

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти)

на тему ДОСЛІДЖЕННЯ ВПЛИВУ ЗМІНИ ПАРАМЕТРІВ НА
ПРОДУКТИВНІСТЬ БЕЗДРОТОВИХ МЕРЕЖ СТАНДАРТУ IEEE 802.11

Виконав: студент 2 курсу, групи КНТ-512м
спеціальності _____

123 Комп'ютерна інженерія

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Комп'ютерні системи та мережі

МОРОЗ Ю. А.

(ПРИЗВИЩЕ та ініціали)

Керівник

КИРИЧЕК Г.Г.

(ПРИЗВИЩЕ та ініціали)

Рецензент

СТЕПАНЕНКО О.О.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти магістерський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) «Комп'ютерні системи та мережі»
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Зав. кафедри Кудерметов Р.К.

“14” листопада 2023 року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

МОРОЗА Юрія Анатолійовича

(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження впливу зміни параметрів на продуктивність бездротових мереж стандарту IEEE 802.11

керівник проєкту (роботи) к. т. н., доцент, КИРИЧЕК Галина Григорівна

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

затверджені наказом вищого навчального закладу від “24” жовтня 2023 року № 400

2. Строк подання студентом проєкту (роботи) 10 грудня 2023 року

3. Вихідні дані до проєкту (роботи) Оцінювання системи бездротових мереж IEEE 802.11 та експлуатаційних характеристик. Стандарти: 802.11n/ac/ax.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз бездротових мереж стандарту IEEE 802.11. Аналіз методів оцінювання продуктивності бездротових мереж. Моделювання мережі. Оцінювання продуктивності мережі при зміні параметрів.

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

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	КИРИЧЕК Г. Г., доцент		
нормоконтроль	ПОЛЬСЬКА О.В., ст. викл.		

7. Дата видачі завдання 01.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз технології IEEE 802.11	10.11.2023 р.	
2	Аналіз методики оцінювання пропускну здатності бездротової мережі	12.11.2023 р	
3	Моделювання та налаштування мережі	16.11.2023 р.	
4	Дослідження зміни впливу параметрів на робочі характеристики мереж технології 802.11	20.11.2023 р.	
5	Оформлення отриманих результатів у ПЗ	25.11.2023 р.	
6	Оформлення додаткового матеріалу	05.12.2023 р.	

Студент


(підпис)

Юрій МОРОЗ
(ім'я, ПРИЗВИЩЕ)

Керівник проєкту (роботи)


(підпис)

Галина КИРИЧЕК
(ім'я, ПРИЗВИЩЕ)

РЕФЕРАТ

ПЗ: 80 с., 42 рис., 7 табл., 19 джерел

TAMOGRAPH SITE SURVEY, IEEE 802.11AC, IEEE 802.11AX, IPERF, LAN, WI-FI, WLAN, ЕКСПЛУАТАЦІЙНІ ХАРАКТЕРИСТИКИ БЕЗДРОТОВИХ МЕРЕЖ

Об'єкт дослідження – Wi-Fi мережа стандарту IEEE 802.11.

Предмет дослідження – зона покриття точки доступу бездротової мережі та її пропускна спроможність під впливом зміни параметрів, навантаження та колізій.

Мета роботи – аналіз експлуатаційних параметрів мереж стандарту IEEE 802.11 при розгортанні в сучасних умовах, вплив цих параметрів на ефективність застосування стандарту в побудові бездротових сегментів.

Програмне забезпечення: операційна система Windows, iPerf3, TamoGraph Site Survey. Стандарти: Wi-Fi, 802.11. Обладнання: ноутбук Lenovo ThinkBook 15, маршрутизатор TP-Link Archer AX1500. Протоколи: 802.11a/b/g/n/ac/ax.

У даній роботі описано методику моделювання тестових мереж та отримання показників продуктивності сегментів бездротових локальних мереж.

Порівняння нових стандартів з фізично аналогічними стандартом IEEE 802.11 проводилося шляхом моделювання структури мережі за допомогою спеціального програмного забезпечення та проведення експериментальних досліджень.

Результати – отримані дані дозволять скоротити час розгортання нових бездротових мереж та спростують вибір обладнання для побудови мереж необхідної продуктивності.

ABSTRACT

Explanatory note to the master's work: 80 p, 42 figures, 7 tables, 19 sources

TAMOGRAPH SITE SURVEY, IEEE 802.11AC, IEEE 802.11AX, IPERF, LAN, WI-FI, WLAN, PERFORMANCE CHARACTERISTICS OF WIRELESS NETWORKS

The object of the study is a Wi-Fi network of the IEEE 802.11 standard.

The subject of the study is the coverage area of a wireless network access point and its throughput under the influence of parameter changes, load and collisions.

The purpose of the work is to analyze the operational parameters of the IEEE 802.11 standard networks in the conditions of deployment in modern conditions, the influence of these parameters on the effectiveness of the application of the standard in the construction of wireless segments.

Standards: Wi-Fi, 802.11. Software: Windows 10 OS, TamoGraph Site Survey, iPerf3. Protocols: 802.11a/b/g/n/ac/ax. Equipment: Lenovo ThinkBook 15 laptop, TP-Link Archer AX1500 router.

This work describes the method of modeling test networks and obtaining performance indicators of segments of wireless local networks.

The comparison of the new standards with the physically similar IEEE 802.11 standard was carried out by modeling the network structure using special software and conducting experimental studies.

Results - the obtained data will allow to reduce the deployment time of new wireless networks and simplify the selection of equipment for building networks of the required performance.

ЗМІСТ

Вступ.....	7
1 Аналіз бездротових мереж стандарту IEEE 802.11	8
1.1 Структура мережі бездротового доступу Wi-Fi	8
1.2 Аналіз стандартів доступу до мережі сімейства IEEE 802.11.....	12
1.3 Аналіз протоколів захисту мереж бездротового доступу Wi-Fi.....	24
1.4 Механізм доступу до середовища	35
2 Аналіз методів оцінювання продуктивності бездротових мереж.....	38
3 Моделювання мережі.....	47
3.1 Радіообстеження місцевості розгортання	47
3.2 Проектування мереж із зменшенням домену колізій	50
3.3 Коефіцієнт ослаблення сигналу Wi-Fi	53
3.4 Вибір програмного та апаратного комплексу для дослідження	55
4 Оцінювання продуктивності мережі при зміні параметрів.....	60
4.1 Налаштування програмно-апаратного комплексу.....	60
4.2 Результати моделювання	66
Висновки.....	78
Перелік джерел посилання	79

ВСТУП

З розвитком технологій і збільшенням кількості бездротових пристроїв, бездротові мережі стають все більш поширеними. Інтернет став невід'ємною складовою нашого життя, і бездротові мережі дозволяють нам отримувати доступ до Інтернету практично в будь-якому місці та в будь-який час. Зараз бездротові мережі використовуються майже у всіх галузях, від дому до офісу та до громадських місць, де доступ до Інтернету є необхідністю. Ноутбуки, смартфони, планшети, телевізори, системи пожежної безпеки та багато інших пристроїв підтримують бездротове підключення [1]. Проте, продуктивність бездротових мереж 802.11 залежить від багатьох факторів, включаючи параметри мережі, такі як пропускна здатність, діапазони частот та інші [2].

В роботі зроблено огляд бездротових мереж стандарту IEEE 802.11 та розглянуті проблеми вибору програмного забезпечення для моделювання імітаційних моделей мереж, зони покриття точок доступу бездротових мереж.

В першому розділі описується та аналізується розвиток традиційних бездротових локальних мереж та їх стандарти. У другому розділі детально розглядаються методи оцінювання продуктивності мереж стандарту IEEE 802.11. Третій розділ присвячений підбору програмного та апаратного комплексу для дослідження та моделюванню мереж за допомогою спеціалізованого програмного забезпечення. В четвертому розділі проведено експериментальне дослідження експлуатаційних характеристик мережі і аналіз даних отриманих при моделюванні.

1 АНАЛІЗ БЕЗДРотовИХ МЕРЕЖ СТАНДАРТУ IEEE 802.11

За останні кілька років поширення бездротових мереж Wi-Fi є стрімким, 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 в межах 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 [3].

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. Мережі Wi-Fi використовуються для зв'язку та обміну даними між вузлами та є гнучкими системами обміну інформацією, які служать альтернативою дротової мережі в приміщенні або на вулиці. Ці мережі також використовується для організації точок загального доступу, таких як аеропорти, площі та інші місця, де збираються люди, а також для організації тимчасових бездротових мереж на фестивалях, футбольних матчах, музейних виставках тощо [4].

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

- інфраструктурна топологія мережі;
- спеціальна топологія мережі;
- топологія бездротової сітки;
- P2P мережева топологія.

1.1.1 Інфраструктурна топологія

На рисунку 1.1 зображена інфраструктурна топологія.

