

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

«На правах рукопису»
УДК _ 621.396 _

«До захисту допущено»
Завідувач кафедри
_____ Сергій КРАВЧУК
«__» _____ 2021 р.

Магістерська дисертація
на здобуття ступеня магістра
за освітньо-професійною програмою «Інженерія та програмування
інфокомунікацій»
зі спеціальності 172 «Телекомунікації та радіотехніка»
на тему: «Методика розрахунку мережі безпроводового доступу Wi-Fi на
основі протоколу IEEE 802.11ax»

Виконав:
студент II курсу, групи ТЗ-01мп
Підпалій Олександр Іванович _____

Керівник:
професор кафедри ТК
д.т.н., професор Романов О.І. _____

Рецензент:
доцент кафедри ІКТС НН ІТС
к.т.н., доцент Созонник Г.Д. _____

Засвідчую, що у цій магістерській
дисертації немає запозичень з праць
інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Сергій КРАВЧУК

«___» _____ 2021 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Підпалому Олександру Івановичу

1. Тема дисертації «Методика розрахунку мережі безпроводового доступу Wi-Fi на основі протоколу IEEE 802.11ax», науковий керівник професор кафедри ТК, д.т.н, професор Романов Олександр Іванович, затверджені наказом по університету від «04» листопада 2021 р. № 3672-с.

2. Термін подання студентом дисертації 10.12.2021 р.

3. Об'єкт дослідження: протокол роботи Wi-Fi мережі IEEE 802.11ax

4. Предмет дослідження: методи збільшення пропускної здатності мережі, оптимізація процесів.

5. Перелік завдань, які потрібно розробити:

- Обґрунтування актуальності теми. Розглянути основні компоненти мережі Wi-Fi, їх призначення та функції.
- Проаналізувати роботу основних протоколів у мережі Wi-Fi; Детальний аналіз протоколу IEEE 802.11ax;
- Розгляд методик розрахунку мереж бездротового доступу Wi-Fi. Кожна з методик супроводжуватиметься моделюванням в середовищі MATLAB.

6. Орієнтовний перелік ілюстративного матеріалу:

Топологія інфраструктурної мережі.; Спеціальна топологія мережі.; Мережа бездротової локальної мережі; Топологія мережі P2P; Рівні моделі ISO / OSI і їх відповідність стандарту 802.11.; Схема роботи шифрування по протоколу WEP; Автентифікація EAP, яка забезпечує парний головний ключ для рукописання EAPOL; Інформаційний елемент WPA.; RSN – формат; Список протоколів; 802.1X аутентифікація; Підключення до AP за допомогою WPA3.; Повідомлення автентифікації WPA3; Деталі рукописання SAE.; Структура пакету фізичного рівня.; Етапи розробки стандарту IEEE 802.11be.; Зміна інтервалу між несучими OFDM-сигналу у стандарті IEEE 802.11ax; Застарілі формати PPDU та нові формати HE PPDU; OFDM проти OFDMA; Один користувач, який використовує канал із використанням OFDM (а) та мультиплексування різних користувачів в одному каналі з використанням OFDMA (б); Формування діаграми спрямованості точки доступу за допомогою діаграмо утворювальних кадрів для роботи MU-MIMO; Координація розрахованої на багато користувачів операції верхньої лінії зв'язку; Приклад заповнення DL-OFDMA *a = a-фактор; Пілоти IEEE 802.11ax для 26- та 52-тональних RU; Граф поведінки окремих станцій.; Графіки моделювання.

7. Орієнтовний перелік публікацій:

- Міжнародна науково-практична конференція "SCIENTIFIC ACHIEVEMENTS OF MODERN SOCIETY". Збірник матеріалів конференції. 8-10 січня 2020 року – Ліверпуль.
- Міжнародна науково-практична конференція "MODERN SCIENCE: PROBLEMS AND INNOVATIONS". Збірник матеріалів конференції. 5-7 квітня 2020 року – Стокгольм.
- Міжнародна науково-технічна конференція «Перспективи телекомунікацій»; ПТ-2020: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2020.

8. Дата видачі завдання “ 01 ” вересня 2019 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Ознайомлення з основними аспектами обраної сфери телекомунікацій	09.09.2020	виконано
2	Визначення структури магістерської дисертації; вивчення літератури, пошук додаткової літератури, патентний пошук	11.10.2020	виконано
3	Робота над першим розділом магістерської дисертації; проведення наукового дослідження	30.11.2020	виконано

4	Проведення наукового дослідження; робота над другим розділом магістерської дисертації	08.03.2021	виконано
5	Проведення наукового дослідження; робота над третім розділом магістерської дисертації	15.05.2021	виконано
6	Розробка стартап проекту	10.09.2021	виконано
7	Завершення роботи над основною частиною магістерської дисертації; підготовка ілюстративного матеріалу	30.10.2021	виконано
8	Оформлення текстової і графічної частини магістерської дисертації	11.11.2021	виконано
9	Попередній розгляд магістерської дисертації	09.12.2021	виконано

Студент

Науковий керівник дисертації

Підпалий ОЛЕКСАНДР

Олександр РОМАНОВ

РЕФЕРАТ

Робота містить: 98 сторінок, 44 рисунків та 23 таблиці. Було використано 24 джерел.

Актуальність теми. В теперішньому світі пристрої бездротової технології набирають швидкої популярності. Неминучим є те, що кількість бездротових працюючих пристроїв пересягне число яке рівне кількості людей на землі, адже на кожну людину припадає приблизно 3-4 пристрої бездротової мережі, такі як мобільний телефон, планшет, ноутбук і тд. Ці пристрої вже на всі 100% пронизують наше життя і роблять нас залежними від них.

Швидкість роботи, ефективність використання та користь від цих пристроїв наряду залежить від швидкості інтернету. Будьмо чесними навряд чи в найближчі пару років в наших краях з'являться швидкісні мобільні 5G-мережі, зате представлений в минулому році новий стандарт Wi-Fi 6 вже доступний кожному. Пристроїв з його підтримкою на ринку все ще мало, але з кожним днем їх стає дедалі більше.

Впровадження нового протоколу розгортання мережі IEEE 802.11ax або як його називають простіше Wi-Fi6, сприятиме організації більш надійніших, ефективніших і швидших мереж бездротового доступу Інтернет.

Об'єктом дослідження є протокол роботи Wi-Fi мережі IEEE 802.11ax.

Предметом дослідження є методи збільшення пропускної здатності мережі, оптимізація процесів.

Мета роботи: є підвищення ефективності та зменшення енергозатратності мереж бездротового доступу Wi-Fi за рахунок застосування методик розрахунку мереж бездротового доступу Wi-Fi.

Наукова новизна:

1. Отримала подальший розвиток швидкість передачі даних. Підвищення швидкості передачі даних до 1,3 Гбіт / с, більш ніж в два рази в порівнянні з типовими мережами Wi-Fi.
2. Отримала подальший розвиток висока пропускна здатність. До мережі Wi-Fi стандарту IEEE 802.11ax можна одночасно підключити

більше пристроїв без зниження продуктивності, що дозволяє вирішити проблеми з перевантаженням.

3. Отримала подальший розвиток затримка. Продукти стандарту Wi-Fi ас покращують якість роботи таких додатків, як ігри або потокова музика, де навіть найменша затримка може чинити шкідливий вплив.

4. Отримало подальший розвиток ефективне використання електроенергії. Внесення змін до Wi-Fi ах означає зменшення енергоспоживання при передачі даних.

Практична цінність полягає у тому, що запропоновані в ній математичні моделі і методи можуть бути використані при вирішенні важливих прикладних задач побудови та проектування мереж бездротового доступу Wi-Fi. Перерозподілу та збільшення пропускної здатності каналів зв'язку, збільшення робочої частоти в Wi-Fi мережі побудованої на базі протоколу IEEE 802.11ах.

Структура та обсяг роботи. Магістерська дисертація складається з вступу, чотирьох розділів та висновків.

У *вступі* подано загальну характеристику роботи, зроблено оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень, сформульовано мету і задачі досліджень, показано наукову новизну отриманих результатів і практичну цінність роботи.

У *першому розділі* наведено опис базових структур мереж бездротового доступу Wi-Fi.

У *другому розділі* було проаналізовано найактуальніший протокол сімейства IEEE 802.11ах.

У *третьому розділі* розглянуто методики розрахунку метеж бездротового доступу та проведено моделювання в середовищі MATLAB.

У *четвертому розділі* розроблено стартап проект по темі магістерської дисертації.

У *висновках* представлені результати проведеної роботи.

Ключові слова: Wi-Fi, IEEE802.11ах, STA, AP, бездротові мережі.

ABSTRACT

The work contains: 98 pages, 44 figures and 23 tables. 24 sources were used.

Actuality of theme. In today's world, wireless technology devices are gaining popularity. Inevitably, the number of wireless devices will exceed the number equal to the number of people on earth, because each person has about 3-4 wireless devices, such as mobile phone, tablet, laptop, etc. These devices are already 100% permeating our lives and making us dependent on them.

The speed, efficiency and benefits of these devices directly depend on the speed of the Internet. Let's be honest, high-speed mobile 5G networks are unlikely to appear in our region in the next couple of years, but the new Wi-Fi 6 standard introduced last year is already available to everyone. There are still few devices with its support on the market, but they are becoming more and more.

The introduction of the new IEEE 802.11ax deployment protocol, or as it is called simply Wi-Fi6, will help to organize more reliable, efficient and faster wireless Internet access networks.

The object of study is the protocol of Wi-Fi network IEEE 802.11ax.

The subject of research is methods of increasing network bandwidth, process optimization.

Purpose: to increase the efficiency and reduce the energy consumption of Wi-Fi wireless access networks through the use of methods for calculating Wi-Fi wireless access networks.

Scientific novelty:

1. The data transfer rate has been further developed. Increases data transfer speeds to 1.3 Gbps, more than double that of typical Wi-Fi networks.
2. High capacity was further developed. You can connect more devices to the IEEE 802.11ax Wi-Fi network at the same time without reducing performance, which allows you to solve congestion problems.
3. The delay was further developed. Wi-Fi ac products improve the performance of applications such as games or streaming music, where even the slightest delay can have a detrimental effect.

4. Efficient use of electricity has been further developed. Making changes to Wi-Fi ax means reducing power consumption when transmitting data.

The practical value lies in the fact that the mathematical models and methods proposed in it can be used in solving important applications for the construction and design of Wi-Fi wireless access networks. Redistribution and increase the bandwidth of communication channels, increase the operating frequency in the Wi-Fi network built on the IEEE 802.11ax protocol.

Structure and scope of work. The master's dissertation consists of an introduction, four chapters and conclusions.

The introduction presents a general description of the work, assesses the current state of the problem, substantiates the relevance of research, formulates the purpose and objectives of research, shows the scientific novelty of the results and the practical value of the work.

The first section describes the basic structures of Wi-Fi wireless access networks.

The second section analyzes the most current protocol of the IEEE 802.11ax family.

In the third section, the methods of calculating wireless access interference are considered and modeling in the MATLAB environment is performed.

In the fourth section, a startup project on the topic of a master's dissertation was developed.

The conclusions present the results of the work.

Keywords: Wi-Fi, IEEE802.11ax, STA, AP, wireless networks.

ЗМІСТ

ЗМІСТ	9
ПЕРЕЛІК СКОРОЧЕНЬ.....	11
ВСТУП.....	13
РОЗДІЛ 1	14
БЕЗДРОТОВИЙ ІНТЕРНЕТ WI-FI.....	14
1.1. Структура мережі бездротового доступу Wi-Fi.....	14
1.1.1. Інфраструктурна топологія.....	15
1.1.2. Спеціальна топологія мережі.....	15
1.1.3. Топологія бездротової сітки	16
1.1.4. P2P мережева топологія	17
1.2. Аналіз стандартів доступу до мережі Wi-Fi сімейства IEEE 802.11.	17
1.2.1. Базовий стандарт IEEE 802.11	18
1.2.2. 802.11a (Wi-Fi 2).....	19
1.2.3. 802.11b (Wi-Fi 1)	19
1.2.4. 802.11g (Wi-Fi 3)	20
1.2.5. 802.11n (Wi-Fi 4)	20
1.2.6. IEEE 802.11ac (гігабітний WiFi або WiFi 5)	21
1.2.7. IEEE 802.11ad (WiGig).....	22
1.2.8. IEEE 802.11ah (WiFi HaLow)	22
1.3. Аналіз протоколів захисту мереж бездротового доступу Wi-Fi.	26
1.3.1. Протокол безпеки WEP	27
1.3.2. WPA.....	29
1.3.3. WPA2	32
1.3.4. WPA3.....	35
1.4. Механізм доступу до середовища	40
1.4.1. Фізичний рівень (Physical layer) стандарту IEEE 802.11	40
1.4.2. MAC-рівень стандарту IEEE 802.11.....	41
1.5. Новизна розвитку сімейства IEEE 802.11	41
1.5.1. Етапи розробки.....	42
1.5.2. Новизна протоколу.	44
Висновки	45
РОЗДІЛ 2	46

АНАЛІЗ ПРОТОКОЛУ IEEE 802.11AX.....	46
2.1. Структура протоколу IEEE 802.11ax.	47
2.1.1.Формати PPDU	49
2.1.2. Від одного користувача до кількох користувачів (MU)	51
2.1.3. Типи піднесучих.....	57
2.2. Цілі та задачі стандарту IEEE 802.11ax.	61
Висновки	63
РОЗДІЛ 3	63
МЕТОДИКА РОЗРАХУНКУ МЕРЕЖІ БЕЗДРОТОВОГО ДОСТУПУ WI-FI НА ОСНОВІ ПРОТОКОЛУ IEEE 802.11AX.....	63
3.1. Методика розрахунку пропускної здатності мережі стандарту IEEE 802.11ax.	64
3.2. Алгоритм підвищення енергоефективності механізму енергозбереження IEEE 802.11ax	69
3.2.1.Спільний інтервал TWT і алгоритм планування (JTWSA).....	74
3.2.2. Математичне моделювання.	78
Висновки	82
РОЗДІЛ 4 РОЗРОБЛЕННЯ СТАРТАП ПРОЕКТУ	83
4.1.Опис ідеї проекту	83
4.2.Технологічний аудит ідеї проекту.....	84
4.3.Аналіз ринкових можливостей запуску стартап-проекту.....	85
4.4.Розроблення маркетингової програми стартап-проекту	90
Висновки	93
ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ.....	94
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	96

ПЕРЕЛІК СКОРОЧЕНЬ

IEEE	Institute of Electrical and Electronics Engineers (Інститут інженерів з електротехніки та електроніки);
DSSS	Direct Sequence Spread Spectrum (метод прямої послідовності для розширення спектру)
DCF	Distributed coordination function (розподілена функція координації)
PCF	Point coordination function (функція координації точок)
PC	Point Coordination (точка координації)
OFDM	Orthogonal Frequency Division Multiplexing (ортогональне частотне мультиплексування)
MIMO	Multiply Input Multiply Output (множинний вхід, множинний вихід)
QAM	Quadrature Amplitude Modulation (квадратурно-амплітудна модуляція)
BSS	Base Station Subsystem (підсистема базових станцій)
WPA	Wi-Fi Protected Access (Wi-Fi захищений доступ)
CDMA	Code Division Multiple Access (множинний доступ з кодовим розділенням каналів)
WiMAX	Worldwide Interoperability for Microwave Access (загальносвітова сумісність широкосмугового безпроводового доступу)
SAE	System Architecture Evolution (еволюція системної архітектури)
Wi-Fi	Wireless Fidelity
FHSS	(Frequency Hopping Spread Spectrum) – Псевдовипадкова перестройка робочої частоти
CSMA/CA	(Carrier Sense Multiple Access with Collision Avoidance) – Багатостанційний доступ з контролем несучої і запобіганням конфліктів
P2P	мережа Peer-to-Peer
MAC	(Medium Access Control) – Управління доступом до середи

SSID	(Service Set Identifier) – ідентифікатор бездротової мережі
WEP	Wired Equivalent Privacy
AES	Advanced Encryption Standard
CP	cyclic prefix
HE_EXT_SU	Розширений діапазон PPDU
(HE)	high efficiency
CFO	carrier frequency offset
STA	Station
TWT	target wake time
JTWSA	Joint TWT interval and scheduling algorithm
R.H.S	right hand side

ВСТУП

Останні роки стали свідками безперервної і зростаючої популярності бездротових мереж Wi-Fi, які привертають постійно зростаючу кількість користувачів. Це призвело до значного збільшення споживання даних у всіх мережах. Згідно глобальних даних, очікується збільшення трафіку в 10 разів більше від рівня, виміряного у 2014 році.

Оскільки основна частина трафіку формується і споживані всередині приміщень, внутрішні рішення для підключення може сприяти задоволенню сприйнятливих вимог щодо потужності. WLAN на основі IEEE 802.11, які найбільш популярні та успішні бездротові рішення для приміщень, еволюціонували як ключова технологія, що дозволяє охоплювати середні та великі підприємства, громадські зони, житлові комплекси тощо.

Розмір світового ринку Wi-Fi чітко вказує популярність мереж WLAN на основі IEEE. Світова вартість ринку Wi-Fi становила 14,8 мільярдів доларів США в 2015 році, і ще планується збільшити до 38,6 млрд дол 2022 рік. Комітет зі стандартизації IEEE 802.11 має активно продовжувати випуск нових проектів поправок включати новітні технологічні досягнення. Нещодавно робоча група IEEE 802.11 розробила новий стандарт WLAN, IEEE 802.11ax. 802.11ax спрямований на покращення ємності системи та збільшення енергозбереження. Точніше, це задумано для підвищення ефективності в сценаріях з обмеженими перешкодами (через високу щільність IEEE 802.11 пристроїв).

Метою даної роботи є підвищення ефективності та зменшення енергозатратності мереж бездротового доступу Wi-Fi за рахунок застосування методик розрахунку мереж бездротового доступу Wi-Fi.

Об'єктом дослідження є це протокол роботи Wi-Fi мережі IEEE 802.11ax, який розглядається в побудові бездротової мережі Wi-Fi, а предметом - методи збільшення пропускної здатності мережі, оптимізація процесів, в основі яких лежить протокол IEEE 802.11ax.

РОЗДІЛ 1

БЕЗДРОТОВИЙ ІНТЕРНЕТ WI-FI.

За останні кілька років поширення бездротових мереж Wi-Fi було сильним, тому розробники розглядають можливість винайдення, виробництва та впровадження нових стандартів зв'язку, які, на відміну від своїх попередників, будуть більш продуктивними, ефективними та безпечними. На початку свого існування бездротові пристрої могли підтримувати швидкість передачі даних вище 1-2 Мбіт/с, що є незначним порівняно з поточними. У сучасному світі швидкість передачі інформації в бездротових мережах може досягати 1 Гбіт/с а то і більше, що неминуче призводить до конкуренції за дротові мережі. Існує багато типів бездротових мереж, кожна з яких відрізняється від свого попередника різними параметрами – швидкістю передачі даних, діапазоном і типом кодування інформації.

1.1. Структура мережі бездротового доступу Wi-Fi.

Бездротова локальна мережа(Wi-Fi), заснована на стандартах серії IEEE 802.11. На ранніх етапах свого існування термін «Wi-Fi» використовувався лише для позначення технології, яка забезпечувала зв'язок у діапазоні частот вище 2,4 ГГц, але зараз він використовується для бездротових мереж та інших технологій. Мережа Wi-Fi використовується для зв'язку та обміну даними між вузлами, але це гнучка система обміну інформацією, яка працює як альтернативна дротова мережа, розташована в приміщенні або на відкритій території. Мережа також використовується для організації публічних точок доступу, таких як аеропорти, площі та для інших місць скупчення людей, а також для організації тимчасових бездротових мереж для проведення фестивалів, футбольних матчів або музейних виставок.

Для побудови мереж бездротового доступу інженери користуються мережевими топологіями, кожна з яких адаптується під середовище. Мережі бездротового доступу мають декілька мережних топологій [14]:

- Інфраструктурна топологія мережі;
- Спеціальна топологія мережі;
- Топологія бездротової сітки;
- P2P мережева топологія;

1.1.1. Інфраструктурна топологія

На рисунку 1.1 зображена інфраструктурна топологія:

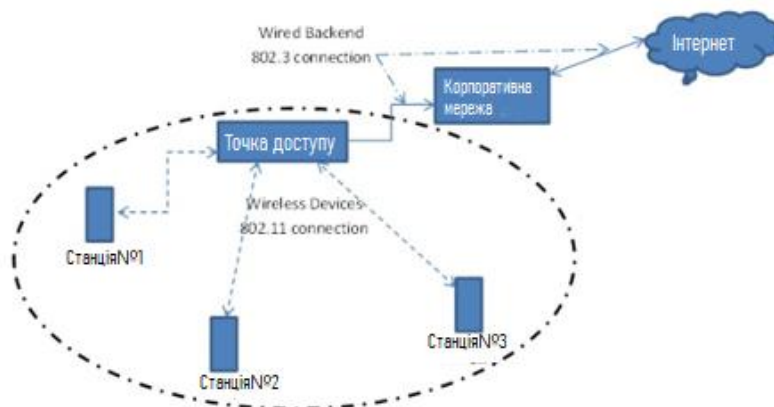


Рис.1.1. Топологія інфраструктурної мережі.

Область, яка позначена пунктирним лінією замкнуту в коло, називається базовим набором послуг (BSS). Всі станції, що підключені до точки доступу, утворюють базовий сервісний набір. Також існує ще базова зона обслуговування (BSA). Основна зона обслуговування - це зона, яка охоплена точкою доступу. Сигнал точки доступу може виходити за межі діапазону підключених до нього пристроїв. Ця зона покриття – являється BSA.

1.1.2. Спеціальна топологія мережі

Спеціальна топологія є самодостатньою мережею Peer-to-Peer. Тобто, це мережа без точки доступу, в якій пристрої не тільки являються кінцевими точками, а й маршрутизаторами. Це показано нижче:

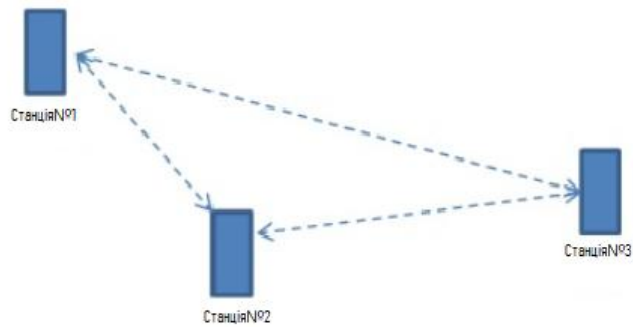


Рис.1.2. Спеціальна топологія мережі.

1.1.3. Топологія бездротової сітки

Мережа Wireless Mesh - це взаємозв'язок підключених вузлів, які утворюють самостійну мережу. Якщо один вузол мережі «падає», то формується новий шлях для створення мережі, що працює. Сітчасті вузли використовують стандарти 802.11, щоб спілкуватись один з одним. Резервний сітчастий вузол також може бути налаштований для підключення до загальнодоступного шлюзу, якщо первинний сітчастий вузол опуститься. До будь-якого мережевого вузла можуть бути підключені користувачі. Навантаження на мережевий трафік потрібно збалансувати між різними вузлами та створити ефективні механізми маршрутизації, щоб забезпечити найшвидший шлях до загальнодоступної мережі.

