WPA2 / I Міжнародна науково-практична конференція “MODERN SCIENCE: PROBLEMS AND INNOVATIONS”. Зб. матер. конф. 5-7 квітня 2020 року. –

Стокгольм, 2020. – 229 с.

11. Підпалий О.І. Аналіз вразливості бездротової мережі Wi-Fi з новим протоколом захищеності WPA3 / XIV Міжнародна науково-технічна конференція «Перспективи телекомунікацій». Зб. матер. конф. – К.: КПІ ім. Ігоря Сікорського, 2020. – С.98-102.

12. Угрозы для беспроводной корпоративной сети WPA2-Enterprise и способы защиты [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://uni.dtln.ru/digest/ugrozy-dlya-besprovodnoy-korporativnoy-seti-wpa2-enterprise-i-sposoby-zashchity.

13. WPA2-Enterprise. Как создать безопасную сеть? [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://wifi-solutions.ru/zashita-korporativnoy-seti-s-wpa2-enterprise.

14. WPA2-Enterprise, или правильный подход к безопасности Wi-Fi сети. [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://habr.com/ru/post/150179.

15. DSSS – Direct Sequence Spread Spectrum. [Електронний ресурс]. – 2005. – Режим доступу до ресурсу: http://www.telecomabc.com/d/dsss.html.

16. Стандарт локальних мереж IEEE 802.11 Wi-Fi. [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://beloshop.ru/uk/ethernet- standard-ieee-80211-wi-fi.

17. Some WLAN Network Topologies – BSS, IBSS, Mesh BSS and P2P [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://www.hitchhikersguidetolearning.com/2017/09/17/some-wlan-network-topologies-bss-ibss-mesh-bss-and-p2p.

18. Стандарт IEEE 802.11 для широкосмугового безпровідного доступу [Електронний ресурс]. – 2011. – Режим доступу до ресурсу: http://www.ce-studbaza.ru/schriebe.php?id=1040.

19. 802.11 b g n методи перевірки. Способи збільшення швидкості з'єднання бездротової мережі Wi-Fi. [Електронний ресурс]. – 2016 – Режим доступу до ресурсу: https://reactor-web.ru/uk/80211-b-g-n- verification-methods.html.

20. Wireless LAN (WLAN). [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://www.hitchhikersguidetolearning.com/wireless-lan-wlan-articles.

21. Wi-Fi .[Електронний ресурс]. – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Wi-Fi.

22. Wi-Fi сети: проникновение и защита. [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://m.habr.com/ru/post/226431.