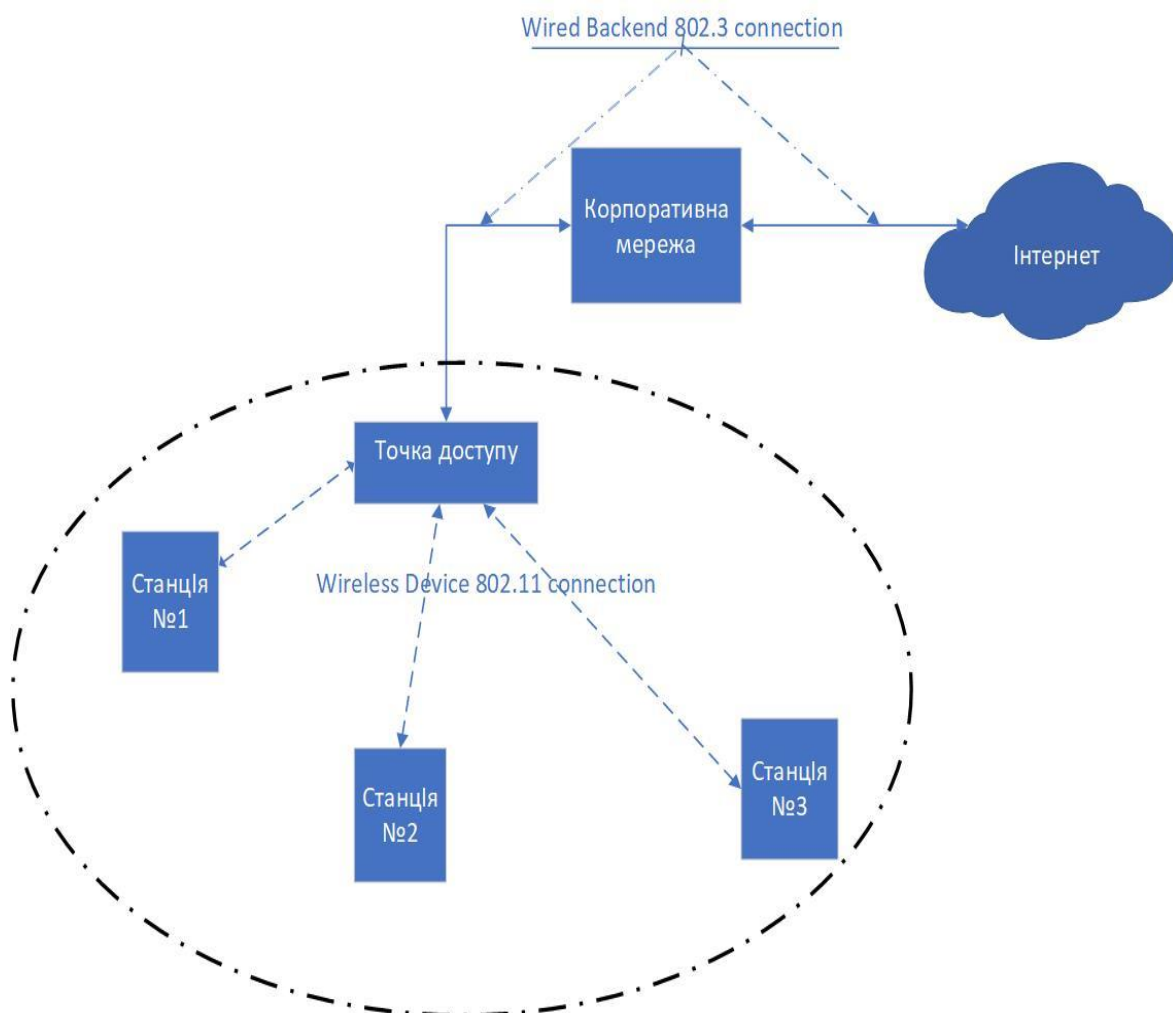


Рисунок 1.1 – Топологія інфраструктурної мережі

Пунктирна область у колі називається базовим набором послуг (BSS). Усі

станції, підключені до точки доступу, утворюють базовий набір послуг. Також існує ще базова зона обслуговування (BSA). Основна зона покриття — це зона, яку охоплює точка доступу. Сигнал точки доступу може виходити за межі діапазону підключених до нього пристроїв. Цією зоною покриття є BSA [5].

1.1.2 Спеціальна топологія мережі

Особливою топологією є автономна однорангова мережа Peer-to-Peer. Іншими словами, це мережа без окремої точки доступу, де пристрій є не лише кінцевою точкою, але й маршрутизатором. Це зображено на рисунку 1.2.

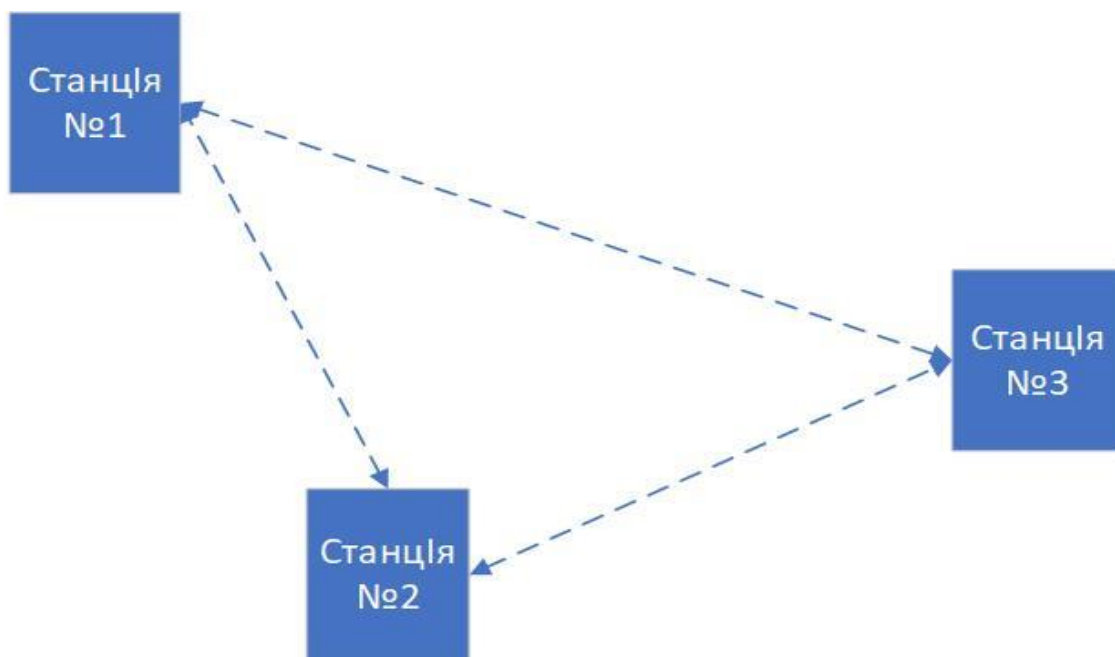


Рисунок 1.2 – Спеціальна топологія мережі

1.1.3 Топологія бездротової сітки

Бездротова сітчаста мережа — це взаємозв'язок підключених вузлів, які утворюють незалежну мережу, так звану Wireless Mesh. Коли вузол мережі «виходить з ладу», формуються нові шляхи для створення функціонуючої мережі. Меш-вузли спілкуються один з одним за допомогою стандарту 802.11. Ви також можете налаштувати резервний вузол сітки для підключення до публічного шлюзу на випадок збою основного вузла сіті. Користувачі можуть підключатися до будь-якого вузла мережі. Мережевий трафік розподіляється між різними вузлами, і для забезпечення найшвидшого маршруту до загальнодоступної мережі необхідно

встановити ефективні механізми маршрутизації. Топологію сітчастої мережі зображено на рисунку 1.3.

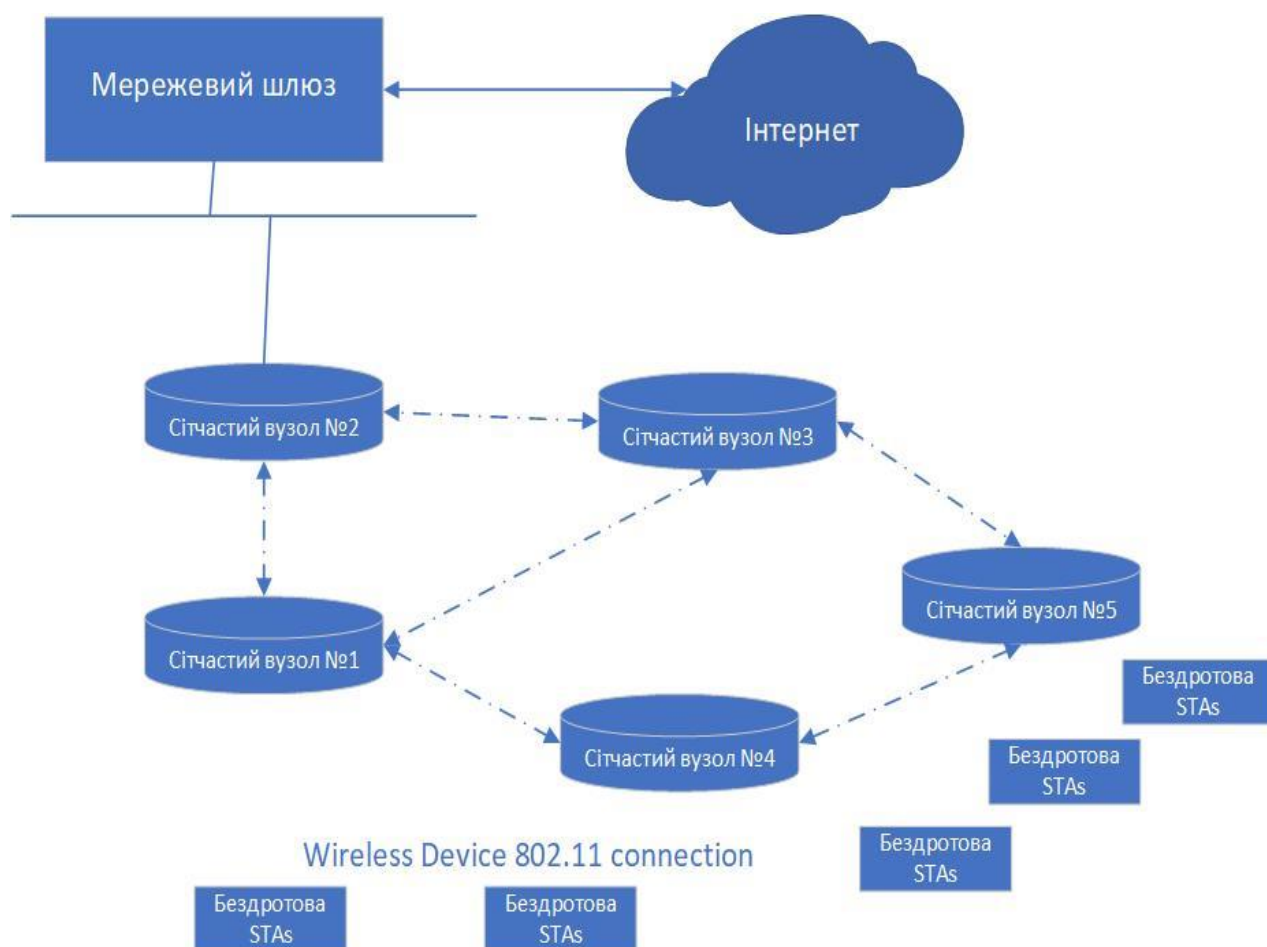


Рисунок 1.3 – Мережа бездротової локальної мереж

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. Топологію такої мережі зображено на рисунку 1.4.