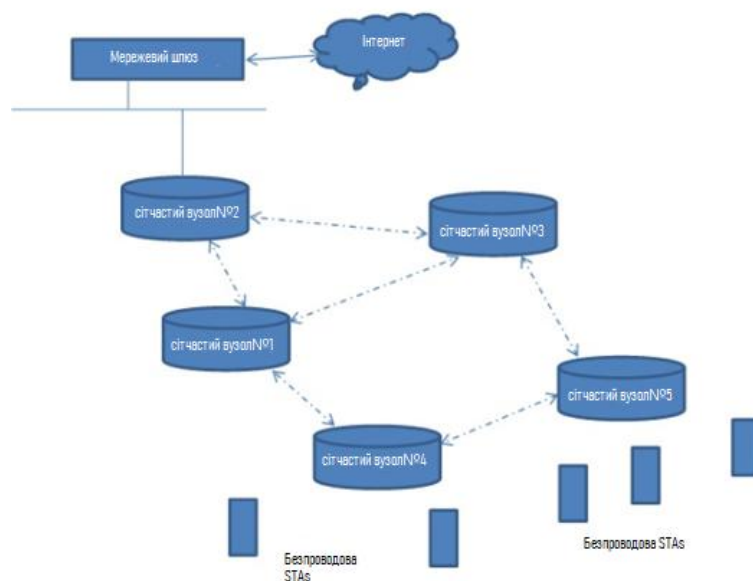


Рис.1.3. Мережа бездротової локальної мережі

1.1.4. P2P мережева топологія

Мережа P2P - це мережа Peer-to-Peer в якій одна бездротова станція виконує роботу бездротової головної станції. Головна станція розсилає маяки і відповідає за підтримку мережі Peer to Peer. Інші бездротові станції підключаються до власника групи. Клієнтську станцію називають груповими клієнтами. Коли власник групи покидає мережу, клієнт групи прийме роль власника групи. Пристрій власника групи також може одночасно приєднатися як пристрій групового клієнта до іншої мережі P2P, якщо він підтримує кілька радіостанцій 802.11[8].

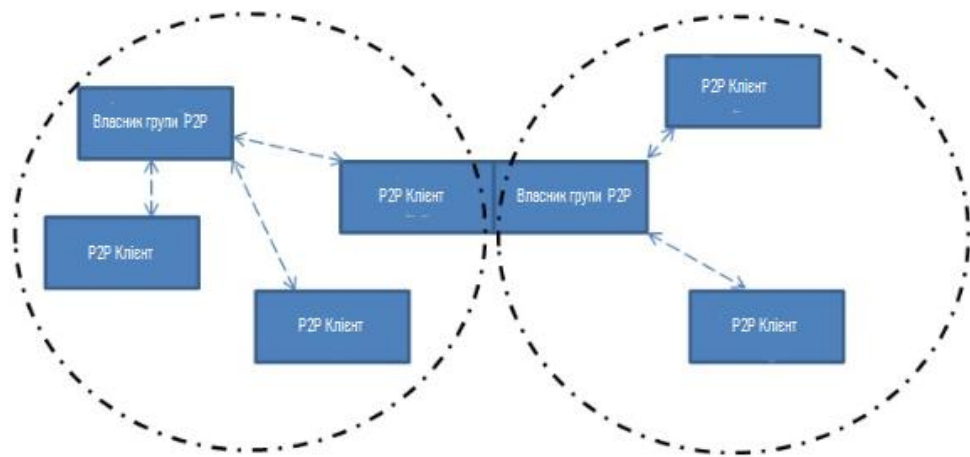


Рис.1.4. Топологія мережі P2P

1.2. Аналіз стандартів доступу до мережі Wi-Fi сімейства IEEE 802.11.

У 1990 році IEEE 802 створив групу для вивчення стандартів для бездротових мереж Wi-Fi. Їхнє головне завдання — створити загальний стандарт для мереж, що працюють у діапазоні частот 2,4 ГГц зі швидкістю з'єднання 1-2 Мбіт/с. У 1997 році була завершена розробка стандарту і була затверджена перша специфікація 802.11.

Цей стандарт вважається першим стандартом для обладнання WLAN. Однак початкова швидкість передачі інформації на той момент не відповідала побажанням користувачів. Саме тому, щоб задовольнити всіх користувачів і

зробити технологію популярною, розробники створили новий стандарт. А восени 1999 року були затверджені удосконалення існуючих стандартів.

На сьогодні існує велика кількість стандартів групи IEEE 802.11. Розглянемо найбільш розповсюдженні і найбільш вживані:

1. Базовий 802.11;
2. IEEE 802.11a (Wi-Fi 2);
3. IEEE 802.11b (Wi-Fi 1);
4. IEEE 802.11g (Wi-Fi 3);
5. IEEE 802.11n (Wireless-N чи Wi-Fi 4);
6. IEEE 802.11ac (гігабітний Wi-Fi або Wi-Fi 5);
7. IEEE 802.11ax (Wi-Fi 6 або високоефективна WLAN);

Всі стандарти IEEE 802.11 працюють на нижніх двох рівнях моделі ISO / OSI, фізичному та каналному, тому будь-який мережевий додаток, мережева операційна система, або протокол (наприклад, TCP / IP), будуть так само добре працювати в мережі 802.11, як і в мережі Ethernet [8].



Рис.1.5. Рівні моделі ISO / OSI і їх відповідність стандарту 802.11.

1.2.1. Базовий стандарт IEEE 802.11

В середині літа 1997 року був оприлюднений стандарт IEEE 802.11 який мав назву «Специфікація фізичного рівня і рівня контролю доступу до каналу

передачі бездротових локальних мереж». Цей протокол ідентифікував архітектуру мережі, формати пакетів, способи захисту даних та автентифікацію, а також різні принципи доступу пристроїв до каналів зв'язку.

В початковому етапі свого існування стандарт 802.11 працював з обладнанням на частоті 2.4ГГц і максимальною швидкістю до 2 Мбіт/сек [14]. Базовий протокол 802.11 на своєму фізичному рівні реалізує 2 методи передачі даних:

- Метод частотних стрибків FHSS (Frequency Hopping Spread Spectrum);
- Метод прямої послідовності DSSS (Direct Sequence Spread Spectrum);

Стандарт 802.11 став «фундаментом» для наступних стандартів.

1.2.2. 802.11a (Wi-Fi 2)

Стандарт IEEE 802.11a був впроваджений в 1999 році. Замість діапазону 2,4 ГГц він передбачає використання частоти 5 ГГц. Як правило, більш високі частоти поєднуються з більш високими швидкостями, але з меншим діапазоном. Для досягнення більш високої швидкості він першим реалізував технологію OFDM (мультиплексування з ортогональним частотним розділенням) - метод цифрової модуляції, що використовується для кодування даних на кількох частотах - у своїй схемі кодування, що дозволило йому мати теоретично максимальну швидкість 54 Мбіт / с, що було радіаційним покращення в порівнянні з вихідним стандартом WiFi.

Недоліками цього стандарту є висока споживча потужність і менший радіус дії обладнання. 802.11a працював у діапазоні 5 ГГц, це зробило продукти більш дорогими [13]. Тому в основному він використовувався у бізнес-мережах.

1.2.3. 802.11b (Wi-Fi 1)

802.11b використовує DSSS (Direct -Sequence Spread Spectrum) - метод модуляції, використовуваний для зменшення приміщень сигналів - у діапазоні 2,4 ГГц, що дозволяє досягти швидкості до 11 Мбіт / с. Діапазон 2.4 відмінно справляється з подоланням перешкод, забезпечуючи більше покриття WiFi. На жаль, дані передаються набагато повільніше, особливо коли це пов'язано із мережевими завадами, винятковими пристроями, працюючими на тих же частотах, таких як радіоняні, мікрохвильові печі, бездротові телефони, швидкісна техніка та пристрої Bluetooth. Завади можуть бути зменшені, якщо утримувати пристрої 802.11b подалі від таких пристроїв.

У зв'язку з тим, що Wi-Fi 1 використовував тільки діапазон 2,4, продукти були набагато дешевші, ніж 802.11a, що зробило його більш популярним для домашніх мереж [13].

1.2.4. 802.11g (Wi-Fi 3)

Стандарт IEEE 802.11g є удосконаленням стандарту IEEE 802.11b. Завдяки застосування ефективніших технологій модуляції сигналу було підвищено швидкість передачі інформації до 54Мбіт/с.

У той час зворотна сумісність була обов'язковою, тому що у багатьох людей все ще були точки доступу та комп'ютери, які використовували попередні стандарти. 802.11g сумісний з продуктами 802.11b. Однак продукти Wi-Fi можуть підключатися тільки до того стандарту, відповідно до якого вони працюють. Комп'ютер 802.11b, підключений до точки доступу 802.11g, може працювати тільки з тією швидкістю, яку дозволяє стандарт b. З іншого боку, який пристрій, підключений до ab AP, буде працювати тільки з тією швидкістю, яку пропонує AP [13].

1.2.5. 802.11n (Wi-Fi 4)

Wireless-N був розроблений в 2009 році для підвищення швидкості, надійності і розширення діапазону бездротової передачі.

Це був перший стандарт, в якому використовувалася технологія MIMO (Multiple-Input Multiple-Output). Продукти MIMO використовують серію антен для прийому більшої кількості даних від одного пристрою за раз, що призводить до більш швидкої передачі даних. Крім того, він першим дозволив використовувати дві радіочастоти - 2,4 ГГц і 5 ГГц. Використання обох частот робить стандарт 802.11n сумісним з пристроями 802.11a / b / g. Основними покращеннями були:

1. Створення багатоканального входу/виходу(MIMO);
2. Збільшення ширини смуги пропускання від 20МГц до 40МГц;

З усіма поліпшеними функціями Wi-Fi 4 підтримує швидкість передачі даних до 600 Мбіт / с і теоретичну дальність дії в 70 метрів в приміщенні, що є значним оновленням у порівнянні з попередніми стандартами [13].

1.2.6. IEEE 802.11ac (гігабітний Wi-Fi або Wi-Fi 5)

5-е покоління Wi-Fi було створено в 2013 році. Щоб зменшити перешкоди в діапазоні 2,4 ГГц, він був розроблений для роботи в діапазоні 5 ГГц. Технологія Wi-Fi 802.11ac використовує дві смуги частот для бездротового зв'язку. Щоб зробити це можливим, деякі постачальники включили технологію Wireless-N, щоб продукти змінного струму були сумісні з діапазоном 2,4 ГГц. Швидкості передачі даних розрізняються залежно від того, яка частота використовується, швидкість смуги пропускання до 1300 Мбіт / с може бути досягнута в діапазоні 5 ГГц, а в діапазоні 2,4 ГГц максимальна швидкість складає 450 Мбіт / с.

Wi-Fi 802.11ac перший стандарт, який використав багато користувачів MIMO спадного каналу. Технологія Wireless-N MIMO зробила ще один крок вперед, щоб ще більше поліпшити передачу даних. DL MU-MIMO дозволяє бездротовим маршрутизаторам передавати інформацію на кілька пристроїв одночасно, підвищуючи швидкість смуги пропускання і зменшуючи затримку. Завдяки технології Wireless-N 802.11ac сумісний з 802.11a / b / g / n [9]. Також

протягом декількох років розроблялись доповнення на основі цього типу стандарту - IEEE 802.11ad та IEEE 802.11ah.

1.2.7. IEEE 802.11ad (WiGig)

Розроблений для забезпечення багатогігабітної бездротової системи (MGWS) з високою пропускнуою здатністю даних, 802.11ad став частиною серії 802.11 в 2012 році. Він досяг неймовірно високій швидкості - до 6,7 Гбіт / с. На відміну від попередніх стандартів, він не використовував діапазони 2,4 або 5 ГГц, він працював в діапазоні 60 ГГц. Пам'ятайте, що чим вище частота, тим менше діапазон. В ідеальних умовах пристрою 802.11ad повинні знаходитися на відстані близько 9 метрів від точки доступу.

1.2.8. IEEE 802.11ah (WiFi HaLow)

Стандарт 802.11ah, прийнятий в травні 2017 року, був націлений на використання неліцензованих діапазонів частот нижче 1 ГГц. Його мета полягала в зниженні енергоспоживання і створення мереж WLAN з розширеним діапазоном, що перевершують діапазони 2,4 / 5 ГГц. WiFi HaLow працював в діапазоні 900 МГц, що дозволяло йому мати теоретичний діапазон 543 м в приміщенні (1781,5 футів) і швидкість передачі даних до 347 Мбіт / с. Через низьку потреби в енергії 802.11ah корисний для пристроїв, які намагаються обмінюватися даними на великих відстанях без використання великої кількості енергії [13].

Таблиця 1.1.

Стандарти сімейства IEEE 802.11.

Стандарти WiFi	Інша назва	Рік впровадження	Опис
802.11	N / A	1997 р.	Оригінальний стандарт. Використовував смугу частот 2,4 ГГц, мав максимальну

			пропускну здатність 2 Мбіт / с і дальність дії 66 футів.
--	--	--	--

Продовження таблиці 1.1

802.11a	Wi-Fi 2	1999 р.	В ідеальних умовах він досяг швидкості до 54 Мбіт / с в діапазоні 5 ГГц.
802.11b	Wi-Fi 1 чи 802.11 High Rate	1999 р.	Набагато дешевше в розробці, тому що він використовував смугу 2,4 ГГц, тому він став більш популярним, ніж 802.11a. Досягнуто швидкості до 11 Мбіт / с.
802.11c	N / A	1998 р.	Пов'язаний з мостом для бездротового клієнтського пристрою 802.11 (тепер є частиною поправки 802.1D).
802.11d	N / A	2001 р.	Дозволяє клієнтам автоматично налаштовуватися відповідно до специфікацій країни, в якій вони працюють (так званий всесвітній режим), що спрощує завдання для країн, які не є частиною великого домену.
802.11e	N / A	2005 р.	Пропонує функції якості обслуговування (QoS) для поліпшення чутливих до затримок додатків, таких як дані, голос і відео.
802.11F	N / A	2003 р.	Забезпечує зв'язок між точками доступу стандарту 802.11 в системі розподілу (протокол між точками доступу).
802,11 г	Wi-Fi 3	2003 р.	Поєднання кращих характеристик 802.11a / b дозволило досягти швидкості до 54 Мбіт / с в діапазоні 2,4 ГГц.
802.11h	N / A	2003 р.	Спочатку розроблений відповідно до європейських правил для вирішення проблем, пов'язаних з перешкодами для супутників і радарів, що використовують діапазон 5 ГГц.

Продовження таблиці 1.1

802.11i	N / A	2004 р.	Усунені уразливості в безпеці WEP і покращено шифрування бездротової мережі шляхом заміни короткою аутентифікації і конфіденційності на детальну безпеку для мереж 802.11a / b / g.
802.11j	N / A	2004 р.	Розроблений для Японії, він містить специфікації для використання діапазонів 4,9 ГГц і 5 ГГц для зовнішніх, внутрішніх і мобільних додатків.
802.11k	N / A	2008 р.	Поліпшення розподілу трафіку в WLAN.
802.11 м	802.11 Housekeeping чи 802.11 Cleanup	1999 р.	Обслуговування серії 802.11 і супутньої документації.
802.11n	WiFi 4 чи Wireless-N	2009 р.	Використовує діапазони 2,4 ГГц і 5 ГГц і збільшує швидкість до 600 Мбіт / с.
802.11p	N / A	2010 р.	Додає бездротовий доступ в автомобілі (WAVE).
802.11r	Швидкий перехід на BSS.	2008р.	Розроблено для підвищення швидкості передачі обслуговування між точками доступу в WLAN.
802.11s	N / A	2011 р.	Визначає, як бездротові пристрої можуть підключатися для створення комірчастої мережі, яка може використовуватися для відносно фіксованих топологій і мереж з довільним підключенням.

802.11T	N / A	2008 р.	Прогнозування продуктивності бездротової мережі (WPP)
802.11u	N / A	2011 р.	Покращує взаємодію з зовнішніми мережами.

Продовження таблиці 1.1

802.11v	N / A	2011 р.	Покращення бездротової мережі для управління і настройки клієнтських пристроїв.
802.11 Вт	N / A	2009 р.	Підвищує безпеку фрейму управління.
802.11y	N / A	2008 р.	Підтримує роботу в діапазонах 3650-3700 МГц в США.
802.11ac	Wi-Fi 5	2013р.	Підтримує діапазони 2,4 ГГц (через технологію 802.11n) і 5 ГГц і має швидкість до 1300 Мбіт / с.
802.11ad	WiGig	2012 р.	Досягає надзвичайно високій швидкості (до 6,7 Гбіт / с) на частоті 60 ГГц.
802.11af	White-Fi или Super WiFi	2014 р.	Дозволяє WLAN працювати в спектрі білого ТВ-простору між 54 і 790 МГц.
802.11ah	Wi-Fi HaLow	2016 р.	Використовує смуги частот нижче 1 ГГц для зниження енергоспоживання і розширення діапазону.
802.11ai	N / A	2016 р.	Встановлює методи швидкої початкової установки з'єднання (FILS).
802.11aj	Китай міліметро ва хвиля	2018 р.	Забезпечено роботу в діапазонах частот китайського міліметрового діапазону - 60 ГГц і 45 ГГц - шляхом зміни фізичного та середнього рівнів контролю доступу 802.11ad.
802.11ak	N / A	2018 р.	Розширює можливості середовища IEEE 802.11 для забезпечення внутрішніх транзитних каналів для

			мостових мереж IEEE 802.1Q.
802.11ax	Wi-Fi 6	2019 р.	Забезпечує більш високу швидкість, підтримує більшу кількість пристроїв одночасно, зменшує затримку, підвищує безпеку і збільшує пропускну здатність.

Продовження таблиці 1.1

802.11ay	Наступне покоління 60 ГГц	В розробці	Визначає новий фізичний рівень (PHY) для мереж 802.11 для роботи в діапазоні 60 ГГц і буде розширенням 802.11ad для збільшення пропускну здатності і діапазону.
802.11az	N / A	В розробці	Визначте модифікації рівнів PHY і MAC.
802.11ba	Пробудження Радіо (WUR)	В розробці	Має намір продовжити час автономної роботи пристроїв і датчиків, особливо в мережах Інтернету речей (IoT).
802.11be	Wi-Fi 7	В розробці	Будуть засновані на 802.11ax для досягнення надзвичайно високої пропускну здатності (EHT) і будуть використовувати діапазони 2,4, 5 і 6 ГГц.

1.3. Аналіз протоколів захисту мереж бездротового доступу Wi-Fi.

Існує багато технологій безпеки, кожна з яких забезпечує рішення для найважливіших компонентів стратегії захисту даних: перевірка ідентичності, цілісність даних та активна перевірка. Ми визначаємо перевірку ідентичності як автентифікацію користувача або термінального пристрою та його місцезнаходження, а потім авторизацію користувача та кінцевого пристрою. Цілісність даних включає такі сфери, як безпека мережевої інфраструктури, безпека периметра та конфіденційність даних. Проактивний огляд допомагає

забезпечити дотримання встановлених політик безпеки на практиці та відстежувати всі відхилення та спроби несанкціонованого доступу.

1.3.1. Протокол безпеки 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 злоумисників, а просто зробити її недоступною для читання. Основним завданням цієї технології було шифрування потоку даних, що передавались в межах безпроводної 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 [8].

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.

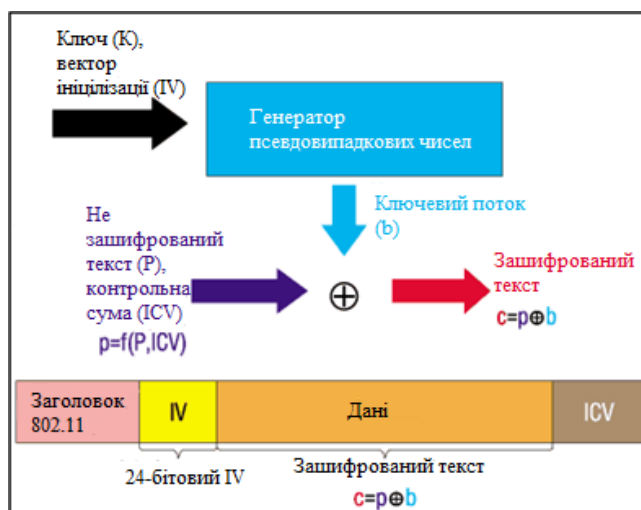


Рис 1.8. Схема роботи шифрування по протоколу WEP

Зашифроване повідомлення (Рисунок 1.8.) утворюється в результаті виконання операції XOR над незашифрованим повідомленням з ICV і ключовим потоком. Коли інформація приймається на іншій стороні, проводиться зворотний процес ($p = c + b$) [2]. 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, зашифрованих RC4 за допомогою того ж значення b , являє собою не що інше, як операцію XOR до двох початковим текстам.

$$\begin{aligned} c_1 &= p_1 + b & c_2 &= p_2 + b & (1.1) \\ c_1 + c_2 &= (p_1 + b) + (p_2 + b) = p_1 + p_2 \end{aligned}$$

Таким чином, ми можемо отримати незашифрований текст, який є результатом операції XOR між двома іншими оригінальними текстами. Процедура їх видалення 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 $2^{24} = 16\,777\,216$, 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 ($224 / 1\,497\,600 = 11,2$ ч). 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.

1.3.2.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 (рукопостискання EAPOL);
2. 802.1X рукопостискання верхнього шару EAP / EAPOL для автентифікації користувача;

Обидва вищевказані механізми автентифікації 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 [1].

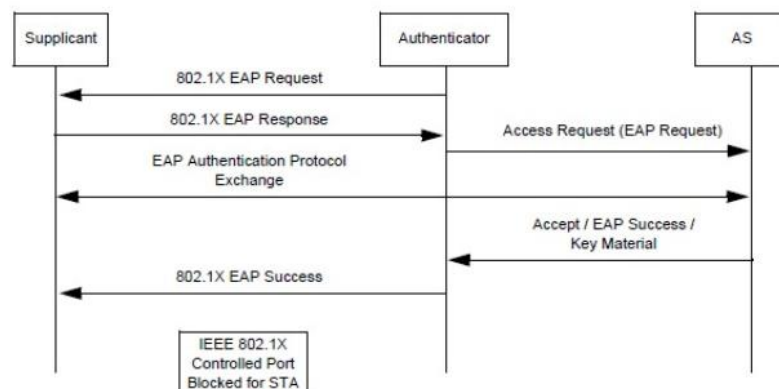


Рис. 1.9. Автентифікація EAP, яка забезпечує парний головний ключ для рукостискання EAPOL

Інформаційний елементи WPA і RSN

Стандарт Wi-Fi / 802.11 представив два нові інформаційні елементи для забезпечення нової схеми шифрування WPA:

- 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 рукошукання безпеки 802.11i / 802.1X.



Рис. 1.10. 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 потрібно перевірити AP/Station, щоб побачити, чи є інформаційний елемент WPA. Якщо це не WPA - AP/Station може вирішити ігнорувати аналіз інформаційного елемента [8].

Таблица 1.2.

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

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 широкополосний / широкополосний 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 наведено нижче. Розмір IE RSN обмежений максимум 255 байтами.