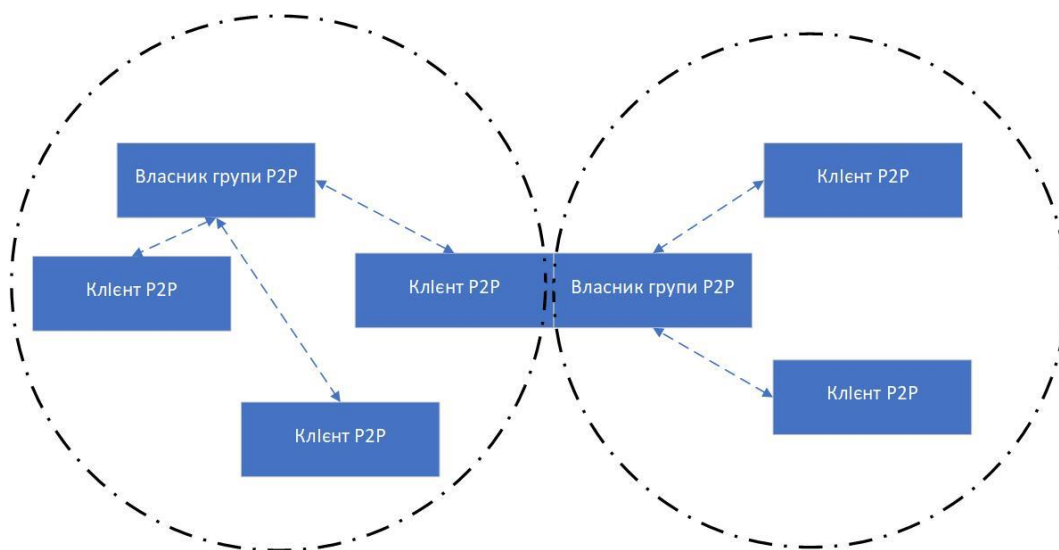


Рисунок 1.4 – Топологія мережі P2P

1.2 Аналіз стандартів доступу до мережі 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 [6].

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.

Зараз існує ціла низка стандартів що належить до групи IEEE 802.11. Розглянемо найпоширеніші і ті що широко використовуються:

- базовий 802.11;
- IEEE 802.11a (Wi-Fi 2);

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

Усі стандарти IEEE 802.11 працюють на двох нижніх рівнях моделі ISO/OSI, фізичному та каналному, тому будь-яка мережева програма, мережева операційна система чи протокол (наприклад, TCP/IP) працює однаково в мережах 802.11, та і в мережі Ethernet. Рівні моделі ISO / OSI зображено на рисунку 1.5.

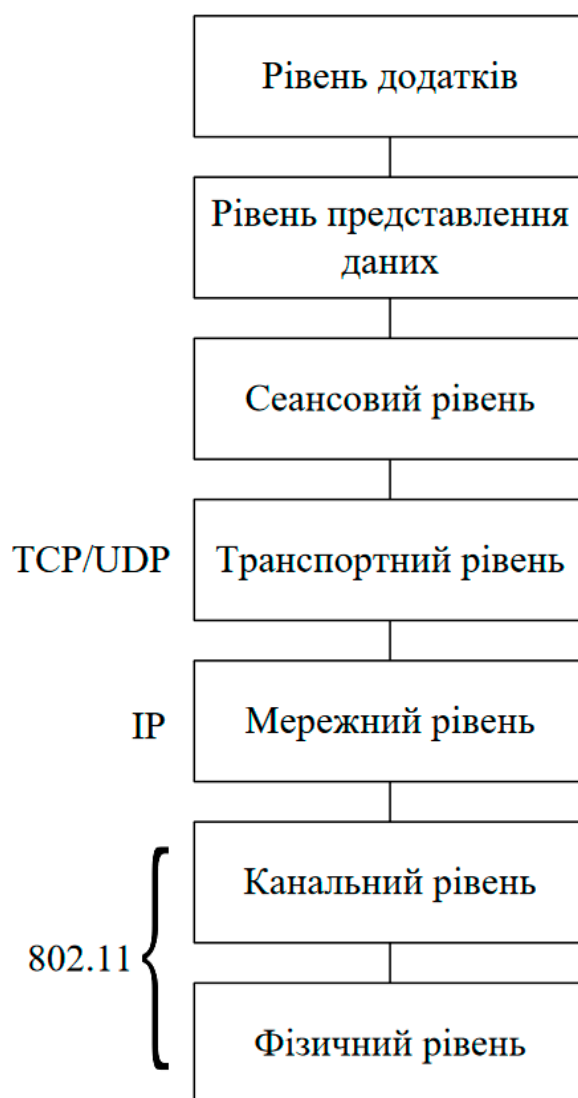


Рисунок 1.5 – Рівні моделі ISO / OSI і їх відповідність стандарту 802.11

1.2.1 Базовий стандарт IEEE 802.11

Стандарт IEEE 802.11 під назвою «Специфікація фізичного рівня та рівня контролю доступу каналів передачі в бездротових локальних мережах» був опублікований в середині літа 1997 року. Цей протокол визначає різні принципи архітектури мережі, форматів пакетів, конфіденційності та методів автентифікації, а також доступу пристрою до каналів зв'язку[7].

На ранніх етапах свого існування стандарт 802.11 працював на пристроях з частотою 2,4 ГГц і максимальною швидкістю 2 Мбіт/с. Базовий протокол 802.11 реалізує два методи передачі даних на фізичному рівні:

- 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 Стандарт 802.11a (Wi-Fi 2)

Стандарт IEEE 802.11a 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 революційним покращення в порівнянні з вихідним стандартом Wi-Fi.

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

1.2.3 Стандарт 802.11b (Wi-Fi 1)

Стандарт 802.11b використовує DSSS (Direct -Sequence Spread Spectrum) - метод модуляції, який працює у діапазоні 2,4 ГГц, що дозволяє досягти швидкості до 11 Мбіт / с. Діапазон 2,4 ГГц відмінно справляється з подоланням перешкод, забезпечуючи більше покриття Wi-Fi. 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 ГГц, продукти були набагато дешевші, ніж 802.11a, що зробило його більш популярним для домашніх мереж.

1.2.4 Стандарт 802.11g (Wi-Fi 3)

Стандарт IEEE 802.11g є покращенням 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 802.11b.

1.2.5. Стандарт 802.11n (Wi-Fi 4)

Wireless-N 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. Основні вдосконалення:

- багатоканальний вхід/вихід(MIMO);
- ширину смуги пропускання збільшено 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.

1.2.6 Стандарт 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.

1.2.7 Стандарт IEEE 802.11ah (WiFi HaLow)

Стандарт 802.11ah, прийнятий в травні 2017 року, 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.

1.2.8 Стандарт IEEE 802.11ac (гігабітний WiFi або WiFi 5)

В кінці 2008 року була утворена робоча група TGac, яка розпочала розробку стандарту 802.11ac. Головною метою цієї ініціативи є значне підвищення пропускнуої здатності стандарту 802.11, що дозволяє бездротовим мережам працювати на швидкості, конкуруючій із дротовими мережами Ethernet.

З метою підтримки нових програм та майбутніх випробувань пристроїв, TGac встановив три основні вимоги до продуктивності та функціональності стандарту 802.11ac.

Ефективність системи мережі. Вимоги до продуктивності та функціональності стандарту 802.11ac визначають досягнення максимальної пропускнуої здатності не менше 500 Мбіт/с у режимі однієї станції і не менше 1 Гбіт/с у режимі кількох станцій. Ці значення вимірюються на рівні керування

доступом (MAC) в точці доступу до служби (SAP) у діапазоні 5 ГГц, використовуючи ширину каналу 80 МГц або менше. Ця продуктивність пов'язана з рівнем MAC і не передбачає вирішення проблеми ефективності MAC лише за рахунок збільшення швидкості передачі фізичного рівня. Зазначено, що ці вимоги стандарту 802.11ac стосуються самого стандарту, а не окремих пристроїв. Згідно з документом, пристрій може вважати себе пристроєм 802.11ac, якщо він підтримує швидкість 293 Мбіт/с для одного користувача при використанні частоти 80 МГц і не надає підтримку для багатьох користувачів.

Зворотна сумісність. Стандарт 802.11ac призначений для зворотної сумісності та взаємодії з пристроями 802.11a/n. 802.11ac працює в діапазоні 5 ГГц, тому він несумісний із пристроями 802.11b/g.

Співіснування. В стандарті 802.11ac повинні бути вбудовані механізми для забезпечення співіснування пристроїв 802.11ac з вже впровадженими пристроями 802.11a/n.

Для забезпечення сумісності назад і співіснування, стандарт 802.11ac використовує технологічні схеми з 802.11n, де це можливо. Зокрема, він застосовує ту саму модуляцію OFDM на фізичному рівні та підтримує архітектуру кодування та чергування, аналогічну тій, що використовується в 802.11n. Проте для поліпшення продуктивності виконані певні зміни в існуючих функціях і введені нові.

Під час створення стандарту було виявлено ряд додатків, які вимагають підвищеної пропускної здатності. Ці додатки охоплюють шість основних моделей використання:

- велика пропускна здатність для передачі відео високої роздільної здатності та потокового відео: Стандарт 802.11ac забезпечує значну ширину каналу, що дозволяє без перешкод і затримок передавати високоякісне відео, включаючи потокове відео HD та 4K;

- підтримка мереж з великою кількістю підключень: Стандарт 802.11ac має підвищену щільність підключень, що дозволяє без значного втручання в продуктивність багатьом пристроям працювати одночасно в одній мережі;

– мобільність і роумінг: Стандарт 802.11ac підтримує можливість переходити між різними точками доступу в одній мережі без втрати з'єднання (роумінг), що робить його ідеальним для мереж інфраструктури в місцях з великими площами, такими як аеропорти і конференц-центри;

– підтримка VoIP і VoLTE: Завдяки високій пропускну́й здатності та низькій затримці, 802.11ac ідеально підходить для передачі голосу через IP (VoIP) та для мереж підтримки голосу через LTE (VoLTE);

– безпека і аутентифікація: 802.11ac підтримує різні методи безпеки, такі як WPA2 і WPA3, що забезпечують захист від несанкціонованого доступу та шифрування даних;

– використання в публічних мережах і готелях: 802.11ac широко використовується в публічних бездротових мережах, таких як Wi-Fi в готелях, кафе, аеропортах і торгових центрах, для забезпечення безкоштовного доступу до Інтернету для гостей і клієнтів.