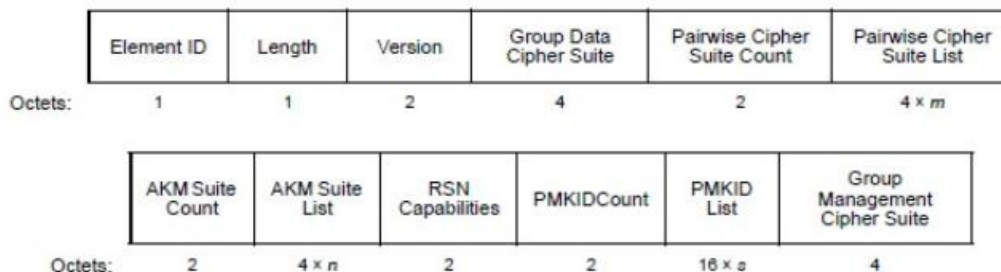


Рис. 1.11. RSN – формат

1.3.3.WPA2

Стандарт IEEE 802.11i, також відомий як Wi-Fi Protected Access 2 (WPA2), є поправкою до 802.11 стандарт із зазначенням механізмів захисту бездротових мереж. Проект стандарту був ратифікований на початку літа 2004 р. Він замінює попередні технічні умови безпеки, конфіденційність провідної еквівалентної конфіденційності (WEP), яка виявила серйозні недоліки в безпеці. Захищений доступ Wi-Fi (WPA) раніше був представлений як проміжне рішення щодо невпевненості в WEP. WPA реалізував лише підмножину IEEE 802.11i. WPA2 використовує специфічний режим Розширеного стандарту шифрування (AES), відомого як протокол автентифікації коду ланцюга блоку шифрування контр режимного режиму (CBC-MAC) (CCMP). CCMP забезпечує як конфіденційність даних (шифрування), так і цілісність даних. Використання розширеного стандарту шифрування (AES) є більш безпечною альтернативою шифру потоку RC4, який використовується WEP та WPA [4].

Стандарт WPA2 має два компоненти, шифрування та автентифікація, які мають вирішальне значення для безпечної бездротової локальної мережі. Елемент шифрування WPA2 передбачає використання AES (Advanced Encryption Standard), але TKIP (Temporal Key Integrity Protocol) доступний для

зворотної сумісності з існуючим обладнанням WAP. Елемент автентифікації WPA2 має два режими: Персональний та Підприємницький.

Персональний режим вимагає використання PSK (попередньо діленого ключа) і не вимагає, щоб користувачі мали окрему автентифікацію.

У режимі Enterprise, який вимагає індивідуальної автентифікації користувачів на основі стандарту автентифікації IEEE 802.1X, використовується розширений протокол EAP (протокол розширюваної автентифікації), який пропонує п'ять стандартів EAP на вибір:

- EAP-MD5;
- безпека рівня EAP-транспортного рівня (EAP-TLS);
- захищеність транспортного шару з підтримкою EAP (EAP-TTLS);
- захищений протокол автентифікації виклику рукостискання EAP vo / EAPMicrosoft;
- v2 (PEAPv2 / EAP-MSCHAPv2);
- захищена карта EAP v1 / EAP-Generic (PEAPv1 / EAPGTC) та модуль посвідчення абонента EAP-абонента Глобальної системи мобільних комунікацій (EAPSIM);

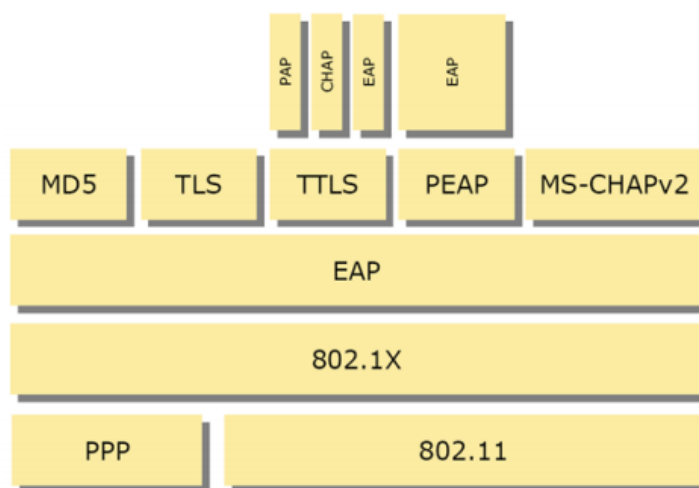


Рис. 1.12. Список протоколів

EAP-MD5 використовує MD5 алгоритм для обчислення хеш-значення пароля, які відправляються на сервер і на його стороні звіряються зі збереженим хеш-значенням. Протокол EAP-FAST дозволяє авторизуватися за логіном і паролем, а PEAP-GTC - за спеціальним токеном. Протоколи PEAP-

MSCHAPv2 і EAP-TLS проводять авторизацію по клієнтським сертифікатами [6].

Максимальний захист мережі Wi-Fi забезпечує тільки WPA2-Enterprise і цифрові сертифікати безпеки в поєднанні з протоколом EAP-TLS або EAP-TTLS. Сертифікат - це заздалегідь згенеровані файли на сервері RADIUS і клієнтському пристрої. Клієнт і сервер автентифікації взаємно перевіряють ці файли, тим самим гарантується захист від несанкціонованих підключень з чужих пристроїв і помилкових точок доступу. Протоколи EAP-TTL / TTLS входять в стандарт 802.1X і використовують 63 для обміну даними між клієнтом і RADIUS інфраструктуру відкритих ключів (PKI). PKI для авторизації використовує секретний ключ (знає користувач) і відкритий ключ (зберігається в сертифікаті, потенційно відомий всім). Поєднання ці ключів забезпечує надійну автентифікацію [6].

WPA2 встановлює захищений комунікаційний контекст у чотири фази. На першому етапі сторони, AP та клієнт, домовляться про політику безпеки (метод автентифікації, протокол для одноадресного трафіку, протокол для багатоадресної передачі та метод попередньої автентифікації) для використання, що підтримується AP та клієнтом. На другій фазі (застосовується лише для режиму підприємства).

Однією з найважливіших змін, внесених до стандарту WPA2, є відокремлення автентифікації користувачів від забезпечення цілісності та конфіденційності повідомлення, тим самим забезпечуючи більш масштабовану та надійну архітектуру безпеки, придатну для домашніх мереж або корпоративних мереж з рівними можливостями.

Автентифікація в персональному режимі WPA2, що не вимагає сервера автентифікації, виконується між клієнтом та AP, генеруючи 256-бітний PSK з простої тексту пропуску (від 8 до 63 символів). PSK спільно з ідентифікатором службового набору та довжиною SSID утворюють математичну основу для РМК (Pair-wise Master Key), який буде використаний пізніше при генерації ключів.

Автентифікація в режимі WPA2 Enterprise покладається на стандарт автентифікації IEEE 802.1X. Основними компонентами є заявник (клієнт), що приєднується до мережі, автентифікатор (АР виступає автентифікатором), що забезпечує контроль доступу, і сервер автентифікації (RADIUS), який приймає рішення про авторизацію. Автентифікатор (АР) розділяє кожен віртуальний порт на два логічні порти, один для обслуговування та інше для автентифікації, складання PAE (Port Access Entity). PAE автентифікації завжди відкритий, тоді як служба PAE відкрита лише після успішної автентифікації сервером RADIUS. Автентифікатор перетворює повідомлення EAPoL у повідомлення RADIUS, а потім пересилає їх на сервер RADIUS. Сервер автентифікації, який повинен бути сумісний з типами EAP заявника, отримує та обробляє запит автентифікації. Після завершення процесу автентифікації заявник та автентифікатор мають секретний МК (головний ключ), як показано на рисунку 1.13 [3].

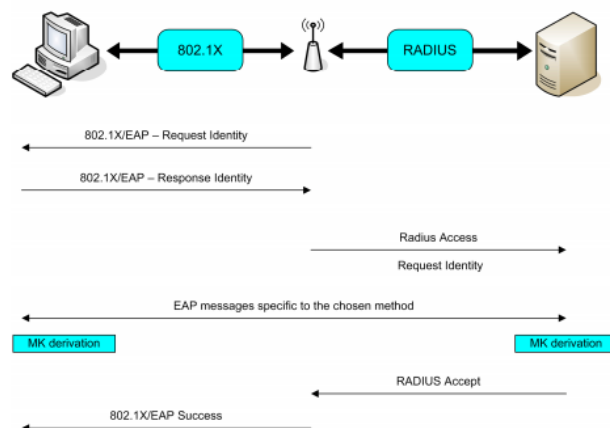


Рис. 1.13. 802.1X аутентифікація

1.3.4.WPA3

Випущена на початку літа 2018 року, WPA3 - це остання схема безпеки, розроблена для посилення безпеки в існуючих мережах Wi-Fi та вирішення проблем, з якими стикалися попередні версії. WPA3 використовує техніку одночасної автентифікації рівних (SAE) на основі пароля для автентифікації клієнта в АР .Після перегляду стандарту RFC 7764 у 2015 році було

вдосконалено протокол, який пропонує обіцяний захист. Цей захист досягається за допомогою рукостискання Dragonfly для використання дискретної криптографії логарифмічної та еліптичної кривих. Результат рукостискання генерує РМК, який потім використовується у стандартному чотиристоронній рукостисканні, який використовувався у схемі WPA2.

Сертифікація WPA3 була створена з урахуванням двох типів мереж:

- Перша - це домашня мережа, де користувачі автентифікуються за допомогою загальнодоступного пароля;
- Друга - корпоративна мережа, де можна використовувати більш досконалі методи автентифікації (наприклад, сертифікати, смарт-карти тощо).

Для розмежування обох типів термін WPA3-SAE використовується для домашніх мереж, а термін WPA3-Enterprise - для корпоративних мереж. WPA3-Enterprise використовує існуючі рукостискання, але вимагає, щоб шифри, що використовуються під час автентифікації, забезпечували не менше 192 біт безпеки. Тобто шифри повинні використовувати щонайменше 384-бітні криві для криптографії еліптичної кривої та використовувати принаймні 3072-бітні модулі при використанні RSA або DHE. В даний час сертифікація WPA3 не згадує вимоги щодо тривалості сеансових ключів або хеш-функцій, що використовуються після автентифікації. Однак рівень безпеки принаймні 192 біт, ймовірно, також буде використаний після автентифікації.

Режим WPA3-SAE для домашніх мереж цікавіший. Він передбачає підтримку існуючого одночасного автентифікації рівних (SAE) рукостискання. Це рукостискання - це автентифікований паролем обмін ключами (PAKE), тобто автентифікація проводиться на основі пароля. Рукостискання SAE забезпечує таємницю та стійкість проти атак офлайн-словників. Виведенням SAE рукостискання WPA3 є Pairwise Master Key (PMK), який згодом використовується для виконання 4-х напрямного рукостискання для отримання клавیشі "Pairwise" ("PTK") [5].

1.3.4.1. Механізм роботи WPA3

AP утримує свої підтримувані пакети шифрів, тобто алгоритми автентифікації та шифрування, у надійному мережевому елементі безпеки (RSNE). RSNE включений не авторизовано в маяки які періодично передаються для реклами присутності мережі. Клієнти також використовують RSNE у запитах асоціацій, щоб повідомити AP про шифрові набори, які вони хочуть використовувати.

Спочатку рукостискання SAE узгоджує головний ключ (PMK), а потім чотиристороннє рукостискання отримує сеансовий ключ (PTK). Для підтримки сітчастих мереж було зроблено рукостискання SAE, щоб обидві сторони могли ініціювати його паралельно (отже, перехрещені стрілки).

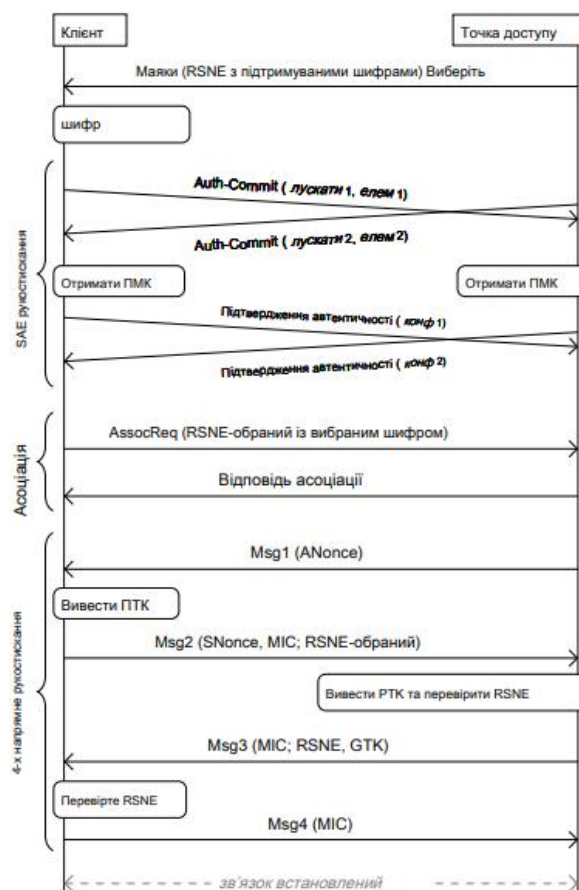


Рис 1.14. Підключення до AP за допомогою WPA3.

Сертифікація WPA3 передбачає підтримку рукостискання SAE. Це рукостискання вперше було введено Харкінсом у 2008 році, і було додане до стандарту 802.11 у 2011 році. Кілька близьких варіантів рукостискання SAE

також використовуються в інших протоколах. Термін Стрекоза (Dragonfly) зазвичай використовується для позначення цього сімейства рукописів.

Рукописання SAE - це врівноважений обмін ключами, підтверджений паролем (PAKE). Зауважте, що в збалансованому PAKE обидві кінцеві точки зберігають пароль в одному представленні (яке знаходиться в простому тексті при використанні SAE). Рукописання SAE приймає як вхід загальнодоступний секрет і виводить головний ключ Pairwise (PMK). Після виконання SAE, чотиристороннє рукописання використовується для узгодження клавіші сеансу під назвою PTK [5].

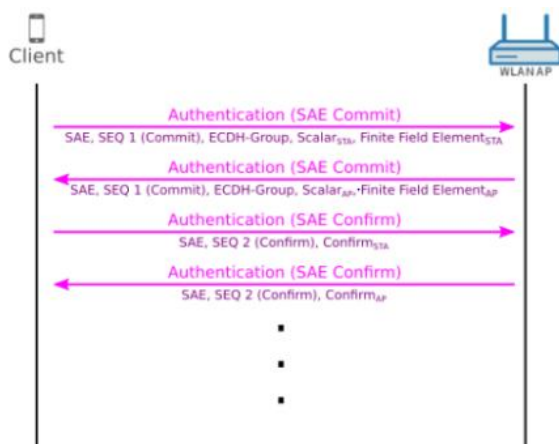


Рис. 1.15. Повідомлення автентифікації WPA3

```
> Frame 924: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
> IEEE 802.11 wireless LAN
  > Fixed parameters (104 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
    SAE Message Type: Commit (1)
    Group ID: 256-bit random ECP group (19)
    Scalar: 37a6fb24eb398c40f276bc2dd259aabd525859dd5a25faaf...
    Finite Field Element: 67bda0b0666db08b8b8ccf1934647sf09a8055d461ec161c46...
```

Рис. 1.16. Повідомлення SAE 1

```
> Frame 928: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
> IEEE 802.11 wireless LAN
  > Fixed parameters (104 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
    SAE Message Type: Commit (1)
    Group ID: 256-bit random ECP group (19)
    Scalar: 60962e7d30a0e7b4cf025333a7f1bcb836bde18194a124bc...
    Finite Field Element: 371bb8cac4f268af96755b08a106d8cf3c9accea93579d26d...
```

Рис. 1.17. Повідомлення SAE 2

```
> Frame 933: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
> IEEE 802.11 wireless LAN
  > Fixed parameters (40 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
    SAE Message Type: Confirm (2)
    Send-Confirm: 1
    Confirm: 9bd771c8a5d75f154101922d13cf78a6a70dd724c4606b3b...
```

Повідомлення SAE 1 - Користувач надсилає повідомлення AP в AP з його ідентифікатором групи, скаляром та новою точкою на Еліптичній кривій.

Повідомлення SAE 2 - AP відправляє своє повідомлення "Здійснювати" на пристрій користувача зі своєю скалярною та ECC точкою

Повідомлення SAE 3 - Користувач надсилає своє повідомлення

підтвердження до AP з маркером підтвердження

Рис. 1.18. Повідомлення SAE 3

```

> Frame 935: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
v IEEE 802.11 wireless LAN
  v Fixed parameters (40 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
    SAE Message Type: Confirm (2)
    Send-Confirm: 0
    Confirm: 4532733f7b8235dc35f4be485fe41b3faf461975a5ab8322...
  
```

Повідомлення SAE 4 - AP відповідає своїм підтвердженням та маркером, і тепер асоціація може статися, якщо був встановлений захищений канал.

Рис. 1.19. Повідомлення SAE 4

Рукописання SAE підтримує криптографію кінцевого поля (FFC), використовуючи мультиплікативні групи modulo a prime (групи MODP), і підтримує криптографію кривої еліптичної кривої (ECC), використовуючи групи еліптичних кривих modulo a prime (групи ECP). Саме рукописання складається з фази фіксації з наступною фазою підтвердження. Ці дві фази разом із супутніми еліптичними кривими операціями проілюстровані на рисунку 1.20. Зауважте, що рукописання може ініціюватись одночасно обома учасниками, що може статися в мережевих мережах після втрати з'єднання. Тим не менш, у більш широко використовуваному інфраструктурному режимі клієнт ініціює рукописання, відправивши свій кадр фіксації, а згодом AP відповість, використовуючи кадр фіксації та підтвердження. У свою чергу клієнт надсилає підтверджуючий кадр, завершуючи рукописання.

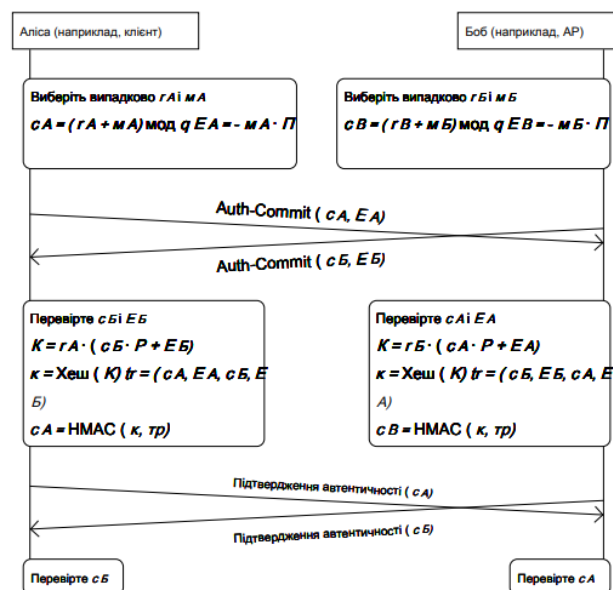


Рис 1.20. Деталі рукописання SAE.

1.4. Механізм доступу до середовища

Щоб створити всі умови для спільної роботи в мережі з великою кількістю пристроїв користувача без взаємних перешкод, було вирішено змінити стандартом спеціальний механізм їх переходу на режим передачі з попереднім повідомленням про передачу даних – множинний доступ з контролем несучої і запобіганням колізій (Carrier Sense Multiple Access with Collision Avoidance, CSMA / CA) [5]. CSMA розшифровується як множинний доступ з контролем несучої. Усі пристрої безпроводної мережі розпізнають, чи знаходиться мережа в режимі очікування. Тільки якщо середовище сприймається як недіюче, пристрій станції 802.11 може передавати кадр.

CA в CSMA / CA означає запобігання зіткнення. Пристрій WLAN не може одночасно передавати та приймати. Якщо середовище розпізнається як зайняте, то пристрій WLAN буде відключатись протягом деякого проміжку часу. Був розроблений алгоритм спеціального відключення, який визначає цей проміжок часу. Також до часу відключення, всі станції 802.11 ще використовують інший віртуальний механізм відключення, який називають векторним розподілом мережі (NAV). NAV – це тривалість часу. Ця тривалість отримується станцією 802.11 в останньому пакеті, який був виявлено станцією в ефірі. Тільки якщо тривалість NAV та таймер відключення відлічуються до нуля, а середовище можна вважати незайманим і може відбутись передача пакету в ефірі [14].

1.4.1. Фізичний рівень (Physical layer) 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 (Рисунок 1.21.).

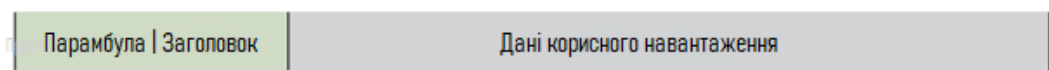


Рис. 1.21. Структура пакету фізичного рівня.

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. д.

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 [2]. 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.

1.4.2. MAC-рівень стандарту IEEE 802.11

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 мережею:

- PCF;
- DCF(розділяється ще на два підтипи);

1.5. Новизна розвитку сімейства IEEE 802.11

У травні 2019 року підгрупа BE (TGbe) Комітету 802.11 з питань стандартів локальних та міжміських мереж розпочала роботу над новим

стандартом Wi-Fi, що дозволить збільшити номінальну пропускну здатність до більш ніж 40 Гбіт / с на одному частотному каналі "типовий" для діапазону Wi-Fi ≤ 7 ГГц. Хоча багато документів посилаються на "максимальну пропускну здатність щонайменше 30 Гбіт / с", новий протокол фізичного рівня забезпечить номінальну швидкість понад 40 Гбіт / с.

Ще одна важлива сфера розвитку Wi-Fi 7-це підтримка додатків у реальному часі (ігри, віртуальна та доповнена реальність, управління роботами). Хоча Wi-Fi обслуговує аудіо- та відеотрафік особливим чином, довгий час вважалося, що гарантування низької затримки (одиниці мілісекунд) на рівні стандарту, також відоме як Time-Sensitive Networking , принципово неможливо у мережах Wi-Fi. Літом 2018 року була створена спеціальна підгрупа для подальшого вивчення цього питання. Оскільки підтримка додатків у реальному часі вимагає як високої номінальної швидкості передачі даних, так і розширеної функціональності шару зв'язку, робоча група 802.11 вирішила розробити методи підтримки додатків у режимі реального часу через Wi-Fi 7.

Важливим питанням, пов'язаним з Wi-Fi 7, є його співіснування із стільниковими технологіями (4G / 5G), які розробляються компанією 3GPP і працюють у тих самих неліцензійних діапазонах частот. Це LTE-LAA / NR-U. Для дослідження проблем, пов'язаних із співіснуванням Wi-Fi та стільникових мереж, IEEE 802.11 запустив Coexisting Standing Committee (Coex SC). Незважаючи на численні зустрічі та навіть спільний семінар учасників 3GPP та IEEE 802.11 у Вені літом 2019 року, технічні рішення ще не затверджені. Можливим поясненням цієї безрезультатної діяльності є те, що як IEEE 802, так і 3GPP неохоче змінюють власні технології, щоб привести їх у відповідність з іншою.

1.5.1. Етапи розробки.

Хоч процес розробки Wi-Fi 7 знаходиться на самій початковій версії, на даний час було майже близько 450 запропонованих нових функцій для майбутнього Wi-Fi 7, а також відомого, як IEEE 802.11be.



Рис.1.22. Етапи розробки стандарту IEEE 802.11be.