Швидкість Wi-Fi визначається добутком трьох факторів: кількістю просторових потоків, пропускну́й здатності каналу, щільністю сузір'я. В цих трьох напрямках і розвивається в стандарт 802.11ac.

Пристрої 802.11ac оперують лише у діапазоні 5 ГГц. Рішення обмежити їх функціонування цим частотним діапазоном передусім пов'язане з вимогами щодо пропускну́й здатності каналу. У зв'язку із суттєвим зростанням пропускну́й здатності каналу, управління каналами стає проблемою, особливо в заповненому та роздробленому діапазоні 2,4 ГГц. Діапазон 5 ГГц дозволяє суттєво розширити смугу пропускання, доступну для бездротового зв'язку. Він також запобігає втручанню від пристроїв, які працюють у діапазоні 2,4 ГГц, таких як пристрої 802.11b/g, пристрої Bluetooth, мікрохвильові печі та інші. Всі канали розміщені в трьох діапазонах спектру: 5,170 - 5,330 ГГц; 5,490 - 5,730 ГГц і 5,735 - 5,835 ГГц. Стандарт 802.11n вимагає, щоб пристрої підтримували канали шириною 20 МГц, а також дозволяє використовувати додатковий канал шириною 40 МГц, об'єднуючи два канали по 20 МГц. Стандарт 802.11ac використовує цей простий метод для забезпечення високої пропускну́й здатності. Сусідні канали шириною 20 МГц

об'єднуються парами, утворюючи канали шириною 40 МГц, а сусідні канали шириною 40 МГц також об'єднуються парами, утворюючи канали шириною 80 МГц. Стандарт 802.11ac підтримує канали шириною 20, 40 і 80 МГц, а також дозволяє використовувати два суміжні канали шириною 80 МГц у режимі 160 МГц або два несуміжні канали в режимі 80+80 МГц, якщо це необхідно. Подвоєння пропускної здатності каналу від 40 МГц до 80 МГц є економічно ефективним засобом підвищення продуктивності. Всього можливо використовувати до 24 каналів шириною 20 МГц, до 11 каналів шириною 40 МГц, до 5 каналів шириною 80 МГц і 2 канали шириною 160 МГц. рисунок 1.6.

Частотні діапазони, що використовуються точками доступу та їх клієнтами в залежності від цілей зазвичай різні. Вибір частотного діапазону в цьому випадку залежить від того, на що спроможний клієнт.

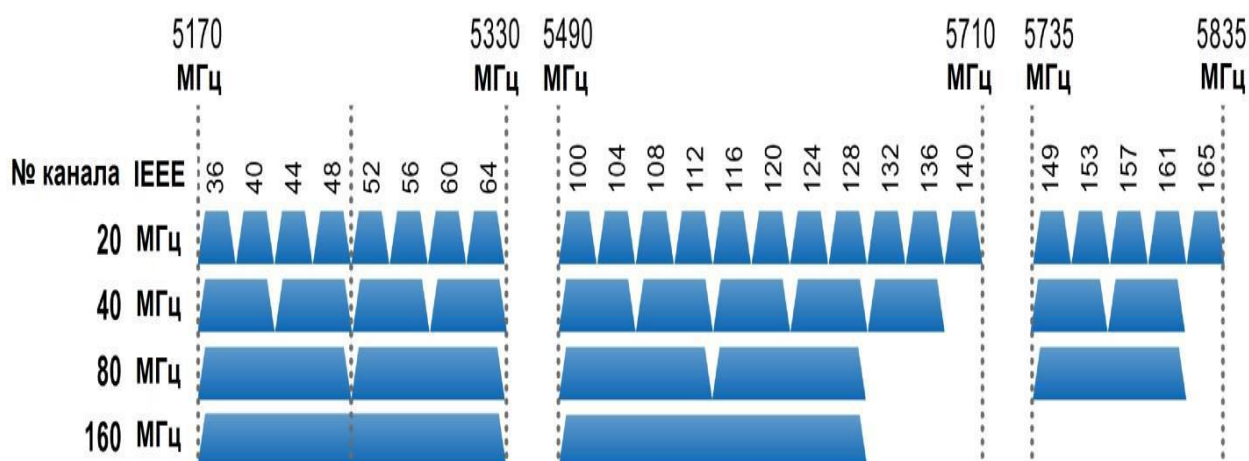


Рисунок 1.6 – Розміщення каналів у частотному діапазоні.

Підвищення пропускної здатності дозволяє кожному просторовому потоку підтримувати приблизно подвійну кількість бітів на символ. Таким чином, використання смуги пропускання 80 МГц для передачі одного потоку може забезпечити аналогічну продуктивність, що і використання смуги пропускання 40 МГц для передачі двох потоків. Для підтримки двох потоків передавач і приймач повинні мати принаймні дві антени, причому одна антена необхідна для передачі (або прийому) одного потоку. Таким чином, система 80 МГц вимагає менше

апаратного забезпечення для досягнення такої ж продуктивності, як система 40 МГц. Це призводить до зменшення енергоспоживання пристрою за рахунок використання меншої кількості радіочастотних компонентів. Хоча конструкція 80 МГц може бути більш витратною, ніж конструкція 40 МГц, система з вищою смугою пропускання зберігає перевагу в ціні. Проте системи з однією антеною не можуть гарантувати надійність, необхідну в певних сценаріях обслуговування. Для забезпечення стабільної передачі відео необхідно мати більшу кількість антен, ніж кількість просторових потоків [8].

Ефективна передача даних з використанням QoS вимагає врахування просторового розподілу, що є важливим елементом. Таким чином, навіть у системи з смугою пропускання 80 МГц необхідно використовувати кілька антен, якщо планується їх використання в застосунках, які потребують надійної передачі даних. Крім того, в реальних сценаріях продуктивність залежить не лише від швидкості фізичного рівня, а також від впливу перешкод від інших близьких мереж. Оскільки канали в стандарті 802.11ac є ширшими, імовірність ситуацій конфлікту збільшується. Для точки доступу з шириною смуги 80 МГц, яка обслуговує всіх клієнтів, стає складніше уникати перешкод від сусідніх мереж (наприклад, мережі 802.11n з шириною смуги 20/40 МГц). Це означає, що точка доступу 802.11ac має спільно використовувати той самий канал із кожною сусідньою точкою доступу, працюючи з нею лише протягом обмеженого часу. Крім того, недоліком системи 80 МГц є те, що всі чотири канали 20 МГц (або два канали 40 МГц) повинні бути вільними для початку передачі по всій ширині каналу 80 МГц. Передача з шириною смуги 20/40 МГц на будь-якій частині каналу 80 МГц призводить до перешкод для передачі на всьому діапазоні.

1.2.9 Стандарт IEEE 802.11ax(Wi-Fi 6)

Стандарт IEEE 802.11ax, відомий як Wi-Fi 6 за новою системою найменувань, володіє рядом характеристик. Першою ключовою особливістю є висока щільність мереж Wi-Fi. Це особливо актуально для місць з великою щільністю, де в одній області простору функціонує сотні точок доступу Wi-Fi. Подібні щільні розташування бездротових мереж часто зустрічаються в житлових або офісних

приміщеннях: сучасні квартири чи офіси, як правило, мають одну або навіть кілька точок доступу Wi-Fi [9].

Друга характеристика пов'язана із різноманітністю руху. У сценаріях використання мережі 802.11ax спостерігається високий рівень різноманітності трафіку, в контрасті до попередніх розширень Wi-Fi, де кожен сценарій зазвичай враховував лише один вид трафіку (наприклад, потокове відео в реальному часі, завантаження файлів або перегляд веб-сторінок). У сценарії 802.11ax клієнти одночасно використовують різні програми з різними видами трафіку.

Третьою особливістю є інтенсивне використання зв'язку в напрямку аплінку (uplink) у сучасних бездротових мережах, що може бути пояснено значущим обсягом завантажень, таких як фотографії, відео та документи, у соціальних мережах та хмарних сервісах.

Фізичний рівень, використовуваний у стандарті 802.11ax, зазвичай має спільні риси з розширеннями 802.11n і 802.11ac. Стандарт бездротових мереж 802.11ax використовує технологію мультиплексування з ортогональним частотним поділом (Orthogonal Frequency Division Multiplexing, OFDM). Метод модуляції OFDM використовує широкосмуговий сигнал і розбиває його на кілька смуг частот, які використовуються одночасно для передачі даних. Стандарт 802.11ax підтримує технологію OFDMA (Orthogonal Frequency Division Multiple Access), яка дозволяє розділяти кожен широкосмуговий канал на менші піднесені піддіапазони для ефективного одночасного обслуговування багатьох пристроїв. Також збільшено захисний інтервал (Guard Interval,) порівняно з попередніми стандартами Wi-Fi, щоб зменшити міжсимвольні перешкоди. Використання довших символів OFDM призводить до збільшення циклічного префіксу для кожного символу, що додає частину кінця символу OFDM до початку корисного навантаження передачі, щоб забезпечити захисний інтервал проти перешкод і покращити надійність. Стандарт IEEE 802.11ax підтримує вдосконалений механізм об'єднання каналів – виклювання преамбули, що дозволяє неперервно з'єднувати непослідовні канали, збільшуючи доступну пропускну здатність. Кожен кадр починається з преамбули, яка повторюється в кожному підканалі 20 МГц. Якщо ширина каналу перевищує

20 МГц., преамбула складається з двох частин: стандартної частини та преамбули 802.11ах. Стандартна преамбула зображена на рисунку 1.7.



Рисунок 1.7 – Стандартна преамбула та доповнення у преамбулі 802.11ах

Будь-яка станція Wi-Fi має можливість декодувати стандартну частину преамбули, що забезпечує зворотню сумісність. Преамбула містить заголовки LSTF (Legacy Short Training Field) і LLTF (Legacy Long Training Field) які використовуються для синхронізації та налаштування приймача в процесі прийому даних, це відображено на рисунку 1.8.