Значно планувалося, що розробка основних нових механізмів завершиться до березня 2021 року. Очікуваний варіант стандарту очікується до початку 2024 року. У січні 2020 року в підгрупі 11 буде виражена сповіщення темпу, буде розроблено відповідати графіці на нинішньому темпі роботи. Щоб прискорити процес розробки стандартів, підгрупа узгодила вибір невеликого набору високопріоритетних функцій, які можуть бути випущені до 2021 року (Випуск 1), а інші залишити у Релізі 2. Високопріоритетні функції повинні забезпечувати основну природну продукцію та включати в себе підтримку 320 МГц, 4K- QAM, очевидне покращення OFDMA від Wi-Fi 6, MU-MIMO с 16 потоками [11].

Через коронавірус група зараз очно не збирається, але регулярно проводить телеконференції, тому розробка затримується.

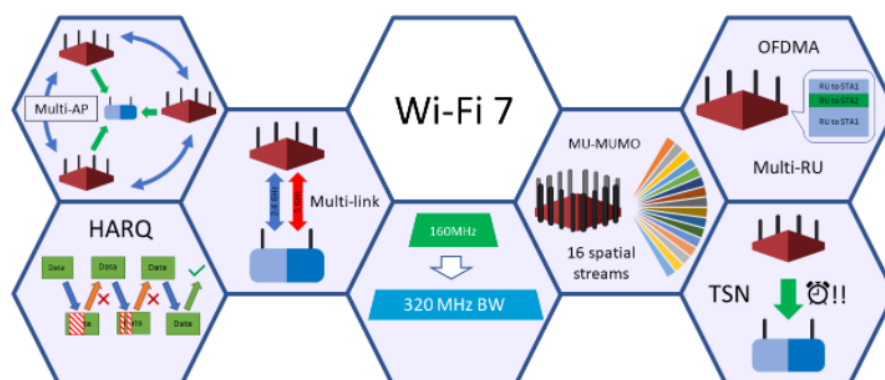


Рис.1.23. Ілюстрація новизни протоколу.

1.5.2. Новизна протоколу.

- Новий протокол фізичного рівня є розвитком протоколу Wi-Fi 6 з двократним збільшенням ширини смуги до 320 МГц, двократним збільшенням числа просторових потоків MU-MIMO, що збільшує номінальну пропускну здатність в $2 \times 2 = 4$ рази. Wi-Fi 7 також починає використовувати модуляцію 4K-QAM, що додає ще 20% до номінальної пропускну здатності. Таким чином, Wi-Fi 7 забезпечуватиме номінальну швидкість передачі даних в $2 \times 2 \times 1,2 = 4,8$ раз вище в порівнянні з Wi-Fi 6: максимальна номінальна пропускну здатність Wi-Fi 7 становить $9,6 \text{ Гбіт / с} \times 4,8 = 46 \text{ Гбіт / с}$.
- Введений в Wi-Fi 6 (802.11ax) OFDMA - метод доступу до каналу з поділом за часом і частоті (аналогічний тому, що використовується в мережах 4G і 5G) - надає нові можливості для оптимального розподілу ресурсів. Однак в 11ax OFDMA недостатньо гнучкий. По-перше, він дозволяє точці доступу виділяти для клієнтського пристрою тільки один ресурсний блок заздалегідь визначеного розміру. По-друге, він не підтримує пряму передачу між клієнтськими станціями. Обидва нестачі знижують спектральну ефективність. Крім того, відсутність гнучкості успадкованого від Wi-Fi 6 OFDMA погіршує продуктивність в щільних мережах і збільшує затримку, що критично для додатків реального часу. 11be вирішить ці проблеми OFDMA.
- Одним із затверджених революційних змін Wi-Fi 7 є вбудована підтримка одночасного використання декількох паралельних з'єднань на різних частотах, яка дуже корисна як для великих швидкостей передачі даних, так і для надзвичайно низької затримки.
- Використанням дуже широких каналів і великого числа просторових потоків призводить до проблеми високих накладних витрат, пов'язаних з процедурою оцінювання стану каналу, необхідної для MIMO і OFDMA.

- Нарешті, ще одним важливим нововведенням, але з неясною долею, є скоординована робота точок доступу.

Висновки

В першому розділі була розглянута класифікація технологій безпроводних мереж передачі інформації (БМПП). Було виявлено, що найпопулярнішою є безпроводних локальні мережах (WLAN - wireless local area network), тобто з Wi-Fi мережі, тому було розглянуто основні параметри та принципи роботи мережі. Основне призначення таких систем - розгортання безпроводних мереж усередині приміщень, хоча є випадки їх використання на відкритих майданчиках. Базова послуга - доступ в Internet або корпоративну мережу.

Було ознайомлено з стандартами безпроводних локальних мереж Wi-Fi, та був проведений аналіз нових стандартів сімейства IEEE 802.11. Розглянуто протокол Wi-Fi, що є новизною сімейства IEEE 802.11, імплементація та впровадження якого планується в найближчі роки.

Було розглянуто основний механізм та рівні доступу до мережі. Вивчена інформація допоможе зрозуміти основні принципи роботи цих мереж і визначити правильний підхід до подальшого розкриття теми.

РОЗДІЛ 2

АНАЛІЗ ПРОТОКОЛУ IEEE 802.11AX.

Wi-Fi став невід'ємним практично для всіх новітніх пристроїв. Поширення Wi-Fi різко підвищило попит на розширений інтерфейс користувача, що створює проблеми з пропускнуою спроможністю, затримкою і енергоефективністю. Зростаюче проникнення підключених пристроїв Wi-Fi і користувачів вимагає високошвидкісного підключення для різних використовуваних, наприклад, потокову передачу мультимедіа і спільне використання - незалежно від місця розташування.

У 2018 році група Wi-Fi Alliance анонсувала нову версію стандарту IEEE 802.11ax (Wi-Fi 6). У вересні 2019 року почалася програма сертифікації Wi-Fi 6 і асоціація стандартів IEEE ратифікувала його у вересні 2020 року. IEEE 802.11ax базується попередньому, актуальному стандарті 802.11ac (Wi-Fi 5, AC) і використовує вже відповідні технології. За словами розробників стандарту, деякі нові технології будуть корисні при розгортанні Wi-Fi-мереж з високою щільністю. Окремі рішення покращать якість зв'язку в умовах високого навантаження радіоефіру (наприклад, в громадському транспорті, торговельних центрах, готелях, на стадіонах або в корпоративних мережах).



Рис.2.1. Емблема стандарту IEEE 802.11ax.

Новий стандарт Wi-Fi 6 безумовно має ряд корисних нововведень і є черговим етапом розвитку мережевих технологій. Але перехід з Wi-Fi 5 на Wi-Fi 6 не виглядає таким проривним і значним для користувачів, як був перехід з 802.11n (Wi-Fi 4) на 802.11ac (Wi-Fi 5). Стандарт AC приніс користувачам можливість використання вільного діапазону частот 5 ГГц, багаторазове збільшення швидкості передачі даних, за рахунок збільшення ширини каналів і впровадження нових технологій Airtime Fairness і Beamforming. Згодом, коли користувачі оновлять свої пристрої, можна буде розраховувати на переваги нових технологій стандарту Wi-Fi 6, адаптація якого і впровадження поки тільки починаються.

2.1. Структура протоколу IEEE 802.11ax.

Пристрій повинен відповідати обов'язковим вимогам застарілих рівнів WLAN PHY. Це означає, що пристрій, що працює в діапазоні 2,4 ГГц, повинен відповідати вимогам IEEE802.11n PHY, а пристрій, що працює в діапазоні 5 ГГц, повинен відповідати IEEE802.11n і IEEE802.11ac PHY специфікації

Незважаючи на цю вимогу відповідності, у IEEE802.11ax є значні зміни порівняно з своїми попередниками. Однією з основних відмінностей є додана підтримка багатокористувацького MIMO (MU-MIMO) як у верхній, так і нижній лінії зв'язку, а також багатокористувацький доступ з ортогональним частотним поділом (OFDMA). Іншою зміною в IEEE802.11ax є час символу, який становить 12,8 мкс, що в чотири рази перевищує час застарілого символу в 3,2 мкс.

Три основні причини збільшення часу символу:

- Міцність зовнішніх каналів;
- Більша толерантність до тремтіння часу між користувачами в UL MU-MIMO/OFDMA;
- Вища ефективність у приміщенні (за рахунок зниження накладних витрат CP);

Поряд із збільшенням часу символів, IEEE802.11ax передбачає підтримку трьох часів циклічного префіксу(CP):

- 0,8 мкс: використання цього старого часу CP з довшим часом символу покращує ефективність, оскільки менше накладних витрат від CP;
- 1,6 мкс: орієнтована на високу ефективність у зовнішніх каналах та в приміщенні UL MU-MIMO/OFDMA;
- 3,2 мкс: цільова надійність у більш вимогливому випадку UL MU-MIMO/OFDMA;

Внаслідок більшого часу символів інтервал між піднесучими зменшується з 312,5 кГц до 78,125 кГц, а розмір ШПФ для смуги каналу 20 МГц збільшується з 64 до 256. Вузький інтервал між піднесучими забезпечує кращу вирівнювання і, таким чином, більшу надійність каналу. Хоча міг бути використаний більший розмір ШПФ, складність реалізації збільшується зі збільшенням ШПФ. Крім того, оскільки відстань між піднесучими стає меншою, корекція зсуву несучої частоти (CFO) повинна бути більш точною [12].

Таблиця 2.1.

Порівняння між IEEE 802.11ac та 11ax

	IEEE 802.11ac	IEEE 802.11ax
Пропускна здатність каналу (МГц)	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160
Відстань між піднесучими (кГц)	312.5	78.125
Час символу (мкс)	3.2	12.8
Циклічний префікс	0.8, 0.4	0.8, 1.6, 3.2
Модуляція	Нижній канал	верхній і нижній канали

Модуляція піднесучих даних	BPSK, QPSK, 16QAM, 64QAM, 256QAM	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM
Кодування	BCC (mandatory), LDPC (optional)	BCC (mandatory), LDPC (optional)

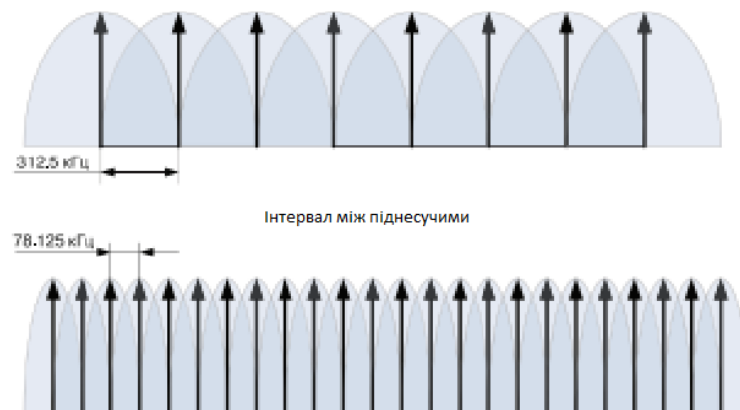


Рис. 2.2. Зміна інтервалу між несучими OFDM-сигналу у стандарті IEEE 802.11ax

2.1.1.Формати PPDU

IEEE802.11ax відрізняється від застарілих кадрів на рівні PHY, вводячи чотири нових формати PPDU (блок даних пакетного протоколу):

- Однокористувацький PPDU (HE_SU), який використовується при передачі одному користувачеві;
- Розширений діапазон PPDU (HE_EXT_SU). Це також призначено для передачі до одного користувача, але призначений для користувача, який може бути далі від точки доступу, наприклад в сценаріях на відкритому повітрі. HE_EXT_SU буде передаватися лише в каналі 20 МГц пропускної здатності. Крім того, HE_EXT_SU використовуватиме лише 1 просторовий потік і MCS0 (BPSK $\frac{1}{2}$), MCS1 (QPSK $\frac{1}{2}$) або MCS2 (QPSK $\frac{3}{4}$).
- Багатокористувацький PPDU (HE-MU), який передає одну або кілька передач одному або більше користувачів;
- PPDU на основі тригера HE (HE_Trig), який несе одну передачу і надсилається у відповідь на кадр тригера. Цей формат кадру надсилається

в передачах верхньої лінії зв'язку OFDMA та/або MU MIMO. Для передачі MU UL зазвичай потрібні налаштовані пристрої і може відповідати суворим вимогам щодо потужності та точності вимірювань. Проте специфікація IEEE 802.11 дозволяє реалізувати пристрої з широким діапазоном можливостей. Для розміщення пристроїв як високого, так і низького класу, пристрої, які підтримують HE_Trig, також повинні будуть оголосити, чи є вони класом А, який ретельно відкалібрований і може відповідати суворішим вимогам до потужності та точності вимірювань, або пристрій класу В, який є недорогим пристроєм з обмеженими можливостями та більш послабленими вимогами.

Хоча ще не визначено, чи буде потрібна підтримка повного PPDU для всіх цих форматів PPDU, усі пристрої повинні будуть розуміти преамбулу для всіх режимів передачі [24].

Таблиця 2.2.

Описи полів PPDU

Поле	Опис
L-STF	коротке поле для навчання
L-LTF	залишок довгого тренувального поля
L-SIG	застаріле сигнальне поле
RL-SIG	повторюване поле сигналу спадщини
HE-SIG-A	сигнал А поля
HE-SIG-B	сигнал В поля
HE-STF	короткий навчальний майданчик
HE-LTF	тривалий навчальний майданчик
Data	Дані
PE	поле розширення пакета
GI	охоронний інтервал
LTS	застаріла послідовність навчання

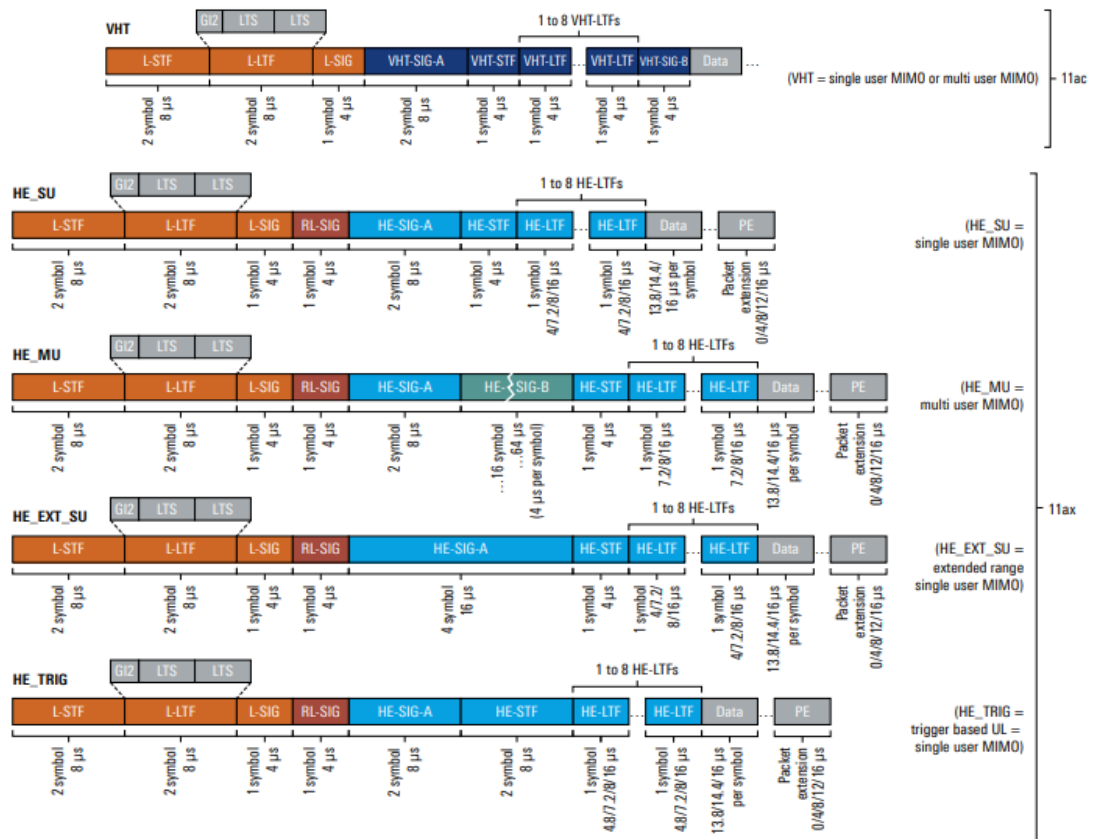


Рис.2.3. Застарілі формати PPDU та нові формати HE PPDU

2.1.2. Від одного користувача до кількох користувачів (MU)

Застарілі технології IEEE 802.11 використовували мультиплексування з ортогональним частотним розділенням (OFDM), де передача призначена для одного користувача. IEEE 802.11ac додає підтримку для передачі кільком користувачам у нижній лінії зв'язку за допомогою MU-MIMO, а IEEE 802.11ax також додає підтримку MU-MIMO верхнього каналу, а також додає OFDMA для кількох користувачів у верхній і нижній лінії зв'язку. Пристрої будуть потрібні для підтримки OFDMA у верхній і нижній лінії зв'язку, але, ймовірно, UL-MU-MIMO не буде потрібно для початкових пристроїв IEEE802.11ax [12].

У OFDMA ресурси розподіляються у двовимірних областях за часом і частотою, які називаються одиницею ресурсу. Таким чином, різні набори піднесучих сигналу OFDM виділяються різним користувачам, як показано на рисунку 2.4.

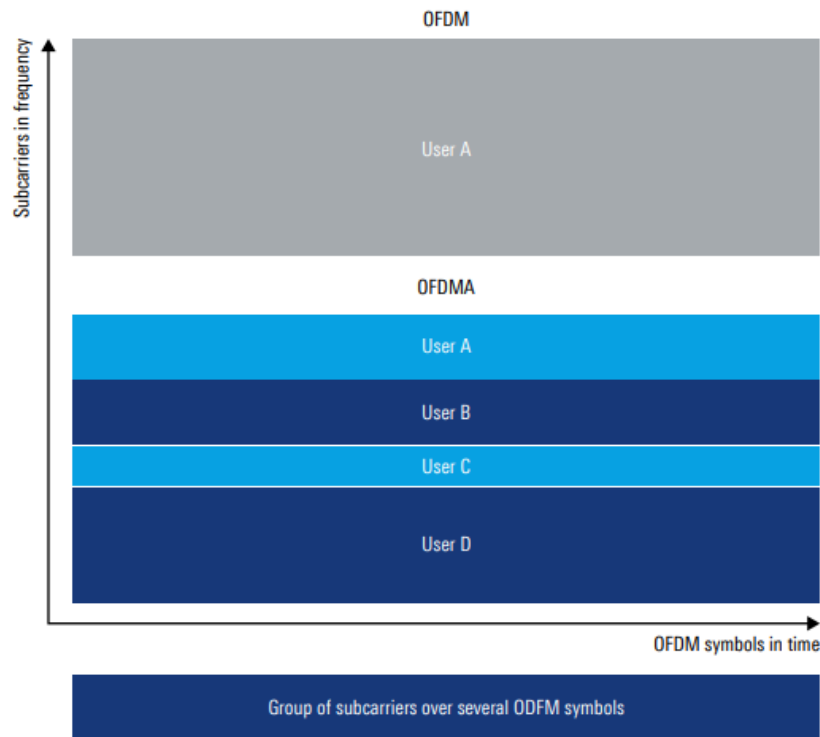


Рис.2.4. OFDM проти OFDMA

Розглянемо докладніше, як організована передача даних у висхідному та низхідному каналах за допомогою технології OFDMA. У разі передачі висхідному каналі кадр містить загальну для всіх одержувачів преамбулу, в якій зазначається інформація про призначення конкретних ресурсних блоків кожному з одержувачів.

Здійснення розрахованої на багато користувачів передачі висхідному каналі більш складне завдання так як передача виконується синхронно декількома користувачами, а точка доступу виступає в ролі координатора і визначає момент початку передачі. Для цього вона повинна отримати інформацію про дані для передачі та призначити ресурсні блоки передачі тим користувачам, які мають дані.

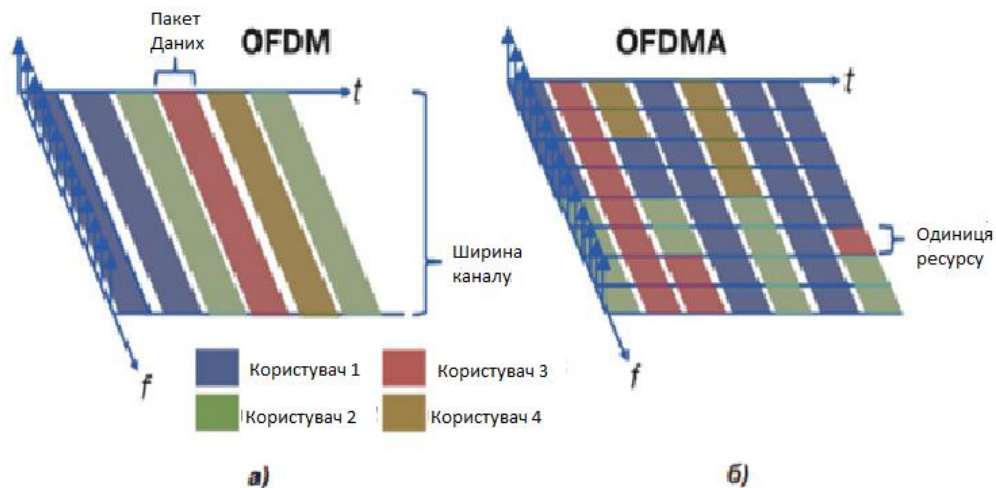


Рис.2.5. Один користувач, який використовує канал із використанням OFDM (а) та мультиплексування різних користувачів в одному каналі з використанням OFDMA (б)

Для інформування точки доступу про наявність даних для передачі користувачі періодично надсилають їй звіти. Такі звіти можуть мати різний ступінь деталізації, можуть відправлятися як за попереднім запитом точки доступу, і без нього. З урахуванням отриманої інформації точка доступу визначає тривалість передачі в висхідному каналі, розподіляє ресурсні блоки між користувачами та інформує їх про ці та інших необхідних параметрах (наприклад, про тривалості захисного інтервалу GI, який має бути однаковим для всіх користувачів при розрахованій на багато користувачів передачі у висхідному каналі) за допомогою відправки нового службового тригер-кадра (Trigger frame або просто Trigger) [24].

Для забезпечення синхронізації часу між передаючими пристроями розрахована на багато користувачів передача у висхідному каналі починається відразу після отримання тригер-кадра [21, 22].

Точка доступу також може ініціювати багато користувача систему у висхідному потоці, запитуючи інформацію зворотного зв'язку для формування променів від усіх, хто бере участь у передачі пристроїв користувачів.