Рисунок 1.8 – Структура кадру 802.11ах

Преамбула стандарту 802.11ах може бути розкодована лише станціями, що підтримують 802.11ах. Ключовою є можливість швидко та точно відрізнити кадр 802.11ах від раніше переданого кадру. Для цього вирішено використовувати подвійне поле LSIG у стандартній частині преамбули. Станція 802.11ах розпізнає кадр 802.11ах, виявляючи дублювання поля LSIG. Нова преамбула включає обов'язкове поле HE-SIG-A, необов'язкове поле HE-SIG-B та спеціальну навчальну послідовність, необхідну для налаштування технології MIMO [9].

Поле HE-SIG-A має тривалість у два символи OFDM, якщо

використовується канал ширше за 20 МГц. Це поле дубльоване в кожному підканалі шириною 20 МГц і включає пакети обробки інформації, необхідні для прийому, такі як структура кодування сигналу (SCS), ширина каналу та кількість просторових потоків (Number of Spatial Streams). В попередніх варіантах стандарту Wi-Fi, деяку інформацію про протокол каналу передачі даних (MAC) було включено до преамбули пакета. В групі TGax цей підхід отримав додатковий розвиток. Наприклад, поле HESIG-A тепер містить інформацію, таку як унікальний ідентифікатор мережі, тривалість запланованої передачі (TXOP), прапор, який показує, чи це висхідна або низхідна лінія, і так далі. Включення цієї інформації в преамбулу дозволяє отримати важливі дані без необхідності повного декодування пакета. Це особливо корисно, оскільки службова інформація в полі HE-SIG-A може бути важливою не лише для призначеного отримувача, але й для інших станцій у мережі, тому надійна передача цього поля має велике значення. [10].

В разі багатокористувацької передачі неможливо помістити всю необхідну інформацію для управління передачею даних в поле HE-SIG-A. Для цього вводиться додаткове поле HE-SIG-B. Поле HE-SIG-B використовується для оптимізації передачі даних та містить індивідуальну службову інформацію для кожної станції і спільну для всіх приймальних станцій. При передачі через канал, ширина якого перевищує 20 МГц, поле HE-SIGB, так само, як і поле HE-SIG-A, реплікується в кожному підканалі 20 МГц. Однак для підвищення ефективності використання ресурсів каналу було вирішено використовувати наступний підхід: коли канал ширини ≥ 40 МГц використовується для передачі, два прилеглих підканали ширини 20 МГц містять різні частини поля HE-SIG-B, а решта підканалів повторюють цю інформацію. (рис. 1.9).

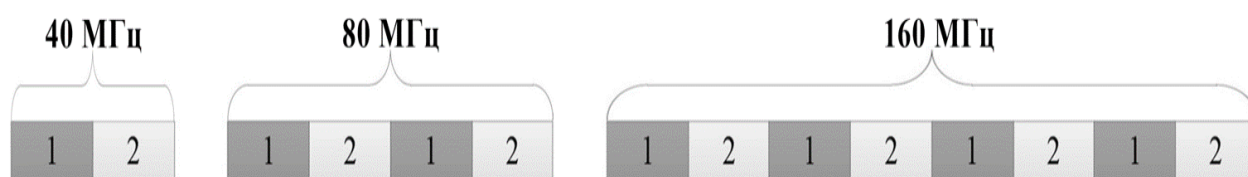


Рисунок 1.9 – Наповнення підканалів 20 МГц при передачі полів HE-SIG-B

Нарешті, давайте розглянемо нову схему модуляції, яку запропонувала робоча група TGax. Вперше додана функціональність дозволяє використовувати квадратурну модуляцію 1024-QAM у Wi-Fi мережах. Зрозуміло, що використання такої високопорядкової модуляції потребує значного відношення сигнал/перешкода/шум (SINR), що може викликати часті помилки декодування, і в основному підходить для приміщень, де відстань між передавачем і приймачем відносно невелика. Крім того, введення 802.11ax дозволяє використовувати модуляцію подвійної піднесучої (DCM). DCM передає ту ж інформацію на парі піднесучих, які розташовані достатньо далеко одна від одної в частотній області, щоб уникнути високих взаємних перешкод.

Передача службових кадрів вимагає значних ресурсів каналу. З метою зменшення накладних витрат через присутність службового трафіку, 802.11ax вводить заборону на передачу маячків та багатьох інших службових кадрів зі швидкістю менше 5,5 Мбіт/с у діапазоні 2,4 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 [11].

1.3.1 Протокол безпеки WEP

Одночасно з публікацією базового стандарту IEEE 802.11 механізм захисту Wired Equivalent Privacy (WEP) також був схвалений IEEE. WEP (Wired Equivalent Privacy) — це технологія стандарту 802.11, яка забезпечує безпеку передачі інформації. Шифрування даних здійснювалося за допомогою алгоритму RC4 для ключів зі статичною складовою від 40 до 104 біт і додатковим стартовим вектором 24 біт. Це означає, що всі дані були зашифровані за допомогою ключа від 64 до 128 біт. Протокол WEP не призначений для повного захисту інформації від зловмисників, а лише для того, щоб зробити її нечитабельною. Основним завданням цієї технології було шифрування потоків даних, що передаються по бездротових мережах. Для підвищення захисту використовуються так звані вектори ініціалізації (IV). Це призначено для рандомізації додаткової частини ключа, таким чином забезпечуючи різні шифри для різних пакетів даних. Цей вектор має 24 біти. Результатом є загальне шифрування з розрядністю від 64 ($40 + 24$) до 128 ($104 + 24$) бітів..

Сам процес шифрування WEP відбувається у два етапи:

- на початку обчислюється значення контрольної суми цілісності (ICV) за допомогою алгоритму циклічної перевірки надмірності (CRC-32). Цей алгоритм використовується шляхом додавання його в кінець незашифрованих повідомлень і забезпечує перевірку цілісності, прийнятої сторонами;
- шифрування здійснюється безпосередньо на другому етапі.

Ключ для шифрування WEP є загальною таємницею, яку повинні знати пристрої з обох сторін бездротового з'єднання даних. Цей 40-бітний закритий ключ разом із 24-бітним випадковим вектором ініціалізації (IV) є вхідною послідовністю для генератора псевдовипадкових чисел на основі шифру Вернама, який генерує випадкову послідовність символів, яка називається потоком ключів. Цей процес виконується, щоб уникнути методів злому, заснованих на статистичних властивостях звичайного тексту. Вектор ініціалізації використовується для надання кожному повідомленню власного унікального потоку ключів. Зашифровані повідомлення створюються при виконанні операції XOR над незашифрованим

повідомленням з ICV і ключовим потоком. При отриманні інформації від іншої сторони відбувається протилежний процес ($p = c+b$). Значення b обчислюється одержувачем, застосовуючи код Вернама до вхідної послідовності, що складається з ключа K (відомого заздалегідь) і IV , доставленого відкритим текстом разом з тим самим повідомленням. Для кожного наступного пакета процес повторюється з використанням нововибраного значення IV . Однією з добре відомих властивостей алгоритму RC4 є те, що використання того самого значення ключа та вектора ініціалізації завжди призводить до того самого значення b . Таким чином, застосувати операцію XOR до двох текстів, зашифрованих RC4 з однаковим значенням b , неможливо, окрім як XOR перших двох текстів (лістинг 1.1).

Лістинг 1.1 – Операції XOR до двох текстів

$$\begin{aligned} c1 &= p1 + b & c2 &= p2 + b \\ c1 + c2 &= p1 + b + p2 + b = p1 + p2 \end{aligned}$$

Тобто, ви можете отримати відкритий текст, який є результатом операції XOR між двома іншими вихідними текстами. Етапи їх видалення не складні. Наявність оригінального тексту та IV дозволяє розрахувати ключ, який згодом дає можливість читати всі повідомлення в цій бездротовій мережі. Після деякого простого аналізу легко обчислити, коли b повториться знову. Оскільки ключ K постійний, а кількість варіантів IV дорівнює $2^{24} = 16\,777\,216$, середній розмір пакета для бездротової мережі з достатнім завантаженням точки доступу становить 1500 байт (12 000 біт), а середня швидкість передачі даних становить 5 Мбіт/с (до 11 Мбіт/с), бачимо, що точка доступу надсилає 416 повідомлень на секунду, або рівно 1 497 600 повідомлень на годину. Це повторення займає 11 годин 12 хвилин ($2^{24} / 1\,497\,600 = 11,2$ години). Ця проблема називається «векторне зіткнення». Існує багато способів прискорити цей процес. Крім того, може бути використана атака «відомий відкритий текст», коли одному з користувачів мережі надсилається повідомлення з відомим вмістом і прослуховується зашифрований трафік. В даному випадку, коли три з чотирьох компонентів відомі

(незашифрований текст, вектор ініціалізації і зашифрований текст), можна обчислити ключ.

1.3.2 Протокол безпеки WPA

Стандарт WPA був представлений Wi-Fi Alliance. WPA означає бездротовий захищений доступ. Стандарт WPA представив TKIP (протокол цілісності тимчасового ключа), еволюцію WEP, щоб забезпечити кращу безпеку. WPA також представив автентифікацію користувача верхнього рівня для пристроїв 802.11. Описує два методи автентифікації користувача:

- початковий ключ (рукописання EAPOL(Extensible Authentication Protocol over LAN));
- 802.1X тимчасові ключі для автентифікації користувача [12].

Обидва вищевказані механізми автентифікації включають автентифікацію користувача, а також генерують набір ключів шифрування, які можуть бути використані для захисту даних (рис. 1.10).