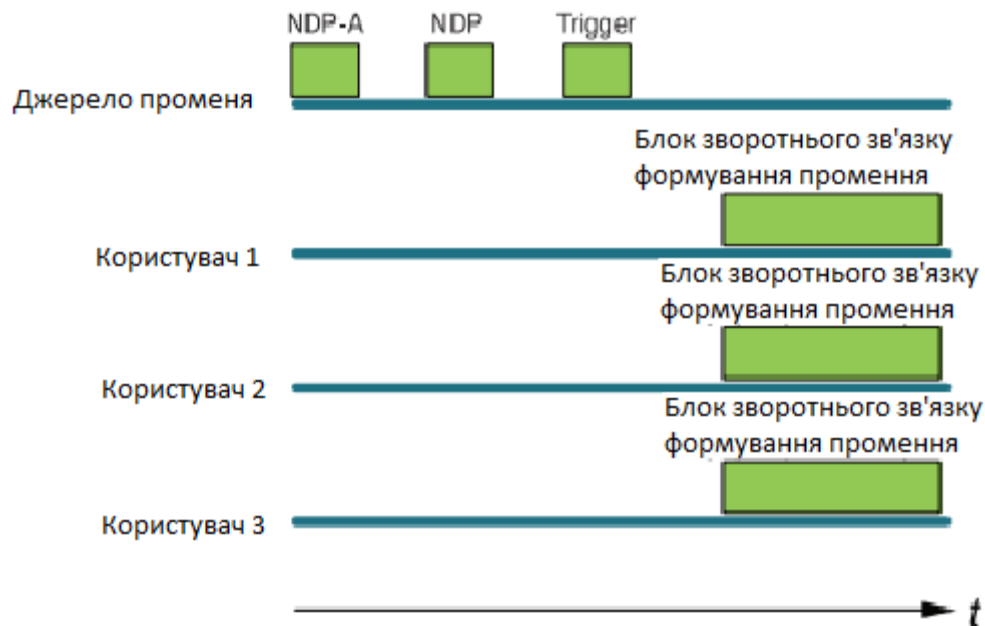


Рис.2.6. Формування діаграми спрямованості точки доступу за допомогою діаграмо утворювальних кадрів (beamforming feedback) для роботи MU-MIMO

IEEE 802.11ax використовує явну процедуру формування променя, аналогічну процедурі IEEE 802.11ac. Відповідно до цієї процедури формувач променя ініціює процедуру зондування каналу за допомогою Null Data Packet. Формувач діаграми спрямованості аналізує канал та формує блок зворотного зв'язку, що містить стислу матрицю зворотний зв'язок V для формування променя. Формувач променя використовує цю інформацію для обчислення матриці каналів H . Потім формувач променя може використовувати цю матрицю каналів для фокусування випромінюваної енергії по відношенню до кожного користувача.

Блок зворотного зв'язку формування променя (Beam forming feedback frame) вказує кількість для мандрівних потоків та/або розподіл OFDMA (частот та ресурсних блоків) кожного користувача. Він також містить інформацію управління потужністю передавача. Це необхідно для того, щоб зрівняти рівні сигналів, які отримує точка доступу від різних користувачів висхідної лінії зв'язку та покращити прийом кадрів від віддалених пристроїв. Точка доступу також інструктує всіх користувачів при запуску та припинення передачі. Як

показано на рисунку 2.7, точка доступу відправляє розрахований на багато користувачів тригер-кадр висхідної лінії зв'язку, який вказує всім користувачам точний момент, коли вони всі починають передачу і точної тривалості їх кадру, щоб гарантувати, що всі вони завершать передачу одночасно. Коли точка доступу отримує кадри від всіх користувачів, вона надсилає їм кадр підтвердження прийому кадрів (ACK) для завершення операції [23].

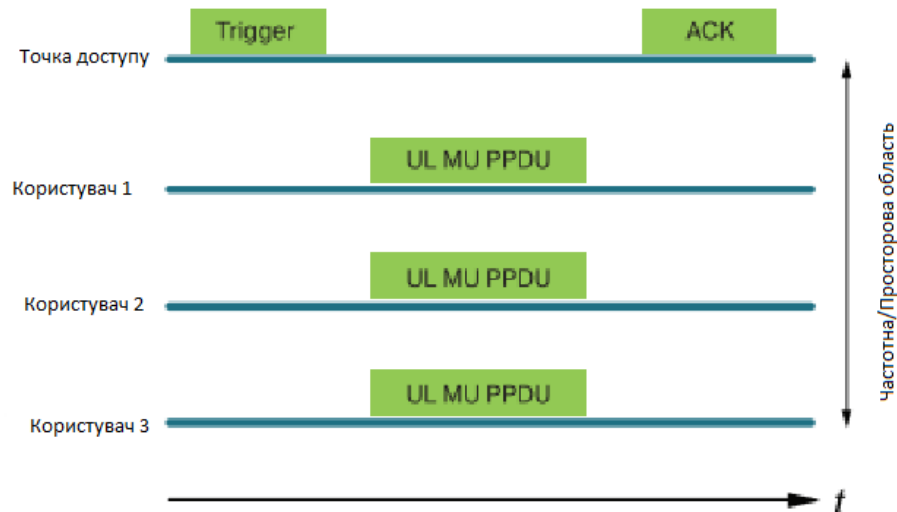


Рис.2.7. Координація розрахованої на багато користувачів операції верхньої лінії зв'язку

Зауважимо, що всі користувачі IEEE802.11ax OFDMA матимуть однаковий розподіл часу і закінчиться в той же час. У нижній лінії зв'язку це буде досягнуто шляхом додавання бітів доповнення до коротших пакетів і вимоги, щоб додаткові біти передавались на тому ж рівні потужності, що й частина даних пакета. Хоча це знижує ефективність, це полегшує виконання вимоги щодо зворотної сумісності із застарілими мережами IEEE 802.11. Це можна зрозуміти, згадавши, що застарілі пристрої можуть використовувати множинний доступ із визначенням несучих (CSMA), щоб визначити, чи є канал вільним для використання. Якщо, наприклад, у одного з користувачів був довший пакет, ніж у трьох інших користувачів, потужність сигналу, яка буде виявлена, коли залишок довшого пакету передається окремо, буде нижчою, ніж коли всі користувачі передають разом. У цьому випадку може визначити застарілий пристрій, що канал доступний і почати передачу. На додаток до

зворотної сумісності, це може зробити синхронізацію сигналів менш складною та зменшити кількість накладної інформації, необхідної в преамбулі. Ілюстрація DL OFDMA в часова область показана на рисунку 2.8.

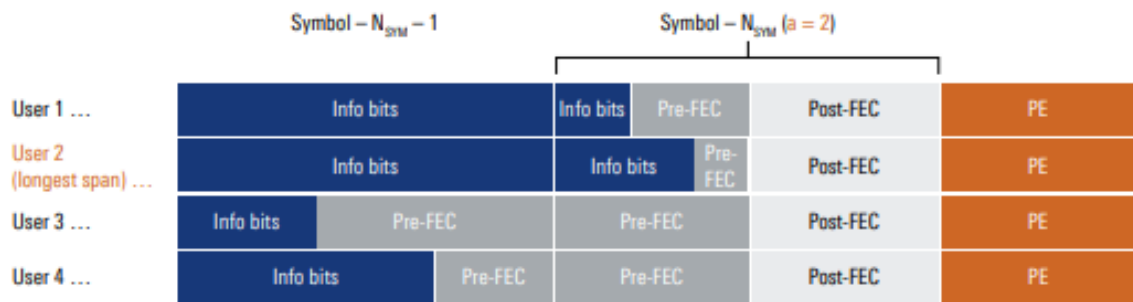


Рис.2.8. Приклад заповнення DL-OFDMA *a = a-фактор

У випадку верхньої лінії зв'язку MU точка доступу не знатиме, скільки даних мають передати окремі користувачі. Тому точка доступу використовує керуючий кадр, який називається тригерним кадром, щоб надати користувачеві інформацію про те, якої тривалості він би хотів, щоб пакет висхідної лінії зв'язку. Для розподілу частот OFDMA (DL і UL) одиниці ресурсів (RU) можуть містити 26, 52, 106, 242, 484 або 996 тонів (піднесучих) і знаходяться у фіксованих місцях. Тони в одиницях ресурсів є сусідніми та суміжними, за винятком середини каналу, де присутні нульові несучі постійного струму. Розташування 26-, 52-, 106-, 242-, 484- і 996-тональних одиниць ресурсу, які залежать від пропускної здатності каналу, показано на рисунку 2.9 (для 20 МГц), на рисунку 2.10 (для 40 МГц) і рисунку 2.11 (для 80 МГц). Зауважте, що, хоча розташування самих ресурсних одиниць фіксоване, можна мати комбінацію різних розмірів RU [24].

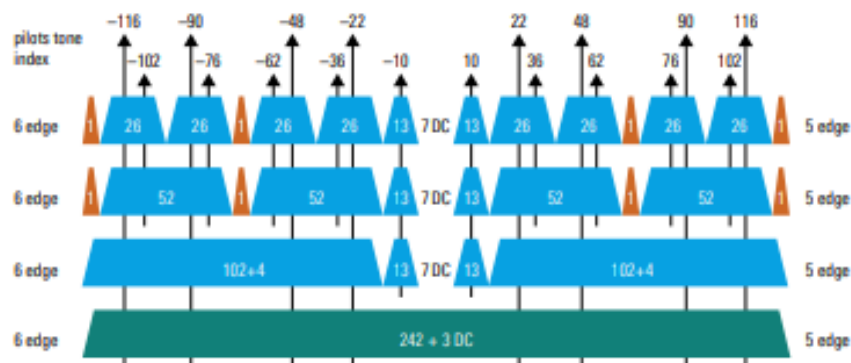


Рис.2.9. Одиниці ресурсу 20 МГц і розподіл тону

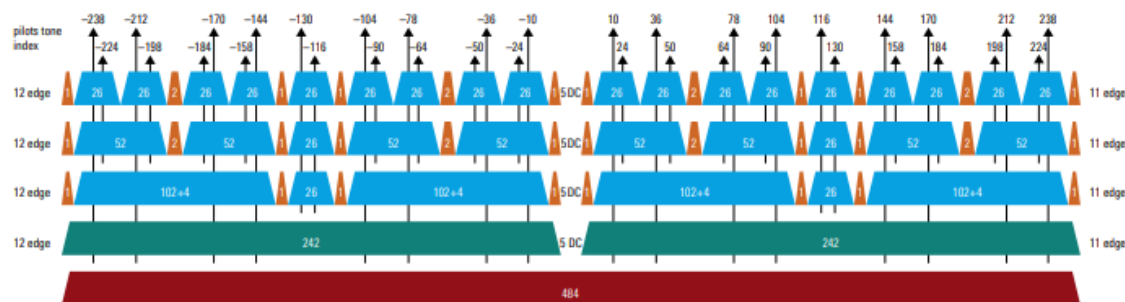


Рис.2.10. Блок ресурсів 40 МГц і розподіл тону

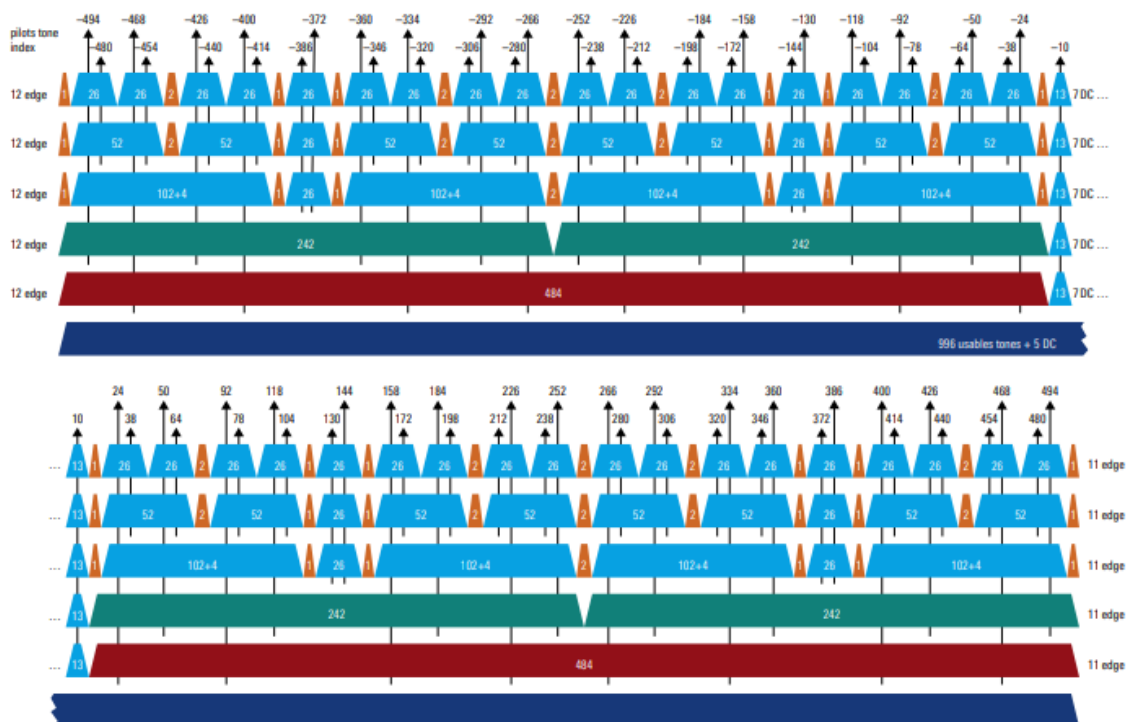


Рис.2.11. Блок ресурсів 80 МГц і розподіл тону

2.1.3. Типи піднесучих

2.1.3.1.Невикористані піднесучі

Присутні три типи піднесучих: піднесучі даних, пілотні піднесучі (для фазового формування та відстеження параметрів) та невикористані піднесучі. Невикористаними піднесучими є піднесучі постійного струму, піднесучі захисного діапазону та нульові піднесучі. Поки вони цього не роблять передачі інформації, ці невикористані піднесучі дійсно служать корисним цілям при передачі сигналу OFDMA. Є 11 піднесучих захисного діапазону на краях каналу для 20 МГц і 23 піднесучих захисного діапазону для випадків 40 МГц і

80 МГц, як показано на рисунках 2.9,2.10,2.11. Ці захисні смуги допомагають захистити від перешкод із сусідніх каналів.

Виконання обчислень (наприклад, у розподілі одиниці ресурсу 20 МГц: 256 піднесучих – 11 граничних піднесучих – 9 одиниць ресурсу $\times$ 26 піднесучих: $RU = 11$) показує, що в кожному блоці з 242 піднесучих є 11 неврахованих піднесучих. Ці 11 піднесучих не будуть передавати енергію. Кілька з 11 піднесучих були розумно розміщені, щоб служити роздільником між RU, особливо меншого розміру, щоб зменшити витік із сусіднього блоку (показаний помаранчевим на рисунках 2.9,2.10,2.11). Крім того, деякі з цих піднесучих використовуються як піднесучі постійного струму. Нульові піднесучі постійного струму важливі для відновлення сигналу OFDMA, особливо у випадку менших ресурсних одиниць поблизу постійного струму. У нижній лінії зв'язку додаткові піднесучі постійного струму допоможуть пом'якшити проблеми через витіку приймача і зміщення несучої частоти (CFO). У верхній лінії нульові піднесучі постійного струму є ще більш критичними, оскільки STA необхідно буде синхронізувати з несучою частотою точки доступу. Якщо компенсація частоти виконується в цифровій області, витік несучої може бути не в центрі переданої форми сигналу OFDMA, що може спричинити перешкоди тонам даних. AP не зможе відкалібрувати ці витіки несучої, коли отримає сигнал, оскільки не буде знати частоти або величину передач STA.

2.1.3.2. Піднесучі даних

Піднесучі даних в IEEE802.11ax використовуватимуть схеми модуляції та кодування (MCS) з IEEE802.11ac і долучають два нових MCS з 1024QAM. Чотири швидкості кодування, використані в IEEE802.11ac, були вивчені як можливості для 1024QAM MCS, а дві (3/4 і 5/6) було вибрано, оскільки 1024QAM з використанням двох інших швидкостей кодування (1/2 і 2/3) не дозволив збільшити пропускну здатність інформаційних бітів, яке вже можливо з MCS IEEE802.11ac. Два нових 1024QAM MCS - це MCS 10 і 11, і разом з 256QAM MCS 8 і 9, ймовірно, будуть необов'язковими. 1024QAM буде

використовуватися лише в ресурсних одиницях (RU), що мають 242 або більше тонів. У таблиці 2.3 наведено швидкість модуляції та кодування для IEEE802.11ax MCS.

Таблиця.2.3.

Індекси MCS IEEE 802.11ax

MCS	Модуляція	Швидкість кодування
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16QAM	1/2
4	16QAM	3/4
5	64QAM	2/3
6	64QAM	3/4
7	64QAM	5/6
8	256QAM	3/4
9	256QAM	5/6
10	1024QAM	3/4
11	1024QAM	5/6

На основі моделювання в більшості сценаріїв у приміщенні 1024QAM MCS вибирається з високою ймовірністю і призводить до збільшення середньої пропускної здатності понад 20%. Однак 1024QAM створює деякі додаткові проблеми для реального обладнання, наприклад:

- Нелінійність підсилювача потужності (ПА);
- Вищий коефіцієнт піку або відношення пікової та середньої потужності;
- Похибка квантування аналого-цифрового перетворювача (АЦП);
- Фазовий шум і дисбаланс I/Q гетеродина (LO);
- Ефект зміщення залишкової центральної частоти (CFO).

2.1.3.3.Пілотні піднесучі

Пілотні - це піднесучі, які передають відомий сигнал. Вони використовуються демодулятором OFDM для компенсації частотних помилок

тощо, і вони мають вирішальне значення для належної демодуляції прийнятого сигналу. Вони є важливою частиною трансмісії. Оскільки вони не передають інформації про дані, кількість пілотів має бути мінімальною, при цьому їх достатньо для належної демодуляції сигналу. Оскільки IEEE802.11ax підтримує кілька ширин смуг і розмірів одиниць ресурсів, групі IEEE802.11ax потрібно було ретельно продумати найкраще розташування для пілотів, щоб забезпечити якомога простіші вимоги щодо реалізації/обчислювальних запитів. Для досягнення цієї мети IEEE802.11ax використовуватиме пілотні сигнали, які фіксовані та вирівняні за місцем розташування для всіх розмірів розподілу ресурсів.

Щоб зрозуміти, що це означає, спрощена картина розміщення пілотів для 26- і 52-тональних ресурсних одиниць показано на рисунку 2.12. 26-тоновий RU використовуватиме 2 пілот-сигнали, а 52-тоновий RU використовуватиме 4 пілот-сигнали. Зауважте, що пілотні розташування для двох випадків вирівняні.

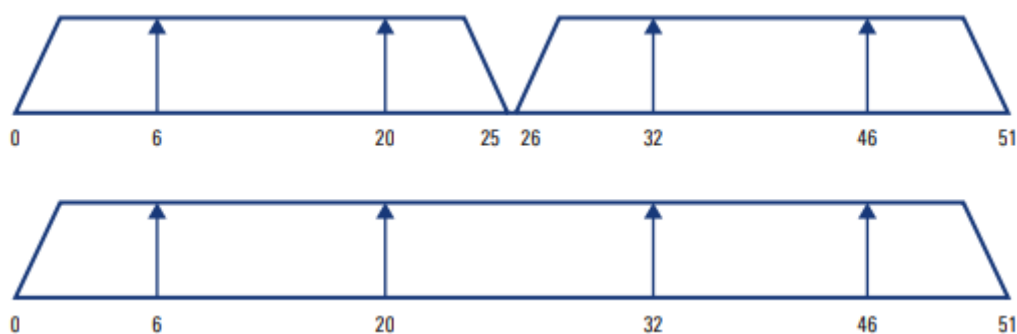


Рис.2.12. Пілоти IEEE 802.11ax для 26- та 52-тональних RU

Хоча можна здогадатися, що для 106-тонального випадку буде використано 8 пілотів, щоб відповідати пілотам у 52-тоновому RU, натомість дійсно потрібні лише 4 пілоти. Тому проводиться пілотне проколювання. Щоб визначити, який із 4 пілотів вирізати в 106-тоновому корпусі, необхідно було розглянути, як решта пілотів будуть узгоджені з 242-тональним випадком у пропускній здатності 80 МГц. В результаті вибір пілотів був зроблений так, щоб пілоти були більш рівномірно розподілені в 242-тоновому RU. Точні місця розташування пілотів можна знайти в таблиці 5 і побачити для різних RU для

смуги пропускання 20 МГц на рисунку 2.9, для смуги пропускання 40 МГц на рисунку 2.10 і для смуги пропускання 80 МГц на рисунку 2.11 [24].

Таблиця 2.4.

Індекси пілотного тону

Ширина каналу	Розмір RU	Індекси пілотного тону
20 MHz	26, 52	$\pm 10, \pm 22, \pm 36, \pm 48, \pm 62, \pm 76, \pm 90, \pm 102, \pm 116$
	106, 242	$\pm 22, \pm 48, \pm 90, \pm 116$
40 MHz	26, 52	$\pm 10, \pm 24, \pm 36, \pm 50, \pm 64, \pm 78, \pm 90, \pm 104, \pm 116, \pm 130, \pm 144, \pm 158, \pm 170, \pm 184, \pm 198, \pm 212, \pm 224, \pm 238$
	106, 242, 484	$\pm 10, \pm 36, \pm 78, \pm 104, \pm 144, \pm 170, \pm 212, \pm 238$
80 MHz	26, 52	$\pm 10, \pm 24, \pm 38, \pm 50, \pm 64, \pm 78, \pm 92, \pm 104, \pm 118, \pm 130, \pm 144, \pm 158, \pm 172, \pm 184, \pm 198, \pm 212, \pm 226, \pm 238, \pm 252, \pm 266, \pm 280, \pm 292, \pm 306, \pm 320, \pm 426, \pm 440, \pm 454, \pm 468, \pm 480, \pm 494, \pm 334, \pm 346, \pm 360, \pm 372, \pm 386, \pm 400, \pm 414,$
	106, 242, 484	$\pm 24, \pm 50, \pm 92, \pm 118, \pm 158, \pm 184, \pm 226, \pm 252, \pm 266, \pm 292, \pm 334, \pm 360, \pm 400, \pm 426, \pm 468, \pm 494$
	996	$\pm 24, \pm 92, \pm 158, \pm 226, \pm 266, \pm 334, \pm 400, \pm 468$

2.2. Цілі та задачі стандарту IEEE 802.11ax.

Стандарт IEEE 802.11ax спрямований на підвищення ефективності роботи мереж Wi-Fi у різних умовах. Особливо це важливо при створенні дротових мереж для стадіонів, аеропортів, вокзалів, виставкових залів, торгових центрів, де сотні точок доступу Wi-Fi працюють порівняно невеликий обмеженої області простору (Рис.2.13.). Подібне щільне розміщення бездротових мереж характерне і для житлових або офісних будівель. На сьогоднішній день у багатьох квартирах або офісах, як правило, є одна або навіть кілька точок доступу Wi-Fi.

При плануванні мереж 802.11ax передбачається наявність сильно неоднорідного трафіку, час як у попередніх версіях Wi-Fi, як правило,

враховувався лише один тип трафіку (наприклад, відеотрансляція у режимі реального часу, завантаження файлів або перегляд веб-сторінок). Ще однією особливістю IEEE 802.11ax є інтенсивне використання висхідного каналу у сучасних бездротових мережах. Це пояснюється численними завантаженнями фото, відео та документів у соціальні мережі та хмарні послуги.



Рис.2.13. Приклад об'єкта з високою щільністю користувачів

IEEE802.11ax використовуватиме ефективність спектра, пропускну здатність області та продуктивність для покращення націлювання на кілька моделей використання, включаючи:

- Аеропорти/залізничні вокзали;
- Електронна освіта;
- Громадський транспорт;
- Щільна багатоквартирна забудова;
- Вуличне розміщення Picocell;

Таблиця 2.5.

Цілі стандарту IEEE 802.11ax в порівнянні з IEEE 802.11ac.