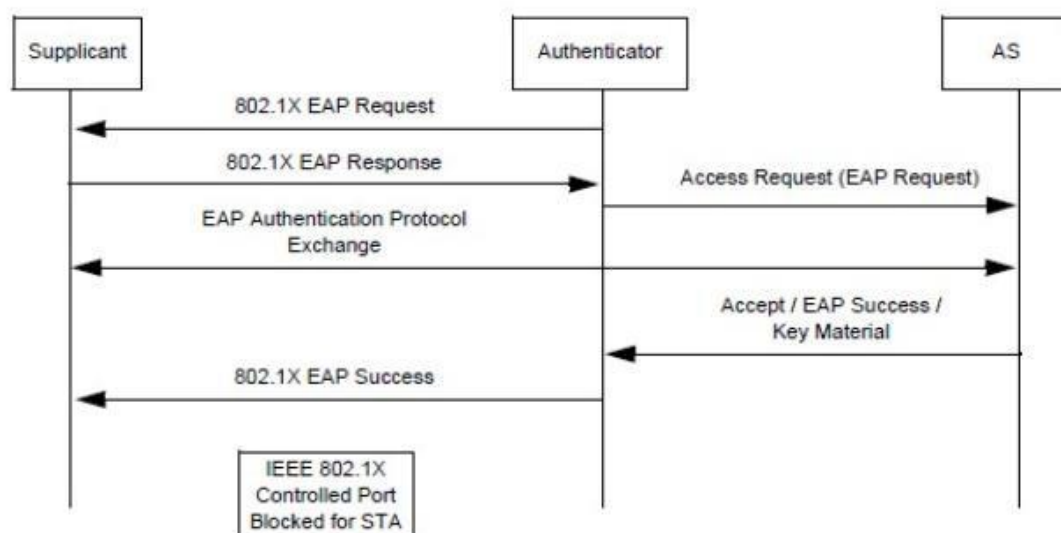


Рисунок 1.10 – Автентифікація EAP, яка забезпечує парний головний ключ для рукописання EAPOL

Процес встановлення тимчасових ключів, які використовують EAPOL для обміну інформацією, автентифікації і ключів включають три етапи:

- після успішної аутентифікації клієнта та точки доступу визначається чи використовується механізм автентифікації за допомогою загальнодоступного ключа 802.1X;
- для забезпечення групового шифрування трафіку між всіма учасниками мережі проводиться Group Key Handshake, під час якого встановлюються тимчасові групові ключі
- головний ключ використовується в чотирьох сторонньому рукоштовуванні EAPOL, отриманому тимчасовими ключами для шифрування даних в кінці фази три.

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

- інформаційні елементи WPA (захисний бездротовий доступ);
- RSN(Robust Security Network) (надійна мережа безпеки).

Інформаційний елемент WPA наведено на рисунку 1.11. Будь-яка станція, що містить інформаційний елемент WPA / RSN у своєму запиті на асоціацію, повинна виконати рукоштовування безпеки 802.11i / 802.1X.

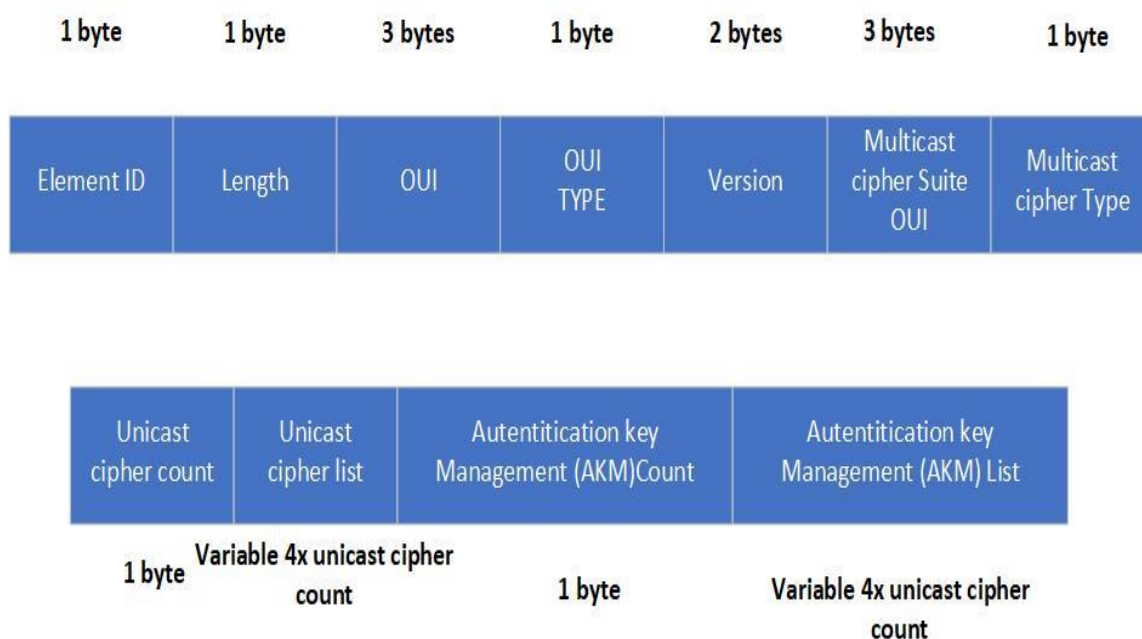


Рисунок 1.11 – Інформаційний елемент WPA

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 (Organizational Unique Identifier) потрібно перевірити AP/Station, щоб побачити, чи є інформаційний елемент WPA. Якщо це не WPA - AP/Station може вирішити ігнорувати аналіз інформаційного елемента, деякі шифри наведені в таблиці 1.1.

Таблиця 1.1 – Списки шифрів

Ідентифікатор OUI	Тип люкс	Значення
00-50-f2	0	Використовується 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 (Temporal Key Integrity Protocol) - 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 введений групою IEEE 802.11i. RSN позначає надійну мережу безпеки, і вона зробила шифр AES обов'язковим при використанні надійної мережі безпеки.

Шифр TKIP може використовуватися як широкосмуговий / широкомовний шифр, а також WEP-40 / WEP104, але якщо метод автентифікації 802.1X, то WEP-40 / WEP-104 / TKIP також не дозволено використовувати як груповий шифр. TKIP як парний шифр з WEP-40 / WEP104 як груповий шифр також не підтримується. Інформаційний елемент RSN наведено на рисунку 1.12. Розмір IE (Information Element) RSN обмежений максимум 255 байтами [13].



Рисунок 1.12 – Структура RSN формату

1.3.3 Протокол безпеки WPA2

Стандарт IEEE 802.11i, також відомий як Wi-Fi Protected Access 2 (WPA2), є доповненням до стандарту 802.11, який визначає механізми безпеки для бездротових мереж. Проект стандарту був затверджений на початку літа 2004 року. Він замінює попередню специфікацію безпеки Wired Equivalent Privacy (WEP), яка мала серйозні недоліки безпеки. Захищений доступ Wi-Fi (WPA) раніше був представлений як проміжне рішення проблем безпеки з WEP. WPA реалізовано лише частину IEEE 802.11i. WPA2 використовує спеціальний режим Advanced Encryption Standard (AES), відомий як CBC-MAC Block Chain Code Authentication Protocol (CCMP). CCMP забезпечує як конфіденційність (шифрування), так і цілісність даних. Використання Advanced Encryption Standard (AES) є більш безпечною альтернативою потоковому шифруванню RC4, яке використовується WEP і WPA [14].

Стандарт WPA2 складається з двох важливих компонентів для безпечної бездротової мережі: шифрування та автентифікації. Елемент шифрування WPA2 використовує AES (Advanced Encryption Standard), але TKIP (Temporal Key Integrity Protocol) доступний для зворотної сумісності з існуючим обладнанням WAP. Автентифікації WPA2 передбачає два режими: Personal і Enterprise.

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

Корпоративний режим потребує індивідуальної автентифікації користувача на основі стандарту автентифікації IEEE 802.1X і використовує розширюваний протокол автентифікації (EAP), розширюваний протокол автентифікації, який дозволяє вибирати з п'яти стандартів EAP:

- EAP-MD5 (Extensible Authentication Protocol with Message Digest 5);
- безпека рівня EAP-транспортного рівня (EAP-TLS);
- безпека тунельного транспортного рівня з підтримкою EAP (EAP-TTLS);
- захищений протокол автентифікації виклику рукостискання EAP vo / EAPMicrosoft;
- v2 (PEAPvo / EAP-MSCHAPv2);
- захищена карта EAP v1 / EAP-Generic (PEAPv1 / EAPGTC) та модуль посвідчення абонента EAP-абонента Глобальної системи мобільних комунікацій (EAPSIM).

EAP-MD5 використовує алгоритм MD5 для обчислення хеш-значення для пароля, яке надсилається на сервер і порівнюється зі збереженим хеш-значенням. Протокол EAP-FAST дозволяє автентифікацію за допомогою логіна та пароля та спеціального токена з PEAP-GTC. Протоколи PEAP-34 MSCHAPv2 і EAP-TLS виконують автентифікацію на основі сертифікатів клієнта..

Тільки WPA2-Enterprise та поєднання цифрових сертифікатів безпеки та протоколів EAP-TLS або EAP-TTLS забезпечують максимальний захист вашої мережі Wi-Fi. Сертифікати — це попередньо згенеровані файли на серверах RADIUS і клієнтських пристроях. Клієнт і сервер автентифікації перевіряють ці файли один на одного, щоб забезпечити захист від несанкціонованих підключень з інших пристроїв і від підроблених точок доступу. Протокол EAP-TTL/TTLS є частиною стандарту 8021X і використовує інфраструктуру відкритих ключів (PKI) для обміну даними між клієнтами та RADIUS. PKI використовує закритий ключ

(відомий користувачеві) і відкритий ключ (зберігається в сертифікаті та потенційно відомий усім) для автентифікації. Ці комбінації ключів забезпечують надійну автентифікацію. Список протоколів відображено на рисунку 1.13.

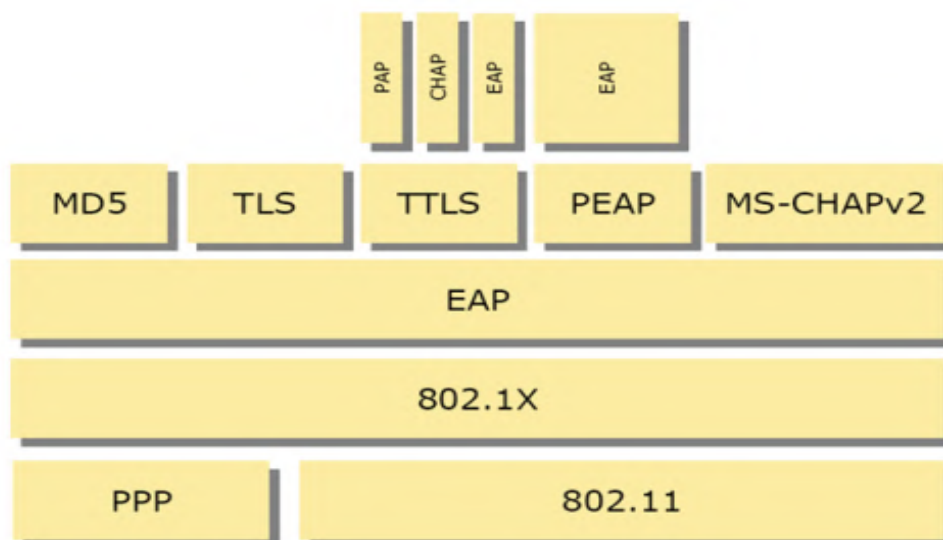


Рисунок 1.13 – Список протоколів

WPA2 створює безпечну лінію зв'язку в чотири етапи. На першому кроці точка доступу та сторони клієнта узгоджують політику безпеки, яку вони підтримують (методи автентифікації, протоколи для одноадресного трафіку, протоколи для багатоадресної передачі та методи попередньої автентифікації).

Другий етап (стосується лише корпоративного режиму). Однією з ключових змін у стандарті WPA2 є відокремлення автентифікації користувача від забезпечення цілісності та конфіденційності повідомлень, що забезпечує більш масштабовану та надійну архітектуру безпеки як для домашніх, так і для корпоративних мереж.

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 PMK (Pair-mud Master Key), який буде використаний пізніше при генерації ключів.

Автентифікація в корпоративному режимі WPA2 базується на стандарті автентифікації IEEE 802.1X. Основними компонентами є суб'єкт (клієнт), який приєднується до мережі, автентифікатор, який керує доступом (точка доступу діє як автентифікатор), і сервер автентифікації (RADIUS), який приймає рішення щодо авторизації.

Автентифікатор (AP) розділяє кожен віртуальний порт на два логічних порти, один для обслуговування та один для автентифікації, утворюючи PAE (об'єкт доступу до порту). Автентифікація PAE завжди відкрита, але служба PAE відкривається лише після успішної автентифікації на сервері RADIUS.

Автентифікатор перетворює повідомлення EAPoL на повідомлення RADIUS і пересилає його на сервер RADIUS. Сервер автентифікації має бути сумісним із типом EAP запитувача та приймати й обробляти запити на автентифікацію. Після завершення процесу автентифікації заявник і сертифікатор отримують секретний МК (Master Key), як показано на рисунку 1.14.

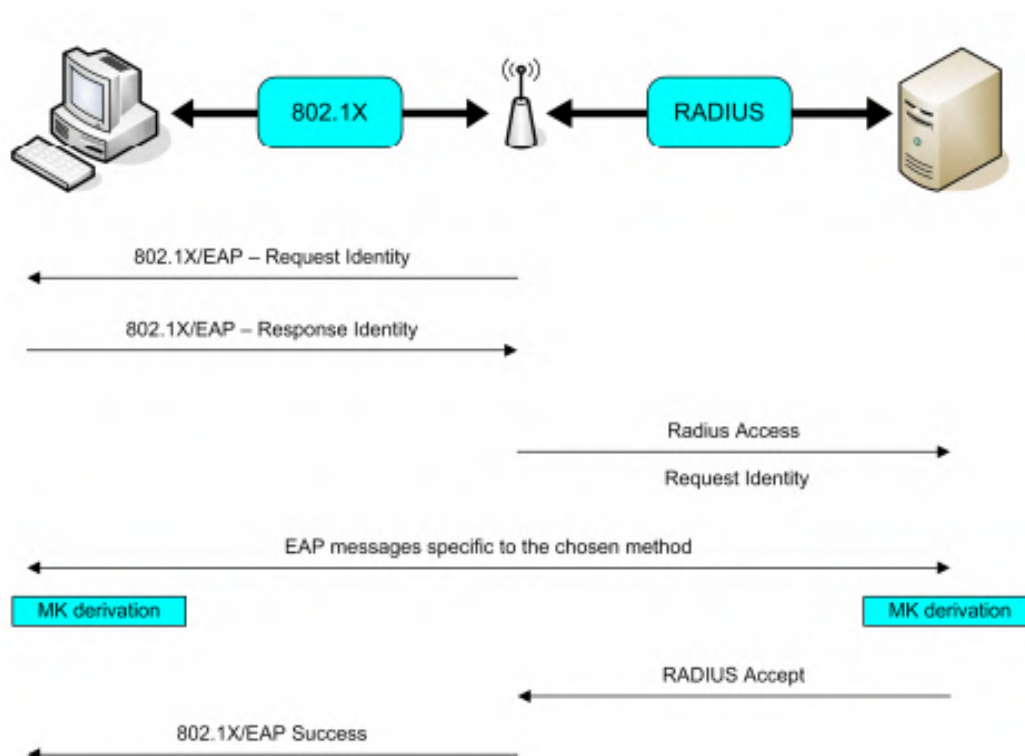


Рисунок 1.14 – 802.1X автентифікація

1.3.4. Протокол безпеки 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 AP. 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:

- домашня мережа, де користувачі автентифікуються за допомогою загальнодоступного пароля;
- 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 рукописання WPA3 є Pairwise Master Key (PMK), який згодом використовується для виконання 4-х напрямного рукописання для отримання клавiші "Pairwise".

1.4 Механізм доступу до середовища

1.4.1 Фізичний рівень (Physical layer) стандарту IEEE 802.11

Стандарт IEEE 802.11 визначає передачу сигналу за допомогою одного з двох методів: розширений спектр прямої послідовності (DSSS) і розширений спектр зі стрибками частоти (FHSS). Ці схеми використовують однакову технологію розширеного спектру, хоча модуляція різна. Основним принципом технології розширеного спектру (SS) є перетворення вузькосмугового спектру сигналу, створеного традиційним прихованим кодуванням, у широкосмуговий спектр, що може значно підвищити надійність переданих даних. Метод FHSS змінює несучу частоту сигналу.

Для підвищення несприйнятливості необхідно збільшити частотний спектр сигналу, що передається. У цьому випадку несуча частота змінюється відповідно до псевдовипадкових законів, і кожен пакет даних передається на цій несучій частоті. При використанні FHSS конструкція трансивера дуже проста, але оскільки цей метод підходить лише для ситуацій, коли пропускна здатність не перевищує 2 Мбіт/с, IEEE 802.11b додає DSSS. Можна побачити, що лише пристрої IEEE 802.11, які підтримують DSSS, можуть взаємодіяти з пристроями IEEE 802.11b, не маючи швидкості передачі, що перевищує максимальну швидкість (2 Мбіт/с) у вузькому місці. Тобто пристрої, які використовують старіші стандарти та не вдосконалені [14].

Метод DSSS заснований на принципі фазової маніпуляції (тобто передачі інформації шляхом раптових змін у початковій фазі сигналу). Щоб розширити спектр сигналу мовлення, передана інформація перетворюється в псевдовипадкову

послідовність, так званий код Баркера. Для кожного переданого біта в послідовності Баркера є 11 біт. Існують прямі послідовності Баркера та зворотні послідовності Баркера. Через високу надлишковість кодування ймовірність того, що перешкода змінить пряму послідовність Баркера на зворотну послідовність Баркера, близька до нуля.

Прямий код Баркера передає логічну одиницю, тоді як інвертований код відображає логічний нуль. Для бездротових комп'ютерних мереж у діапазоні 2,4 ГГц використовується обмежений «коридор» шириною 83 МГц, розділений на 14 каналів. З метою усунення взаємних перешкод між цими каналами, їх смуги частот розділяються на 25 МГц.

Простий розрахунок показує, що в даній зоні можна використовувати лише три канали одночасно. У такому випадку автоматичне перетворення частоти не вирішить проблему шумозаглушення, тому WLAN використовує дуже надмірний код. Якщо ці заходи не забезпечують достатню захищеність передачі даних, швидкість буде поступово зменшуватися від максимального значення 11 Мбіт/с до одного із наступних фіксованих значень: 5,5; 2; 1 Мбіт/с. Уповільнення відбувається не тільки при значній кількості перешкод, але й при достатньо великій відстані між елементами бездротової мережі.

1.4.2 Канальний рівень

Подібно до дротової мережі Ethernet, рівень зв'язку бездротової комп'ютерної мережі Wi-Fi включає підрівень керування логічним з'єднанням (LLC) і підрівень керування доступом до медіа (MAC). Ethernet і IEEE 802.11 використовують ту саму LLC, що дозволяє легко поєднувати дротові та бездротові мережі. Незважаючи на те, що між двома стандартами MAC є багато подібностей, є також деякі нюанси, важливі при порівнянні дротових і бездротових мереж. Ethernet використовує виявлення та обробку колізій, щоб забезпечити множинний доступ до загального середовища передачі, у цьому випадку кабелю. Протокол CSMA/CD використовується для ввімкнення. Це називається одночасним початком передачі.

Мережі IEEE 802.11 використовують напівдуплексний режим передачі, що

означає, що в будь-який момент станція може отримувати або передавати інформацію, унеможливлюючи виникнення колізій під час передачі. Для протоколу IEEE 802.11 була створена модифікована версія протоколу CSMA/CD під назвою CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Робота цього протоколу виглядає наступним чином: перед тим, як станція передає інформацію, вона спочатку "слухає ефір". Якщо на робочій частоті не виявлено активності, станція чекає випадковий проміжок часу, а потім знову "прослуховує трансляцію". Якщо носій даних все ще вільний, станція передає інформацію.

Випадкова затримка необхідна, щоб уникнути затору в мережі, якщо кілька станцій одночасно намагаються отримати доступ до цієї частоти. У випадку, коли пакет надійшов без порушень, приймаюча станція висилає підтвердження. Цілісність пакету перевіряється за допомогою контрольної суми. Після отримання підтвердження станція-відправник вважає передачу цього пакета завершеною. У випадку, якщо підтвердження не надійшло, станція припускає, що сталася колізія, і повторно передає пакет після випадкового періоду часу.