802.11ac (2012)	802.11ax (2018)	Цілі проекту 802.11ax
Тільки 5 ГГц	Підтримка 2.4 і 5 ГГц	Поліпшити взаємодію пристроїв на 2.4 і 5 ГГц

802.11ac (2012)	802.11ax (2018)	Цілі проекту 802.11ax
Більш широкий канал (80 і 160 МГц)	Канал (80 і 160 МГц), OFDMA на прийом і передачу, Опція тільки 20 МГц для Інтернету Речей	Ширше канал - більше можливостей.
Покращена модуляція (256-QAM)	Покращена модуляція (1024-QAM)	Збільшити середню пропускну здатність станції як мінімум в 4 рази в середовищах з великою щільністю пристроїв
Додаткові потоки (до 8)	8 потоків, поняття "ресурсної одиниці"	Застосування: бездротові корпоративні офіси, вуличні Хот-споти, готелі, стадіони, концертні зали
Формування променя (явне), MU-MIMO в низхідному потоці	Формування променя (явне), перерозподіл просторових потоків, MU-MIMO в низхідному і висхідному потоці	Поліпшене енергозбереження на клієнтських пристроях
Зворотна сумісність 11a / b / g / n	Зворотна сумісність 11a / b / g / n / ac	Робота всередині приміщень і зовні

Висновки

В другому розділі було проаналізовано найактуальніший протокол сімейства IEEE 802.11 – IEEE802.11ax або як його називають в народі Wi-Fi6. Wi-Fi6 забезпечує нове покоління Wi-Fi для вирішення проблем із високою пропускну здатністю, низькою затримкою та високою перевантаженістю бездротового середовища. Wi-Fi 6 використовує такі технологічні досягнення, як висхідна та низхідна лінія зв'язку OFDMA, нові тривалості символів та функції з меншим енергоспоживанням, щоб забезпечити покращену взаємодію з користувачем при одночасному використанні старих пристроїв Wi-Fi.

РОЗДІЛ 3

МЕТОДИКА РОЗРАХУНКУ МЕРЕЖІ БЕЗДРОВОГО ДОСТУПУ WI-FI НА ОСНОВІ ПРОТОКОЛУ IEEE 802.11AX

Стандарти сімейства IEEE 802.11 Wi-Fi характеризуються стрімким розвитком номінальних швидкостей передачі даних: від архетипу сімейства 2 Мбіт/с IEEE 802.11 до гігабітних швидкостей останньої діючої версії IEEE 802.11 ac. Розвиток цих швидкостей були результатом покращення та розроблення швидших схем модуляції та кодування, ширших каналів та використання технологій MIMO. Однак подальше збільшення пропускної здатності Wi-Fi в успадкованому спектрі потребує нових підходів до доступу до каналу, а не використання старіших методів. Хоч і номінальна швидкість передачі даних є основною перевагою, вона не повністю характеризує продуктивність та ефективність розгортання W-Fi. На роботу мережі також впливають загасання і перешкоди, а також сценарії конфігурування мереж та неефективність доступу до середовища, тому пропускна здатність в більшості випадків не може бути основною вимогою.

Тобто, наразі потрібна методика, яка може найбільш коректно враховувати всі особливості доступу до мережі Wi-Fi. Метою являється розробка методики розрахунку ємності мережі та зменшення енергоспоживання мережею для нового стандарту IEEE 802.11 ax. Тому дане дослідження розіб'ємо на дві частини з описами методик розрахунку та моделюванням в Matlab.

3.1. Методика розрахунку пропускної здатності мережі стандарту IEEE 802.11ax.

Ще для розрахунку мереж Wi-Fi на основі стандарту IEEE 802.11 була запропонована аналітична модель для розрахунку пропускної здатності в залежності від кількості підключених пристроїв Джузеппом Біаначі [15].

В основу лягала ідея передачі даних в ідеальному каналі, де приховані вузли відсутні. Умова насичення мережі використовувалась для аналізу, а одиницею тимчасової шкали роботи мережі є віртуальний слот. Цей слот може бути трьох типів - «порожній», «успішний» та «колізійний». При порожньому слоті, кожна зі станцій не передає дані, і канал вільний. В успішному слоті

відбувається передача пакетів зі однієї із станцій. Колізійним же вважається слот коли передається з двох чи більше станцій. Станція, що передає виходить на передачу з однаковою ймовірністю τ . Головним припущенням є про постійну ймовірність зіткнення пакета p , переданого кожною станцією, незалежно від числа досконалих повторних передач. Поведінка окремих станцій описується Марківським ланцюгом, його граф представлено на рисунку 3.1.

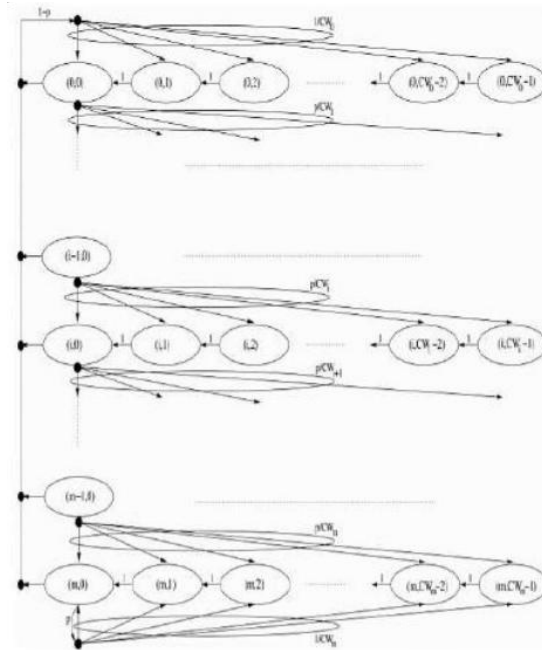


Рис.3.1. Граф поведінки окремих станцій.

На основі вищенаведених ланцюгів буде реалізовано системну модель для IEEE 802.11ax. В якості вихідних даних візьмемо мережу на основі стандарту IEEE 802.11ax, яка складається з однієї точки доступу і N станцій користувача. Усі станції перебувають у межах видимості ТД та інших станцій. Вони можуть передавати і приймати дані, використовуючи однакову схему модуляції і кодування, а також мають аналогічні параметри. Крім того, дотримуємось ідеї ідеальних умов каналу передачі фізично і концентруємося на рівні MAC.

Встановлюємо мінімальний розмір ресурсного блоку RU 242 піднесучих, що відповідає каналу 20 МГц. У кожному ресурсному блоці RU може бути виділено потоки MU-MIMO. Отже, з каналом 160 МГц і 8 антенами можна мультиплексувати до 64 одиночних станцій, виділяючи один просторовий потік для кожної станції. Для ТД та станцій передбачається модель з повним

буферним трафіком, вони завжди мають кадр, готовий до передачі [16]. При кожній передачі агрегованих елементів даних протоколу MAC (A-MPDU) MAC-кадри довжиною LD-бітів агрегуються та відправляються відповідно до схеми агрегації пакетів A-MPDU.

Для розрахунку ємності мережі потрібно не забувати про можливість виникнення колізій, тривалість цих колізій і успішність передачі кадру. Відповідно до вищезазначених умов, і ґрунтуючись на методиці розрахунку Фредеріко Біаначі, формула розрахунку пропускної спроможності каналу вниз буде рівна:

$$S_d = \frac{T_{data}}{T_{csi} + T_{data}} \times \left(\frac{a_1 * N_a * L_D * a_3 * V_u * N_a * L_D}{b_1 * T_e + \sum_{i=1}^4 a_i * (T_{ai} + T_e) + \sum_{i=1}^4 c_i * (T_{ci} + T_e)} \right), \#(3.1)$$

і для каналу вверх:

$$S_d = \frac{T_{data}}{T_{csi} + T_{data}} \times \left(\frac{a_2 * N_a * L_D * a_4 * V_u * N_a * L_D}{b_1 * T_e + \sum_{i=1}^4 a_i * (T_{ai} + T_e) + \sum_{i=1}^4 c_i * (T_{ci} + T_e)} \right) \#(3.2)$$

де:

$T_{a1} = T_{su}(V_s, B)$ - тривалість однокористувацької передачі вниз;

$T_{a2} = T_{su}(V_s, B)$ - тривалість однокористувацької передачі вгору;

$T_{a3} = T_{mu}(V_s, B)$ - тривалість розрахованої на багато користувачів передачі вниз;

$T_{a4} = T_{mu,u}(V_s, V_u, B_{ru})$ - тривалість розрахованої на багато користувачів передачі вгору;

$T_{c1} = T_{c4} = T_{c,su}$ - тривалість колізії для однокористувальних передач;

$T_{c2} = T_{c3} = T_{c,mu}$ - тривалість колізії для розрахованих на багато користувачів передач.

Успішні інтервали передачі та колізії включають порожній інтервал, оскільки в іншому випадку вузли не будуть здатними зменшити свій лічильник відкату/повернення. T_{data} враховує час, що використовується для зондування каналу.

Наступним етапом дослідження є апробування методики практично шляхом математичного моделювання в Matlab. У результаті розрахунків було отримано численні графіки з яких виділимо головні, щоб описати характер ємності. Виділимо графіки пропускної спроможності від:

- Кількості користувачів;
- Ширини каналу;
- Числа антен MIMO;

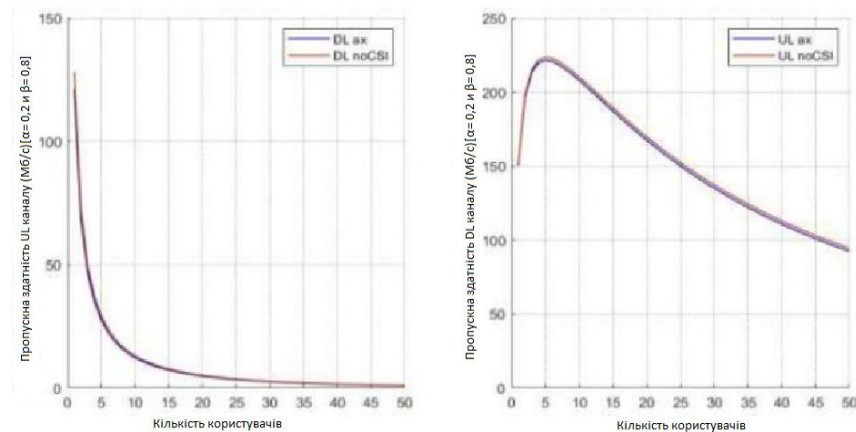


Рис.3.2. Залежність пропускної здатності від кількості користувачів.

Дані графіки зображають пропускну здатність DL та UL, досягнуту мережею на основі стандарту IEEE 802.11 ах ($\alpha=0,2$ та $\beta=0,8$). Як ми зможемо побачити, забезпечується більш висока пропускна здатність як для передачі вгору, так і для передачі вниз за рахунок збільшення кількості кадрів з 64 до 256, об'єднаних в одному A-MPDU та підтримки розрахованої на багато користувачів передачі за участю великої кількості станцій в порівнянні зі своїми попередниками сімейства IEEE 802.11. Відмітимо, що механізм прослуховування каналу не впливає на загальну продуктивність системи 802.11 ах. Це зумовлено тим, що станції користувача відправляють в ТД інформацію про стан каналу CSI паралельно, а не послідовно, як це робиться в IEEE 802.11ас, що для великої кількості станцій користувача призводить до значного скорочення тимчасових втрат [17].

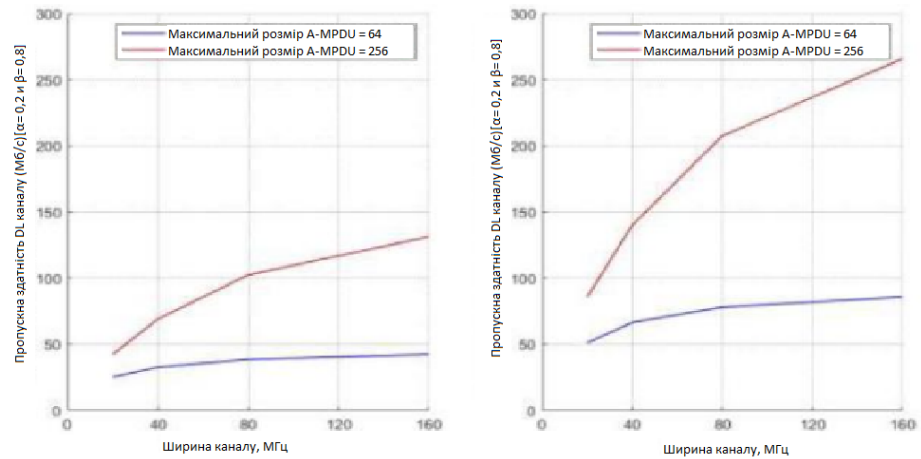


Рис.3.3. Залежність пропускної здатності від ширини каналу.

Дані графіки зображують пропускну здатність для DL і UL в залежності від ширини каналу. Пропускна здатність вгору та вниз збільшується зі збільшенням ширини каналу, що було очевидним. Також звернемо увагу на те, що пропускна здатність під час передачі вниз нижче для більш високих максимальних розмірів A-MPDU. Цей результат пояснюється операцією EDCA, яка дає однакові можливості передачі всім претендентам, при умові використання однакових параметрів CW_{min} та CW_{max} . Станції користувача здійснюють передачу протягом певних періодів часу, пропорційних максимальному розміру A-MPDU, збільшення цього значення зменшує кількість ефективного ефірного часу, виділеного для ТД. Отже, використання великих кадрів A-MPDU негативно впливає на продуктивність DL, і потрібен ретельний підхід до налаштування цього параметра.

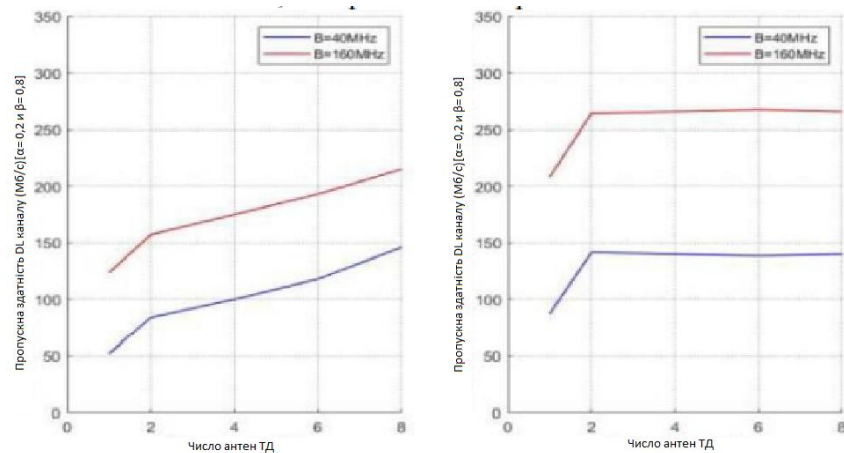


Рис.3.4. Залежність пропускної здатності від числа антен ТД.

Збільшення кількості антен на ТД дозволяє збільшити кількість просторових потоків, що використовуються в однокористувальних і розрахованих на багато користувачів передачах. На рисунку 3.4. показано, що пропускна здатність при передачі вниз збільшується зі збільшенням кількості антен в ТД, оскільки число станцій, мультиплексованих в кожному RU, збільшується пропорційно кількості просторових потоків, виділених кожному користувачеві в однокористувальних передачах. Щоправда, є обмежена кількість антен, встановлених на станціях користувача, рівне двом. Зазначимо, що виграш від збільшення кількості антен збільшується пропорційно до ширини каналу.

Отримані результати показують, як працюють мережі на основі стандарту IEEE 802.11ah для різних конфігурацій, таких як вплив на пропускну здатність мережі швидкості прослуховування каналу, максимального розміру A-MPDU, ширини каналу та кількості антен на точці доступу. Доведено необхідність конфігурування точних пріоритетів при плануванні ТД розрахованих на багато користувачів передач для DL і UL для уникнення колізій з станціями користувача та оптимізації пропускної здатності WLAN. В дослідженні було запропоновано модель сегмента мережі стандарту IEEE 802.11ah, яка враховує тимчасові витрати фізичного та каналного рівня доступу до каналу. Також в моделі було враховано, що при розрахунку пропускної здатності каналу в мережі стандарту IEEE 802.11ah потрібно розглядати як однокористувацькі, так і багатокористувацькі сценарії передач в каналах вниз і вгору. Недоліком даного дослідження є те, що не враховуються втрати, що виникають фізично, а також ефекти різноманітного трафіку. Крім того, ряд припущень, таких як рівновіддаленість усіх станцій, відсутність прихованих вузлів та умова насичення мережі може також змінити загальну пропускну здатність мережі.

3.2. Алгоритм підвищення енергоефективності механізму енергозбереження IEEE 802.11ah

Розглянемо повністю підключену мережу Wi-Fi на основі IEEE 802.11ах, де є точка доступу, яка обслуговує M користувачів. Ми припускаємо випадкове посилення каналу між AP і STA, яке є незалежним у часі та STA. Оскільки на практиці доступний лише дискретний кінцевий набір схем F модуляції та кодування MCS, може підтримуватися лише фіксований набір швидкостей передачі даних, позначений як $R = r_1, r_2, \dots, r_F$. Завдяки новому механізму сну та енергозбереження, запровадженому в IEEE 802.11ах, кожна STA і AP узгоджують загальний набір параметрів і STA можуть прокидатися лише в зазначений час, щоб мінімізувати споживання енергії. Далі ми пояснюємо два важливі параметри TWT, які є найбільш релевантними для цієї роботи та також представлені на рисунку 3.5:

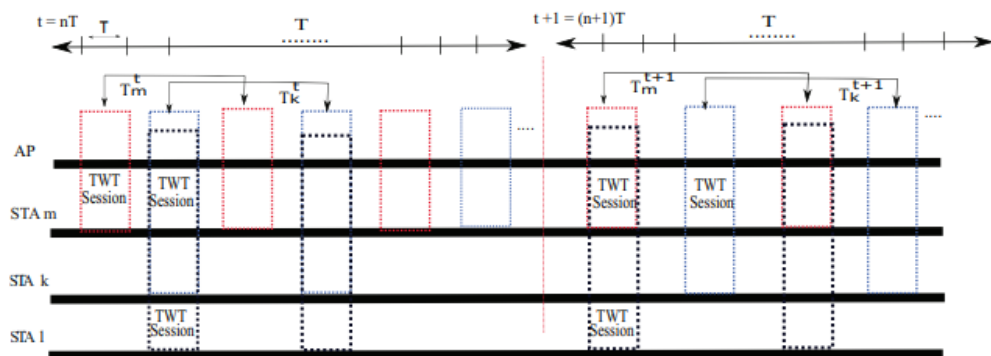


Рис.3.5. Динамічне призначення інтервалу TWT.

- Перший з них це сеанс TWT: тривалість часу (у секундах), протягом якого STA прокидається та отримує чи передає дані. Передбачається, що він однаковий для всіх STA і позначається як t_{up} .
- Другий - інтервал TWT: інтервал часу між двома послідовними часами пробудження STA. Точніше, STA періодично прокидаються, щоб їх обслуговувати AP. Ми розглядаємо окремі TWT, з якими різні STA можуть мати різну періодичність залежно від їхнього трафіку та вимог до застосування. На відміну від попередніх досліджень ця періодичність не є статичною, а може змінюватися динамічно за погодженням STA та AP. Зокрема, на початку епохи, яка починається з $t = nT$

де $n = 1, 2, \dots$, визначається інтервал пробудження TWT STA m , що позначається як T_m^t . Потім STA m прокидається при кожному T_m^t до наступної епохи. Кожна епоха триває T секунд, де $T > T_m^t$ для всіх t і m . На початку наступної епохи T_m^t за потреби оновлюється.

Наприклад, як показано на рисунку 3.5., інтервал пробудження TWT для STA m на початку епохи n (тобто в момент $t = nT$) дорівнює T_m^t . Однак у наступну епоху $t+1 = (n+1)T$ встановлюється на $T_m^{t+1} > T_m^t$, а STA m має меншу кількість сеансів TWT і більше часу для сну. Щоб зобразити інтеграцію багатокористувацьких можливостей у TWT, ми також показуємо на рисунку 3.5., що STA k і STA l мають однаковий інтервал TWT на час і прокидаються в один і той же час.

Інтервал пробудження TWT приймає значення із попередньо визначеного дискретного набору, $T_m^t \in \{T_1, T_2, \dots, T_L\}$ для всіх m і t . Для заданого T_m^t кількість сеансів TWT, які може використовувати STA m під час $t = nT$ (за епоху n), задається як:

$$N_m^t = \left\lfloor \frac{T}{T_m^t} \right\rfloor \quad \#(3.3)$$

де $\left\lfloor \frac{T}{T_m^t} \right\rfloor$ — найбільше ціле число, менше за $\frac{T}{T_m^t}$. Оскільки T_m^t приймає лише дискретні значення зі скінченної множини, T як системний параметр, а набір $\{T_1, T_2, \dots, T_L\}$ можна вибрати так, що $N_m^t = \frac{T}{T_m^t}$. Припустимо, що кожна T секунд розділена на міні-слоти, позначені як τ , $\tau \in \{0, 1, 2, \dots\}$, а τ — кратне ціле число всіх можливих значень T_m^t . Вважаємо, що τ дорівнює t_{up} .

Визначимо споживання енергії для STA m в міні-часовий інтервал τ . Зауважимо, що коли STA m прокидається, він стає активним на тривалість t_{up} секунд. t_d і t_u — це частки t_{up} , які використовуються для передачі по нижній і верхній лінії відповідно. Крім того, енергоспоживання під час нижнього та верхнього зв'язку позначається як P_d і P_u відповідно. Тоді загальне споживання енергії протягом одного сеансу TWT (наприклад, міні-слот τ) визначається як:

$$E_s = P_d \times t_d t_{up} + P_u \times t_u t_{up} \quad \#(3.4)$$

Зверніть увагу, що коли $\tau = iT_m^t$, де $i > 0$ — ціле число, STA m прокидається, щоб почати сеанс TWT. Коли $\tau \neq iT_m^t$, STA m перебуває в режимі сну. Споживання енергії STA m на міні-слоті τ визначається як:

$$E_m(\tau) = \begin{cases} E_s & ; \text{якщо } \tau = iT_m^t \\ E_{sleep} & ; \text{інші} \end{cases} \quad \#(3.5)$$

де E_{sleep} — це енергія, споживана в сплячому режимі за τ секунд, а $E_{sleep} = P_{sleep} \times \tau$, де P_{sleep} — споживання енергії в режимі сну.

Протягом періоду n , починаючи з $t = nT$, існує N_m^t кількість сеансів TWT для STA m . Таким чином, STA m споживає кількість енергії E_m^t за період n , де:

$$\sum_{\tau=1}^{\frac{T}{\tau}} E_m(\tau) = E_m^t = E_s \times N_m^t + \left(\frac{T}{\tau} - N_m^t\right) E_{sleep} \quad \#(3.6)$$

де $\left(\frac{T}{\tau} - N_m^t\right) E_{sleep}$ — загальне споживання енергії STA m у сплячому режимі, оскільки є $\left(\frac{T}{\tau} - N_m^t\right)$ міні-слоти для сну протягом періоду. Тоді середнє за часом споживання енергії для всіх STA визначається наступним чином:

$$E_{avg} = \lim_{t \rightarrow \infty} \sup \frac{1}{S} \sum_{t=0}^{t-1} \sum_{m=2}^M E[E_m^t] \quad \#(3.7)$$

У кожному міні-слоті τ дані надходять до черги кожної з STA. Нехай $A_m(\tau)$ — кількість даних (тобто вхідних бітів), що надходять до черги STA m у слоті τ . Припустимо, що $A_m(\tau)$ є стаціонарним процесом і він незалежний від STA та часових інтервалів. Позначимо вектор швидкості надходження як $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_M)$, де $\lambda_m = E[A_m(\tau)]$. Нехай $Q(\tau) = (Q_1(\tau), Q_2(\tau), \dots, Q_M(\tau))$ позначає вектор розмірів черги, де $Q_m(\tau)$ — довжина черги користувача m у часовий інтервал τ . Черга буде дуже стабільною, якщо:

$$\lim_{S \rightarrow \infty} \sup \frac{1}{S} \sum_{t=0}^{S-1} E(Q_m(\tau)) < \infty \quad \#(3.7)$$

Більше того, якщо кожна черга в мережі є стабільною, то мережа називається стабільною. Динаміка черги STA m є:

$$Q_m(\tau) = \max[Q_m(\tau) - R_m(\tau), 0] + A_m(\tau) \quad \#(3.8)$$

Важливо, що швидкість передачі $R_m(\tau)$ може приймати додатне значення, тобто $R_m(\tau) > 0$ у моменти часу $\tau = iT_m^t$, оскільки STA m прокидається лише в цих випадках. Коли $\tau \neq iT_m^t$, то $R_m(\tau) = 0$. Λ позначає область пропускну здатності мережі, яка є найбільшим можливим набором швидкостей λ , який може підтримуватися спільним алгоритмом планування та призначення інтервалу TWT із забезпеченням стійкості мережі, $\lambda \in \Lambda$.

Оскільки багатокористувацькі можливості передачі 802.11ax покращуються завдяки введенню OFDMA та MU-MIMO у верхній лінії зв'язку, інтервалу TWT можна призначити більше однієї STA. Припустимо, що щонайбільше K STA можуть використовувати один і той же інтервал TWT, і нехай $N_{T_l}(t)$ — кількість STA, які призначаються інтервалу TWT T_l у момент часу t , $l \in \{1, 2, \dots, L\}$. Таким чином, загалом до $L \times K$ STA можуть мати інтервал TWT, призначений для кожної епохи. З нашою установкою керуючим рішенням мережі для STA m є конфігурування T_m^t .

Тобто на початку кожного часу t мережа визначає інтервал пробудження TWT для кожної STA. Отже оглянемо наступну задачу оптимізації:

$$\begin{aligned} & \min E_{avg} \\ & \text{s. t. : 1) Стабільність мережі} \\ & \quad 2) T_m^t \in \{T_1 + T_2, \dots, T_L\} \forall t, m \\ & \quad 3) N_{T_l}(t) \leq K \quad \forall l \in \{1, 2, \dots, L\}, \forall t \quad (3.9) \end{aligned}$$

Обмеження №2 гарантує, що інтервал TWT, визначений для STA m , приймає значення із попередньо визначеного дискретного набору. Крім того, третє обмеження в гарантує, що максимум K STA можна призначити інтервалу TWT. На початку кожного періоду система визначає інтервал пробудження TWT для $L \times K$ кількості STA, а інші STA можуть переходити в режим сну протягом цілих T секунд для економії енергії [18].

Задача (3.9) спрямована на мінімізацію загального середнього споживання енергії STA шляхом правильного вибору інтервалу пробудження TWT з урахуванням умов їх руху. Від дослідження очікується, що при розв'язанні проблеми необхідно досягти балансу між споживанням енергії та

розміром черги. Іншими словами, коли стан каналу хороший і розмір черги великий, це може зменшити інтервал TWT, а коли розмір черги низький, він віддає перевагу більшому інтервалу TWT для більшої економії енергії. Це є задачею стохастичної оптимізації, і далі я пропоную її рішення на основі методики оптимізації Ляпунова.

3.2.1. Спільний інтервал TWT і алгоритм планування (JTWSA)

Ми використовуємо інструменти дрейфу та оптимізації Ляпунова, що дає нам змогу разом вирішувати проблеми оптимізації продуктивності та стабільності мережі в єдиній структурі. Інструмент оптимізації Ляпунова дозволяє одночасно мінімізувати дрейф (тобто стабілізувати мережу) і оптимізувати задану мету (тобто мінімізувати енергію). Щоб використовувати цей інструмент, спочатку визначається функція Ляпунова:

$$L(Q(t)) \triangleq \frac{1}{2} \sum_{m=1}^M Q_m^2(t) \quad \#(3.10)$$

Функція Ляпунова виступає інструментом вимірювання загальних розмірів черги в мережі. Іншою важливою концепцією в цій структурі є дрейф Ляпунова, який вимірює, наскільки очікувані значення розмірів черги змінюються в межах одного слоту. Тут ми використовуємо умовний дрейф Ляпунова T-слоту, який є очікуваною зміною функції Ляпунова над T слотами, який визначається так:

$$\Delta T(t) \triangleq E \{L(Q(t+T)) - L(Q(t)) | Q(t)\} \quad \#(3.11)$$

Щоб стабілізувати мережу, ми повинні переконатися, що дрейф не росте безкінечно, і, отже, кінцевою метою є мінімізувати дрейф для отримання стабільної мережі. Для більш доступного аналізу визначається верхня межа для дрейфу, а потім ця межа мінімізується. Для того, щоб разом обробляти стабільність мережі та об'єктивну оптимізацію, використовується метод штрафу «дрифт плюс». За допомогою цього методу наш штраф $V \sum_{m=1}^M = 1 E[E_m^t | (Q(t))]$ додається до дрейфу:

$$\Delta T(t) + V \sum_{m=1}^M E[E_m^t | Q(t)] \quad \#(3.12)$$

де V – контрольний параметр між затримкою черги та середнім системним штрафом. Тепер у рамках оптимізації Ляпунова ми перетворюємо нашу задачу мінімізації енергії та стабільності мережі на мінімізацію (3.12). Ми спочатку виводимо верхню оцінку для (3.12), а потім пропонуємо наш алгоритм, який мінімізує межу.

Враховуючи $V > 1$ і в момент $t = nT$, для будь-якого можливого керуючого рішення $(T_1^t, T_2^t, \dots, T_M^t)$, ми маємо таку оцінку:

$$\Delta T(t) + V \sum_{m=1}^M E[E_m^t | Q(t)] \leq B_1 + E \left[\sum_{\tau=t}^{t+T-1} \sum_{m=1}^M Q_m(\tau) A_m(\tau) | Q(t) \right] - E \left[\sum_{\tau=t}^{t+T-1} \sum_{m=1}^M Q_m(\tau) R_m(\tau) - V \sum_{m=1}^M E_m^t | Q(t), \right] \quad \#(3.13)$$

де $B_1 = \frac{MT(R_{max}^2 + A_{max}^2)}{2}$;

Доведення починається з визначення верхньої межі дрейфу Ляпунова, наведеного в (3.11), використовуючи такий факт: для користувача m виконується нерівність:

$$Q_m^2(t+1) - Q_m^2(t) \leq R_m^2(t) + A_m^2(t) + 2Q_m(t)[A_m(t) - R_m(t)] \quad \#(3.14)$$

Підводячи (3.14) за $[t, t+T-1]$ і знаючи, що $R_m(t) \leq R_{max}$ і $A_m(t) \leq A_{max}$ для всіх m і t , отримуємо:

$$Q_m^2(t+T) - Q_m^2(t) \leq TR_{max}^2 + TA_{max}^2 - 2 \sum_{\tau=t}^{t+T-1} \sum_{m=1}^M Q_m(\tau)[R_m(\tau) - A_m(\tau)] \quad \#(3.15)$$

Тоді, взявши умовне очікування (14) щодо $Q(t)$ і підсумувавши всіх користувачів і розділивши на $1/2$, отримаємо:

$$\Delta T(t) \leq B_1 - E \left[\sum_{\tau=t}^{t+T-1} \sum_{m=1}^M Q_m(\tau)[R_m(\tau) - A_m(\tau)] | Q(t) \right] \quad \#(3.16)$$

Нарешті, ми додаємо штрафну частину $V \sum_{m=1}^M E[E_m^t | Q(t)]$ до обох частин (3.16) і, переставляючи отримані доданки, отримуємо оцінку в (3.13). На цьому доведення закінчено.

Структура оптимізації Ляпунова тепер допомагає вирішити нашу основну проблему, знайшовши алгоритм, який мінімізує праву частину (R.H.S - right

hand side) межі (3.13). Очевидно, що рішення наступної задачі мінімізує R.H.S [19].

Проблема 1:

$$\max_{T_1^t, T_2^t, \dots, T_M^t} E \left[\sum_{\tau=t}^{t+T-1} \sum_{m=1}^M Q_m(\tau) [R_m(\tau) - A_m(\tau)] - V \sum_{m=1}^M E_m^t |Q(t) \right] \#(3.17)$$

Однак розв'язання задачі 1 вимагає попереднього знання розміру черги та швидкості передачі STA, тобто майбутньої інформації. Ми апроксимуємо майбутні розміри черги як поточне спостереження, тобто $Q_m(\tau) = Q_n(t)$ для всіх $\tau \in [t, t + T - 1]$ для всіх STA m , і тепер ми прагнемо максимізувати наступну проблему:

$$\max_{T_1^t, T_2^t, \dots, T_M^t} E \left[\sum_{\tau=t}^{t+T-1} \sum_{m=1}^M Q_m(\tau) R_m(\tau) - V \sum_{m=1}^M E_m^t |Q(t) \right] \#(3.18)$$

Тепер для вирішення цієї проблеми потрібна лише інформація про розмір черги на початку $t = nT$, але вона потребує майбутньої швидкості передачі протягом T секунд. На щастя, для WLAN час когерентності каналу досить тривалий, оскільки STA зазвичай нерухомі, а мобільність низька. Крім того, швидкість передачі можна оцінити за допомогою передових методів машинного навчання. Припустимо, що швидкість передачі змінюється кожні T секунд, тому проблема зводиться до наступної детермінованої оптимізаційної задачі наступним чином [20]:

$$\max_{T_1^t, T_2^t, \dots, T_M^t} \sum_{m=1}^M Q_m(t) R_m(t) N_m^t - V E_m^t \#(3.19)$$

Використовуючи (3.6), ми можемо переписати (3.19) як:

$$\max_{T_1^t, T_2^t, \dots, T_M^t} \sum_{m=1}^M Q_m(t) R_m(t) N_m^t - V N_m^t (E_s - E_{sleep}) \#(3.20)$$

JTWSA вирішує цю задачу:

Вхідні дані: $V, P_d, P_u, P_{sleep}, t_{up}$. При кожному $t = nT$ робимо:

- Крок 1. Серед усіх користувачів, знайдемо:

$$S(t) = \operatorname{argmax} - (L \times K) \{Q_m(t) R_m(t) - V(E_s - E_{sleep})\} \#(3.21)$$

де $\text{argmax} - (L \times K)$ — операція вибору перших $L \times K$ елементів набору дійсних чисел відсортовано в порядку зменшення.

- Крок 2: Призначимо інтервали TWT $T_1, T_2, \dots, T_L$, відсортовані в порядку зростання, до STAs в $S(t)$, якщо тільки $Q_m(t)R_m(t) > V(E_s - E_{sleep})$. Наприклад, інтервал TWT перших K STA в $S(t)$ встановлюється на T_1 , для наступних K STA в $S(t)$ він встановлюється на T_2 і так далі. Якщо інтервалу TWT присвоєно кількість STA, це K , переходимо до наступного інтервалу TWT.

- Якщо $Q_m(t)R_m(t) < V(E_s - E_{sleep})$, встановлюємо інтервал TWT для цього STA m на T .

- Крок 3: Після визначення T_m^t для кожної STA виконаємо операцію передачі/отримання та оновимо чергу до наступного $t = (n + 1)T$.

Оскільки JTWSA оптимально мінімізує R.H.S (3.13), ми маємо наступну теорему, яка описує та показує продуктивність JTWSA.

Теорема 1 (Оптимізація Ляпунова) Припустимо, що λ — внутрішня точка в $\mathcal{A}$, тоді існує константа $\epsilon > 0$ така, що $\lambda + \epsilon \in \mathcal{A}$. Тоді під JTWSA ми маємо такі межі:

$$\lim_{T' \rightarrow \infty} \sup \frac{1}{T'} \sum_{t=0}^{T'-1} E[E_m^t] \leq E_{avg}^* + \frac{B_2}{V} \quad \#(3.22)$$

Та

$$\lim_{N \rightarrow \infty} \sup \frac{1}{N} \sum_{n=0}^{N-1} \sum_{m=1}^M E[Q_m(nT)] < \frac{B_2 + VE_{max}}{\epsilon} \quad \#(3.23)$$

де E_{avg}^* — оптимальний розв'язок задачі (3.9), $B_2 = \frac{MT^2(R_{max}^2 + A_{max}^2)}{2}$ і $E_{max} = MTE_s$

Доказ виглядає наступним чином: по-перше, він показує існування стаціонарного рандомізованого алгоритму, який є оптимальним і досягає мінімальної середньої енергії за часом, вибираючи T_m^t незалежно від $Q(t)$, але згідно з фіксованим розподілом ймовірностей, відомим мережі. Потім

показано, що JTWSA краще, ніж цей рандомізований алгоритм, в мінімізації R.H.S з (3.13) і, таким чином він також оптимальний [18-19].

З цього випливає, що середня енергія за JTWSA наближається до мінімальної оптимальної енергії E_{avg}^* зі збільшенням V , тоді як середня довжина черги також збільшується з більшими значеннями V .

3.2.2. Математичне моделювання.

Ми розглядаємо мережу Wi-Fi на основі IEEE 802.11ax, де є точка доступу, яка обслуговує $M = 50$ STA. Ми припускаємо, що всі сеанси TWT використовуються для передачі по верхній лінії, і вибираємо параметри, наведені в таблиці 3.1. Ми створюємо середовище моделювання та отримуємо результати в MATLAB.

Таблиця 3.1.

Параметри моделювання

Параметри моделювання	Значення
T	1с, 2с
P_u	1W
P_{sleep}	0.15W
t_{up}	1мс
t_d	0
t_u	1
R	[10, 20, 50, 100, 150, 200] Мбіт/с
M	50 STA
K	5 STA
V	[1000, 5000]
λ	Пуассоновський рух. Період прибуття [5 4,5 4 3,5 3 2,5 2 1,5 1 0,5] с
Розмір файлу	25 Кбайт
Значення TWT	Всього 9 неперекриваючих інтервалів TWT. Мінімальні та максимальні інтервали TWT: 50 мс і 450 мс

Мережа працює наступним чином: на початку кожної T секунд визначаються розміри черги та швидкість передачі для кожної STA, а потім мережа призначає інтервали TWT STA відповідно до JTWSA. Щонайбільше K

$= 5$ STA можна призначити одному інтервалу TWT завдяки можливості багатокористувацької передачі IEEE 802.11ax. Оскільки існує $L = 9$ різних інтервалів TWT і $K = 5$, щонайбільше 45 STA можуть прокидатися для передачі протягом кожного періоду, а інші 5 STA переходять у режим сну протягом цілих T секунд. Після призначення інтервалів TWT, STA прокидаються через визначені інтервали та передають свої дані до точки доступу. Ми порівнюємо JTWSA з еталонним алгоритмом, який призначає інтервали TWT STA випадковим чином на початку кожні T секунд.

Далі ми показуємо продуктивність JTWSA та тестового алгоритму з точки зору середніх розмірів черги та споживання енергії. Згідно моделюванню на рисунках 3.6a та 3.6b зображено загальний середній розмір черги та споживання енергії в рамках JTWSA та алгоритму контрольного тесту, коли T становить 1 с, відповідно. З рисунку 3.6a ми бачимо, що зі збільшенням швидкості прибуття загальний середній розмір черги також збільшується. Однак у алгоритмі контрольного тесту відбувається раптове збільшення розміру черги, коли швидкість надходження становить близько 1, що вказує на те, що мережа більше не стабільна, і контрольний тест не може підтримувати швидкість надходження вище 1. З іншого боку, JTWSA може продовжувати стабілізувати мережу до швидкості прибуття 2. Вищерозглянута теорема вказує, що коли JTWSA працює з вищими значеннями V , це призводить до більшого розміру черги. Малюнок 3.6a підтверджує, що розмір черги з $V = 5000$ вищий порівняно з випадком, коли $V = 1000$.

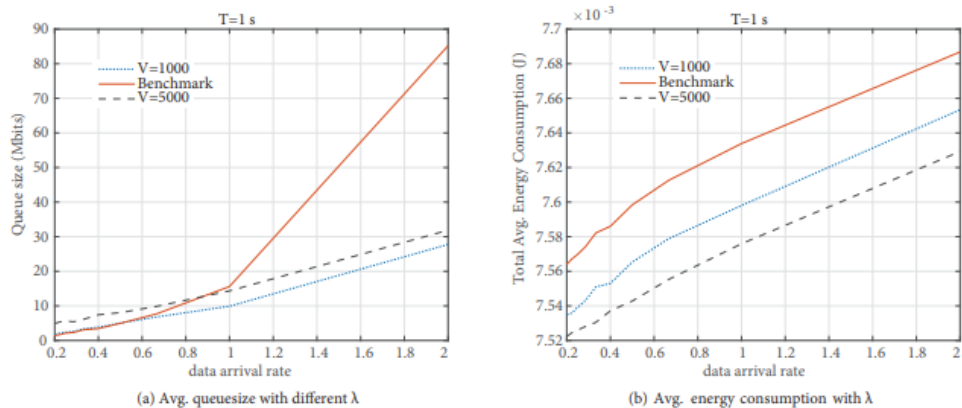


Рис 3.6. Розмір черги (a) та споживання енергії (b) при $T = 1$.

На рисунку 3.6b показано загальне середнє споживання енергії JTWSA та алгоритм порівняння. Зауважимо, що STA можуть прокидатися, навіть якщо їх розміри черги та швидкість передачі даних низькі за допомогою алгоритму порівняння, тобто економія енергії буде нижчою. Це продемонстровано на рисунку 3.6b, де споживання енергії з контрольним показником вище, ніж у JTWSA. Крім того, як теорема передбачає, що зі збільшенням V ми наближаємося до мінімального споживання енергії за допомогою JTWSA. Зрозуміло, що на рисунку 3.6b вище значення V призводить до меншого споживання енергії для JTWSA. Тому, правильно вибравши параметр керування V , можна досягти бажаного компромісу між затримкою черги та споживанням енергії.

Згідно наступному моделюванню 3.7a і 3.7b зображено вплив більшого значення T на розмір черги та споживання енергії. Встановлюємо $T = 2$ с, і відповідно до теореми, як розмір черги, так і споживання енергії зростають із збільшенням T , оскільки B_2 залежить від T .

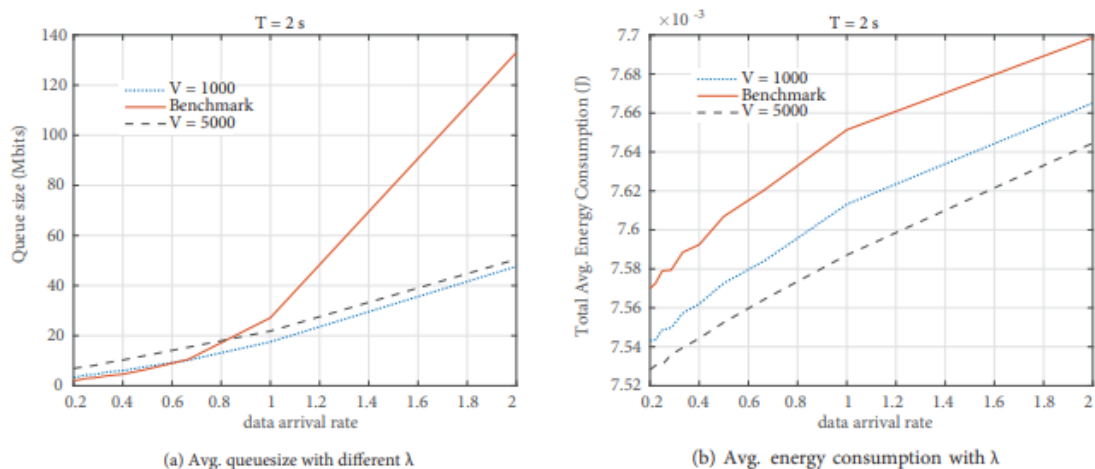


Рис.3.7. Розмір черги(a) та споживання енергії (b) при $T = 2$.

Порівнюючи малюнки 3.6a і 3.7a, можна зробити висновок, що розмір черги більший при більш високих значеннях T . Подібний результат можна вивести для споживання енергії з рисунків 3.6b і 3.7b. Зауважимо, що для того, щоб закрити мінімальне споживання енергії, коли T є високим, нам також потрібні вищі значення V . Також можна побачити, що вплив більшого значення T на споживання енергії менш значний, але вплив на розмір черги не можна

ігнорувати. Хоча вибір нижчих значень T здається кращим з точки зору середнього розміру черги та споживання енергії, це призведе до збільшення накладних витрат на передачу сигналів, оскільки АР має спілкуватися та погоджуватися з кожною STA на інтервалі TWT кожні T секунди. Цей компроміс можна вирішити, враховуючи переваги оператора щодо цільової мети та продуктивності. І в фіналі, на рисунку 3.8 показано, як довго користувачі перебувають у сплячому режимі з різними показниками прибуття, значеннями V та алгоритмами.

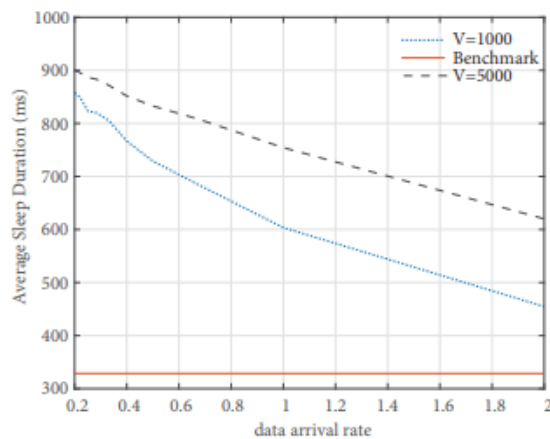


Рис.3.8. Середня тривалість сну з різними умовами руху.

За допомогою тестового алгоритму середня тривалість сну не залежить від стану трафіку, оскільки інтервали TWT призначаються випадковим чином, а середня тривалість сну становить близько 328 мс. Тобто понад 60% часу користувачі за допомогою алгоритму тесту залишаються активними. З іншого боку, користувачі під JTWSA залишаються в активному режимі залежно від умов їхнього руху. Зокрема, коли трафік низький (тобто швидкість прибуття низька), наприклад, швидкість прибуття становить 0,2, користувачі перебувають у сплячому режимі більше 80% часу. Зі збільшенням швидкості трафіку вони частіше залишаються в активному режимі, щоб спустошити свої черги, і, як наслідок, тривалість їхнього сну зменшується. Це також пояснює, чому JTWSA споживає менше енергії, ніж тестовий алгоритм. Крім того, з вищими значеннями V користувачі довше залишаються в режимі сну і, отже, заощаджують більше енергії.

Висновки

З першого моделювання в середовищі MATLAB були отримані значення пропускної спроможності, які виявилися меншими за рахунок урахування витрат фізичного та канального рівня. Процедура прослуховування і зміна швидкості запитів CSI мінімально впливають на загальну продуктивність системи (відхилення значень пропускної спроможності каналу для DL = 5.83-5.88%, для UL = 0.79-1.27%) оскільки станції користувача відправляють в ТД інформацію CSI паралельно, а не послідовно, як це робиться у IEEE 802.11ac. Потрібно ретельне налаштування величини A-MPDU, оскільки збільшення цього значення зменшує кількість ефективного ефірного часу, виділеного для ТД та зменшує пропускну здатність мережі у напрямку вниз на 60%.

В другій частині було представлено алгоритм, який спрямований на підвищення енергоефективності механізму енергозбереження IEEE 802.11ax шляхом оптимізації інтервалів TWT STA відповідно до їх трафіку та стану каналу. Цей алгоритм призначає менший інтервал TWT, коли розмір черги великий та/або висока швидкість передачі, і дозволяє більше часу сну, якщо трафік досить низький. Ми проаналізували алгоритм за допомогою системи оптимізації Ляпунова та знайшли межі продуктивності щодо споживання енергії та розмірів черги. Ми визначили два важливі компроміси: по-перше, висока економія енергії може бути досягнута, коли допускається велика середня затримка черги. Крім того, більш низьку середню затримку можна отримати, якщо інтервали TWT оновлюються частіше, але вартість у цьому випадку є високими накладними витратами сигналізації.

РОЗДІЛ 4

РОЗРОБЛЕННЯ СТАРТАП ПРОЕКТУ

В даному розділі викладено маркетинговий аналіз перспектив реалізації мереж бездротового доступу інтернет на основі протоколу IEEE 802.11ах, а також оцінено можливості її ринкового впровадження.

4.1.Опис ідеї проекту

Проект направлений на модифікацію розгортання мереж бездротового доступу інтернет Wi-Fi, за рахунок впровадження нового протоколу сімейства IEEE802.11ах, а також проектування та моделювання майбутньої мережі в спеціальних програмних засобах. Така система допомагає, здешевити розгортання мережі, з максимальною ефективністю системи.

Таблиця 4.1

Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Система підвищення ефективності мереж бездротового доступу Wi-Fi, що допомагає здешевити розгортання мережі, з максимальною ефективністю системи.	1. Підвищення ефективності мереж. 2. Зменшення вартості розгортання. 3. Визначення параметрів мережі які мають найбільший вплив на користувачів систем.	Мережі бездротового доступу Wi-Fi зможуть зменшити неефективні витрати на розгортання мережі, а також оптимізувати роботу систем у великих приміщеннях.

При порівнянні з конкурентами в першу чергу увага надається архітектурному підходу, що забезпечує швидкість роботи та ефективність у кожному конкретному випадку. Порівняння з конкурентами, а також визначення переваг і недоліків наведено у наступні таблиці.

Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко- економічні характеристики ідеї	(потенційні) товари/концепції конкурентів		W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій пр.	MiaTis			
1	Використання безкоштовного програмного забезпечення	ні	ні		так	
2	Непередбачуване зростання вартості	ні	так		так	
3	Індивідуальні можливості кастомізації системи	так	ні			так
4	Єдина підтримка апаратної та програмної частини	ні	так			так

Конкуренти володіють лише частковим функціоналом, який реалізований в даному проекті. Серед сильних сторін визначені єдина підтримка апаратної та програмної частини та можливості кастомізації під конкретні задачі, які ставляться перед обраним проектом.

4.2. Технологічний аудит ідеї проекту

Технологічна здійсненність ідеї проекту

No п/п	Ідея проекту	Технології реалізації	Доступність технологій
1	Система підвищення ефективності мереж бездротового доступу Wi-Fi	Протокол IEEE802.11ax	Є доступними та безкоштовними для використання
		Протокол WPA3	Є доступними та безкоштовними для використання
Обрана технологія реалізації проекту: Протокол IEEE802.11ax			

Для реалізації проекту було обрано два протоколи: протокол доступу IEEE 802.11ax та протокол захисту WPA3. Протокол IEEE 802.11ax було обрано для розгортання мережі, а протокол WPA3 для надійного захисту мереж бездротового доступу.

4.3. Аналіз ринкових можливостей запуску стартап-проекту

При дослідженні ринкових можливостей, в першу чергу проведений аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку. Дані наведені у таблиці нижче.

Таблиця 4.4

Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	2
2	Загальний обсяг продаж	Більше 10 тис одиниць
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу	Немає
5	Специфічні вимоги для стандартизації, специфікації	Немає
6	Середня норма рентабельності в галузі, %	-

Враховуючи сьогоденішню необхідність ринку рішень стосовно підвищення лояльності клієнта, за попереднім оцінюванням ринок є привабливим для входження.

Таблиця 4.5

Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Підвищення ефективності мереж Wi-Fi	Підприємства, офіси, коворкінги, відкриті площадки (AtlasWeekend, футбольні матчі)	Точки розгортання мережі в свою чергу можуть визначати самостійно формат взаємодії та внести свої коригування.	Підвищення працездатності мереж. Можливість отримати перелік параметрів котрі оказують найбільший вплив на клієнтів. Використання новітніх методів обробки даних для швидкості та правильності роботи системи.

Таблиця 4.6.

Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Моральне зношення технологій	Успіх системи залежить від підтримки пристроями нових протоколів. Адже система зможе повністю функціонувати за рахунок пристроїв, що мають підтримку новітніх протоколів IEEE 802.11ax та WPA3.	Відмова у зміні старих пристроїв на нові.

Загрозою вважається застарілі пристрої, моральне зношення яких не дозволяє розгортання мереж на основі новітніх протоколів, по банальній причині не підтримки цих стандартів. Функціонал протоколів попросту буде відсутнім.

Таблиця 4.7

Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
1. Тип конкуренції: олігополія	На ринку представлені декілька компаній, що поставляють подібні послуги рішення проблеми відтоку	Акцентування переваг продукту, що забезпечує використання нових методів розгортання мереж безпроводового доступу Wi-Fi.
2. Рівень конкурентної боротьби: національний/інтернаціональний	Першим етапом є боротьба за ринок України з подальшим виходом на ринки інших країн	Маркетингова компанія в першу чергу орієнтована на захоплення місцевого ринку
3. Галузева ознака: внутрішньогалузева	Економічна боротьба з конкурентами відбувається в одній галузі економіки, пропонуються аналогічні послуги, що мають архітектурні відмінності у функціонуванні	Пропозиція суттєвих переваг у порівнянні з продуктами конкурентів у визначеній галузі економіки

4. За характером конкурентних переваг: нецінова	Передбачається ведення конкурентної боротьби не за рахунок зниження ціни на аналогічні послуги, а за рахунок новизни та унікальних характеристик технології, на якій базується функціонування системи	Акцент на унікальних характеристиках пропонованого товару
---	---	---

Таблиця 4.8

Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	MiaTis	Доступні та гнучкі ціни, Перевіреність, Патент на продукт	Змінні витрати постачальників	Рівень чутливості до ефективності мереж.	Ціна, надійність, швидкодія
Висновки	Конкуренція не інтенсивна, кожен працює в окремому регіоні	Можливість виходу в ринок висока. Потенційні конкуренти присутні	Постачальник може диктувати умови: ціни на розгортання мереж.	Кожен з клієнтів потребує індивідуального підходу для вирішення його задач	Обмеження для роботи на ринку з боку товарів-замінників на даний момент не існує

В результаті проведення аналізу таблиці 1.9, можна зробити висновок, що можливість виходу на ринок з огляду на конкурентну ситуацію є досить високою. Для виходу на ринок товар в першу чергу повинен пропонувати унікальні характеристики, ефективність та швидкодію, які відсутні у продуктах конкурентів.

Таблиця 4.9

Обґрунтування факторів конкурентоспроможності

№ п/п	Фактори конкурентоспроможності	Обґрунтування
1	Динаміка галузі	Підвищення ефективності роботи мереж бездротового доступу має високий пріоритет, великі підприємства, офіси, коворкінги зацікавленні в цьому.

Продовження таблиці 4.9

2	Концепція товару і послуги	Система підвищення ефективності мереж бездротового доступу Wi-Fi.
3	Після продажне обслуговування	Підтримка щодо використання системи після її продажу

Таблиця 4.10.

Порівняльний аналіз сильних та слабких сторін системи підвищення лояльності абонентів операторів мобільного зв'язку

№ п/п	Фактори конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з власною системою						
			-3	-2	-1	0	1	2	3
1	Динаміка галузі	3							✓
2	Концепція товару і послуги	1							✓
3	Після продажне обслуговування	2						✓	

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities) на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін (таблиця 4.11).

Таблиця 4.11

SWOT-аналіз стартап проекту

Сильні сторони: • Інноваційні технології • Новизна технологій • Висока якість	Слабкі сторони: • Слабкий імідж компанії • Незарекомендований бренд • Слабкий маркетинг • Невідома торгівельна марка • Невеликий початковий капітал
--	--

Продовження таблиці 4.11

Можливості: • Нові технології • Нові потреби клієнтів • Тенденції попиту	Загрози: • Продукти-замінники • Конкуренти з більшим капіталом
---	--

Таблиця 4.12

Альтернативи ринкового впровадження стартап-проекту

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Державні підприємства	Не готові	Дуже високий	Дуже висока	Важко
2	Малий бізнес	Переважно готові	Дуже високий	Висока	Легко
Цільовими групами обрано державні компанії, що зацікавлені у модернізації мереж бездротового доступу Wi-Fi, шляхом отримання тендеру від держави.					

4.4. Розроблення маркетингової програми стартап-проекту

Маркетингова програма - це розроблений на основі комплексних маркетингових досліджень стратегічний план-рекомендація щодо виробничо-збутової і науково-технічної діяльності фірми на певний період часу,

покликаний забезпечити оптимальний варіант її майбутнього розвитку з урахуванням запитів споживачів і відповідно до висунутим цілям і стратегії.

В процесі розробки маркетингових програм враховуються множинні умови, перспективи та обмеження як в розвитку ринку, так і у внутрішньо фірмової розвитку, а також дію прямих і зворотних зв'язків з ринком, необхідність пристосування до мінливих запитам ринку і активного впливу на формування та розширення ринкового попиту.

Першим кроком є формування маркетингової концепції товару , який отримає споживач. Для цього потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару (таблиця 4.13).

Таблиця 4.13

Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентом
1	Підвищення швидкодії мережі	Можливість, що забезпечується новітніми покращених технологій.	Використання новітніх технологій до рішення цієї задачі
2	Адаптивність мереж	Дозволяє розглядати кожен параметр телекомунікаційної мережі окремо	Проектування та моделювання мережі перед розгортанням
3	Вигідність	Отримання списку з вказанням у відсотках про затрати та окупність технологій	Подання інформації для більшого розуміння продукту.

Надалі розробляється трирівнева маркетингова модель товару: уточняється ідея продукту та послуги , його фізичні складові , особливості процесу його надання (таблиця 4.14).

Таблиця 4.14

Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові
1. Товар за задумом	Товар забезпечує підвищення ефективності та швидкодії мереж бездротового доступу Wi-Fi.

2. Товар у реальному виконанні	Властивості: доступність, надійність, зручність, релевантність, окупованість
	Продукт представляє собою програмний комплекс реалізований за допомогою протоколів IEEE 802.11ax та WPA3.
	Поставляється у вигляді застосунку для всіх популярних платформ.

Продовження таблиці 4.12

	Назва: FWFA – Faster Wi-Fi for All
3. Товар із підкріпленням	До продажу: відбувається інсталяція та конфігурування системи,
	Після продажу: відбувається обслуговування програмного забезпечення та його доопрацювання по бажанню клієнта

Аналіз системи збуту передбачає визначення ефективності кожного елемента цієї системи, оцінювання діяльності апарату працівників збуту. Аналіз витрат обігу передбачає зіставлення фактичних збутових витрат за кожним каналом збуту і видом витрат із запланованими показниками для того, щоб виявити необґрунтовані витрати, ліквідувати затрати, що виникають у процесі руху товарів і підвищити рентабельність наявної системи збуту.

Дані щодо визначення системи збуту надаються в таблиці 4.15.

Таблиця 4.15

Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
-------	---	---	----------------------	--------------------------

1	Власна система збуту	Проведення та розгортання програмного забезпечення на стороні компанії-клієнта	Канал нульового рівня, продаж товару відбувається безпосередньо споживачам через відділ збуту	Оптимальною системою збуту є прямий збут з каналом нульового рівня за відсутності посередників
---	----------------------	--	---	--

Таблиця 4.16

Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення
1	Готовність до впровадження новітніх технологій	Соцмережі, корпоративна пошта, інші інформативні площадки	Можливості модифікації наявних систем вже	Висвітлити унікальні характеристики продукту

У якості концепції маркетингових комунікацій були обрані інтегровані маркетингові комунікації, де компанія ретельно обмірковує і координує роботу своїх численних каналів комунікації, створює рекламну кампанію для популяризації товару в засобах масової інформації, залучення креативних агенств для подальшого просування товару, особистий продаж та колаборації з іншими стартапами, стимулювання збуту, прямий маркетинг.

Висновки

У ході розробки стартапу було обдумане та доведено такі пункти:

- Стартап має високу можливість ринкової комерціалізації проекту, за рахунок наявного попиту, та високого попиту в майбутньому в ході розвитку технологій, сприятливої динаміки ринку та рентабельності роботи на ринку.

- Проаналізувавши конкурентоспроможність проекту, було освідомлено, що стартап має високу конкурентну спроможність. Перспектива впровадження з огляду на потенційні групи клієнтів є доволі сприятливою, використання новітніх технологій мінімізує бар'єри входження, та збільшує стан конкуренції.
- В залежності від стартового капіталу та готовності клієнту залежатиме ріст та популяризація продукту.

Проведений аналіз підтверджує, що подальша імплементація проекту є доцільною.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У магістерській дисертації була розглянута методика розрахунку мережі бездротового доступу Wi-Fi на основі протоколу IEEE 802.11ax.

Мета, яка була поставлена перед виконанням роботи, виконана, а отримані результати в ході виконання дипломної роботи відповідають сформульованим завданням і повністю задовольняють їх. Для досягнення мети були зроблені такі дії:

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

- Були опрацьовані стандарти мережі Wi-Fi;
- Розглянуто основні протоколи захисту мереж Wi-Fi;
- Розглянуто основний механізм доступу та рівні мережі.

Протокол WPA3 є найбільш придатним для забезпечення безпеки та надійності персональних даних користувачів мережі. Переваги наведені у висновку до другого розділу.

Найефективнішим та більш перспективним протоколом доступу є протокол сімейства IEEE 802.11ax. Очевидно, що саме цей протокол було обрано в основу магістерської дисертації.

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

2) У другому розділі був розглянутий найактуальніший протокол сімейства IEEE 802.11ax. Розглянуто структуру та функціонал протоколу, наведено точні характеристики та проаналізовані основні переваги IEEE 802.11ax над своїми попередниками.

Наведено основні цілі та задачі протоколу IEEE 802.11ax. Результатом аналізу є те, що протокол є ефективнішим в 1.5 рази за свого найбільш актуального попередника IEEE 802.11ac.

3) У третьому розділі було розглянуто дві методики розрахунку мереж бездротового доступу Wi-Fi. Кожна з методик супроводжується розрахунком та моделюванням в середовищі MATLAB:

- З першого моделювання в середовищі MATLAB були отримані значення пропускної спроможності, які виявилися меншими за рахунок урахування витрат фізичного та канального рівня. Потрібно ретельне налаштування величини A-MPDU, оскільки збільшення цього значення зменшує кількість ефективного ефірного часу, виділеного для ТД та зменшує пропускну здатність мережі у напрямку вниз на 60%.
- В другій частині було представлено алгоритм, який спрямований на підвищення енергоефективності механізму енергозбереження IEEE 802.11ax шляхом оптимізації інтервалів TWT STA відповідно до їх трафіку та стану каналу.

Обидва моделювання показали ефективність застосування методик. З урахуванням отриманих результатів, можна вважати що розробка мережі набагато ефективнішої ніж наявна в будь якому приміщенні є реальною.

4) У четвертому розділі запропоновано стартап який повністю виконує всі вимоги перспективного стартапу. Основні пункти:

- Стартап має високу можливість ринкової комерціалізації проекту;

- Стартап має високу конкурентну спроможність;
- Перспектива впровадження з огляду на потенційні групи клієнтів є доволі сприятливою.

Я можу з впевненістю стверджувати, що подальша імплементація проекту є доцільною.

Отже, я вважаю, що поставлена мета виконана.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Олифер В. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вишів. 5-те вид. - СПб.: Пітер, 2016. — 992 с.: іл. - (Серія «Підручник для вузів»).
2. Таненбаум А. Комп'ютерні мережі / А. Tanenbaum, D. Wetherall. – Новий Джерсі, Пірсон, 2012. – 959 с. – (5-те видання).
3. Підпалій 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". Збірник матеріалів конференції. 8-10 січня 2020 року – Ліверпуль. 2020. – 803 с.
4. Підпалій О.І. АНАЛІЗ РОБОТИ ПРОТОКОЛУ ЗАХИСТУ БЕЗПРОВОДОВИХ МЕРЕЖ WPA2. I Міжнародна науково-практична конференція "MODERN SCIENCE: PROBLEMS AND INNOVATIONS". Збірник матеріалів конференції. 5-7 квітня 2020 року – Стокгольм. 2020. – 229 с.
5. Підпалій О.І. АНАЛІЗ ВРАЗЛИВОСТІ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI З НОВИМ ПРОТОКОЛОМ ЗАХИЩЕНОСТІ WPA3. XIV Міжнародна науково-технічна конференція «Перспективи телекомунікацій»; ПТ-2020: Збірник матеріалів конференції. К.: КПП ім. Ігоря Сікорського, 2020. – С. 98-102. ISSN(print) 2663-502X

6. WPA2-Enterprise. Як створити безпечну мережу? [Електронний ресурс]. – 2018. - Режим доступу до ресурсу: <https://wifi-solutions.ru/zashita-korporativnoy-seti-s-wpa2-enterprise/>
7. Деякі топології мережі WLAN – BSS, IBSS, Mesh BSS і 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/>
8. Wireless LAN (WLAN) [Електронний ресурс]. – 2017. – Режим доступу до мережі: <http://www.hitchhikersguidetolearning.com/wireless-lan-wlan-articles/>
9. Wi-Fi (Wireless Fidelity) стандарт бездротового зв'язку [Електронний ресурс]. – 2017. – Режим доступу до мережі: [https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Wi-Fi \(Wireless Fidelity\) - %D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82 %D0%B1%D0%B5%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D0%BE%D0%B9 %D1%81%D0%B2%D1%8F%D0%B7%D0%B8 802.11](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Wi-Fi%20(Wireless%20Fidelity)%20-%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B1%D0%B5%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D0%BE%D0%B9%D1%81%D0%B2%D1%8F%D0%B7%D0%B8%20802.11)
- 10.Що таке 802.11ax - огляд нового стандарту WI-FI 6 [Електронний ресурс]. – 2017. – Режим доступу до мережі: <https://translate.google.com.ua/?hl=ru&sl=ru&tl=uk&text=%D0%A7%D1%82%D0%BE%20%D1%82%D0%B0%D0%BA%D0%BE%D0%B5%20802.11ax%E2%80%93%D0%BE%D0%B1%D0%B7%D0%BE%D1%80%20%D0%BD%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE%20%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B0%20WI-FI%206&op=translate>
- 11.Що нас чекає на Wi-Fi 7, IEEE 802.11be? [Електронний ресурс]. – 2017. – Режим доступу до мережі: <https://translate.google.com.ua/?hl=ru&sl=ru&tl=uk&text=%D0%A7%D1%82%D0%BE%20%D0%BD%D0%B0%D1%81%20%D0%B6%D0%B4>

<https://help.keenetic.com/hc/ru/articles/360010536300-%D0%B5%D1%82%20%D0%B2%20Wi-Fi%207%2C%20IEEE%20802.11be%3F&op=translate>

- 12.Що потрібно знати про стандарт Wi-Fi 6 (IEEE 802.11ax) [Електронний ресурс]. – 2017. – Режим доступу до мережі: <https://help.keenetic.com/hc/ru/articles/360010536300-%D0%A7%D1%82%D0%BE-%D0%BD%D1%83%D0%B6%D0%BD%D0%BE-%D0%B7%D0%BD%D0%B0%D1%82%D1%8C-%D0%BE-%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B5-Wi-Fi-6-IEEE-802-11ax->
- 13.What are IEEE 802.11 Standards? : 802.11a/b/g/n/ac/ax [Електронний ресурс]. – 2017. – Режим доступу до мережі: <https://www.signalboosters.com/blog/ieee-802.11-standards-explained-802.11abgnacax/>
- 14.Підпалій О. І. Захист мереж безпроводового доступу на базі технології Wi-Fi з протоколом WPA2-Enterprise : диплом, студент / Підпалій Олександр Іванович – Київ, 2019. – 92 с.
15. Bianchi G. Аналіз продуктивності розподіленої координаційної функції IEEE 802.11, 2000. – В. 3. – С. 535-547.
- 16.Ahn W., Kim Y. Y. and Kim R. Y. Енергоефективна багатокористувацька схема передачі висхідного зв'язку в WLAN нового покоління для Інтернету речей, Int. J. Distrib. Сенсорні Мережі, 2016. – В. 12. – С. 1-10.
- 17.Afaqui M. S., Garcia-Villegas E. and Lopez-Aguilera E. Алгоритм керування динамічною чутливістю, що використовує адаптивний RTS/CTS для IEEE 802.11ax, IEEE конф., Доха, Катар, 2016. – С. 1-6.
- 18.Georgiadis L, Neely MJ, Tassiulas L. Розподіл ресурсів і міжрівневий контроль у бездротових мережах. Бостон, США: Основи та тенденції в мережі, 2006.

19. Fang W, Yao Y, Huang L, Sharma A. B, Golubchik L et al. Коментар щодо зниження витрат на електроенергію в розподілених центрах обробки даних: підхід із двома часовими шкалами для робочих навантажень із стійкістю до затримок. Транзакції IEEE в паралельних і розподілених системах 2015; 26 (5): 1495–1496.
20. Kulkarni A, Seetharam A, Ramesh A, Herath JD. DeepChannel: передбачення якості бездротового каналу за допомогою глибокого навчання. Транзакції IEEE щодо транспортних технологій 2020; 69 (1): 443-456. doi: 10.1109/TVT.2019.2949954
21. [Електронний ресурс]. – 2017. – Режим доступу до мережі: <http://www.techonline.com/electrical-engineers/education-training/tech-papers/4442856/802-11ax-High-Efficiency-Wireless/viewpdf>
22. А.Г. Кір'янов, А. І. Ляхов, Д. А. Міхліна, Е. М. Хоров, І.А. Щолкіна Проблеми створення IEEE 802.11ax — нового покоління мереж Wi-Fi / Інформаційні процеси, Том 16, № 1, 2016, стор. 1–12.
23. Макаренко В.В., Доля С.О. Особенности стандарта беспроводной связи IEEE 802.11ad (WiFi) / Электронные компоненты и системы, №4-6, 2014. с. 50-58. – http://www.ekis.kiev.ua/UserFiles/Image/pdfArticles/4-6_2014/V.Makarenko_IEEE_802.11ad_EKIS_4-6_200-02-2.pdf.
24. IEEE 802.11ax TECHNOLOGY INTRODUCTION. // ROHDE&SCHWARZ. – 2019. – С. 36.