Ще одна трудність, характерна для бездротових мереж, полягає в обмеженій взаємодії між двома клієнтськими станціями, незважаючи на те, що кожна з них має стабільне з'єднання з точкою доступу. У такому випадку транспортний клієнт може надіслати запит до точки доступу для оптимізації використання повітря. Після цього, отримавши вказівку від точки доступу, інші клієнтські станції припиняють передачу під час "спілкування" між двома точками з менш ефективним зв'язком.

Примусовий бездротовий режим (протоколи Request to Send/Clear to Send - RTS/CTS) не є стандартним для всіх пристроїв у мережах IEEE 802.11 і, навіть якщо він включений, активується лише у виняткових ситуаціях. У мережах Ethernet, при передачі поточкових даних, використовується загальний контроль доступу до каналу, що призначений для всіх станцій. Натомість, у стандарті IEEE 802.11 для цього застосовується централізоване керування від точки доступу.

Клієнтські станції послідовно запитують можливість передачі поточкових даних. Якщо яка-небудь станція вказує, що планує передавати поточкові дані, точка

доступу відводить їй часовий інтервал, протягом якого сама передає дані з усіх станцій в мережі. Слід відзначити, що використання примусового видалення повітря призводить до зниження ефективності бездротових мереж через короточасні перерви в передачі додаткової службової інформації та комунікації. У дротовій мережі Ethernet можна досягти не лише напівдуплексної, але і повнодуплексної передачі, при виявленні колізій (що підвищує фактичну пропускну здатність мережі). Отже, на жаль, при інших однакових умовах фактична пропускну здатність бездротової мережі IEEE 802.11b буде нижчою, ніж у дротового Ethernet.

Отже, якщо ви надаєте однакове навантаження обом мережам, Ethernet 10 Мбіт/с та IEEE 802.11b (максимальна швидкість передачі 11 Мбіт/с), і поступово збільшуєте навантаження, то, починаючи з певного порогу, мережа IEEE 802.11b почне "сповільнюватися", тоді як Ethernet продовжить нормально працювати.

Оскільки клієнтами можуть бути мобільні пристрої з автономним живленням, стандарт IEEE 802.11 приділяє велику увагу керуванню живленням. Зокрема, визначено режим, коли клієнтська станція періодично "прокидається" для прийому сигналу пробудження від точки доступу. Якщо отримано цей сигнал, клієнтський пристрій активується, в іншому випадку він повторно переходить у "режим сну" до наступного циклу отримання інформації.

2 АНАЛІЗ МЕТОДІВ ОЦІНЮВАННЯ ПРОДУКТИВНОСТІ БЕЗДРОТОВИХ МЕРЕЖ

Номінальна швидкість передачі даних є одним з основних показників, але не повною мірою характеризує продуктивність і ефективність розгортання мережі Wi-Fi. У більшості випадків пропускну спроможність не є ключовою вимогою,

оскільки на продуктивність мережі також впливають загасання, перешкоди та неефективні сценарії й умови конфігурації мережі. Для розрахунку Wi-Fi мереж на базі стандарту IEEE 802.11 Джузеппе Б'янчі запропонував модель для розрахунку пропускної здатності в залежності від кількості підключених пристроїв.

В основі лежить ідея передачі даних в ідеальному каналі, де немає прихованих вузлів. Для аналізу використовується умова насичення мережі, а одиницею масштабу мережевого часу є віртуальний слот. Ця позиція може бути трьох видів: «порожня», «вдала» і «зіткнення». Коли слот порожній, кожна станція не передає дані, і канал порожній. У вдалому слоті пакети передаються від однієї зі станцій. Слот вважається колізією, якщо він передається від двох або більше станцій. Передавальна станція передає з тією ж імовірністю τ . Основним припущенням є постійна ймовірність зіткнення пакета p , переданого кожною станцією, незалежно від кількості вдалих повторних передач. Поведінка окремих станцій описується ланцюгом Маркова.

На основі наведених вище ідей буде реалізована модель системи для IEEE 802.11ax. В якості вихідних даних візьмемо мережу за стандартом IEEE 802.11ax, що складається з однієї точки доступу (ТД) і N станцій користувача. Усі станції знаходяться в зоні видимості ТД та інших станцій. Вони можуть передавати та отримувати дані, використовуючи однакову схему модуляції та кодування, а також мають схожі параметри. Крім того, ми дотримуємося ідеї ідеальних фізичних умов каналу передачі та фокусуємося на рівні MAC [15].

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. 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.

Щоб розрахувати пропускну здатність мережі, ми не повинні забувати про можливість колізій, тривалість колізій і успішність передачі кадру. Згідно з наведеними вище умовами та на основі методу розрахунку Джузеппе Б'янчі, формула для розрахунку пропускну здатності низхідного каналу дорівнюватиме:

$$S_d = \frac{T_{data}}{T_{csi} + T_{data}} * \left(\frac{a_1 * N_a * L_D + a_3 * V_u * N_a * L_d}{b_1 * T_e + \sum_{i=1}^4 a_i * (T_{ai} + T_e) + \sum_{i=1}^4 c_i * (T_{ci} + T_e)} \right), \quad (2.1)$$

для каналу вверх:

$$S_u = \frac{T_{data}}{T_{csi} + T_{data}} * \left(\frac{a_2 * N_a * L_D + a_4 * V_u * N_a * L_d}{b_1 * T_e + \sum_{i=1}^4 a_i * (T_{ai} + T_e) + \sum_{i=1}^4 c_i * (T_{ci} + T_e)} \right), \quad (2.2)$$

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 інакше вузли не зможуть зменшити свої лічильники відкату/повернення. T_{data} враховує час, що використовується для зондування каналу.

Наступним етапом дослідження є практична перевірка цього методу шляхом математичного моделювання в Matlab. Серед отриманих графіків виділимо графіки пропускну спроможності в залежності від кількості користувачів, ширини каналу та числа антен. На графіках (див. рис. 2.1) показана пропускну здатність DL і UL, досягнута мережами на основі стандарту IEEE 802.11ax ($\alpha=0,2, \beta=0,8$).

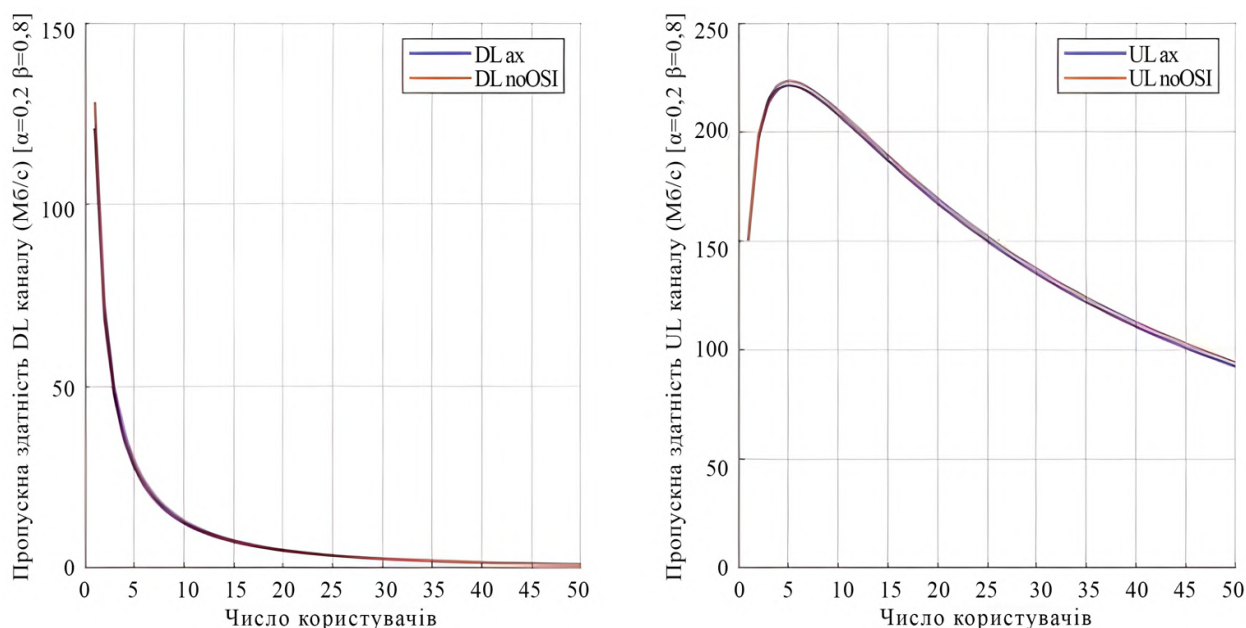


Рисунок 2.1 – Пропускна здатність в залежності від кількості користувачів

Як видно, порівняно з попередником у сімействі IEEE 802.11, вища пропускна здатність досягається як у висхідному, так і в низхідному потоці завдяки збільшенню кількості кадрів, об'єднаних в одному A-MPDU, з 64 до 256 і підтримці багатокористувацької передачі, включаючи велику кількість станцій.

Наведена система забезпечує вищу пропускну здатність як у висхідному, так і в низхідному потоці. Зверніть увагу, що механізм прослуховування каналу не впливає на загальну продуктивність системи IEEE 802.11ax. Це пов'язано з тим, що користувачькі станції надсилають інформацію про стан каналу CSI до точки доступу паралельно, а не послідовно, як у стандарті IEEE 802.11ac, що може значно зменшити втрати часу для великої кількості користувачьких станцій.

Графіки на рисунку 2.2 показують пропускну здатність DL і UL в залежності від ширини каналу. Очевидно, що зі збільшенням ширини каналу пропускна здатність висхідної та низхідної лінії збільшується. Також зверніть увагу, що зі збільшенням максимального розміру A-MPDU пропускна здатність низхідної лінії зменшується [16].

Цей результат пояснюється процесом EDCA, який надає однакову пропускну здатність всім претендентам, якщо використовуються однакові параметри CW_{min} і CW_{max} .

Оскільки користувачські станції передають певний час, пропорційний максимальному розміру A-MPDU, збільшення цього значення зменшує кількість доступного ефірного часу, виділеного для ТД. Отже, використання великих кадрів A-MPDU негативно впливає на продуктивність ТД, тому слід бути обережним при налаштуванні цього параметра.

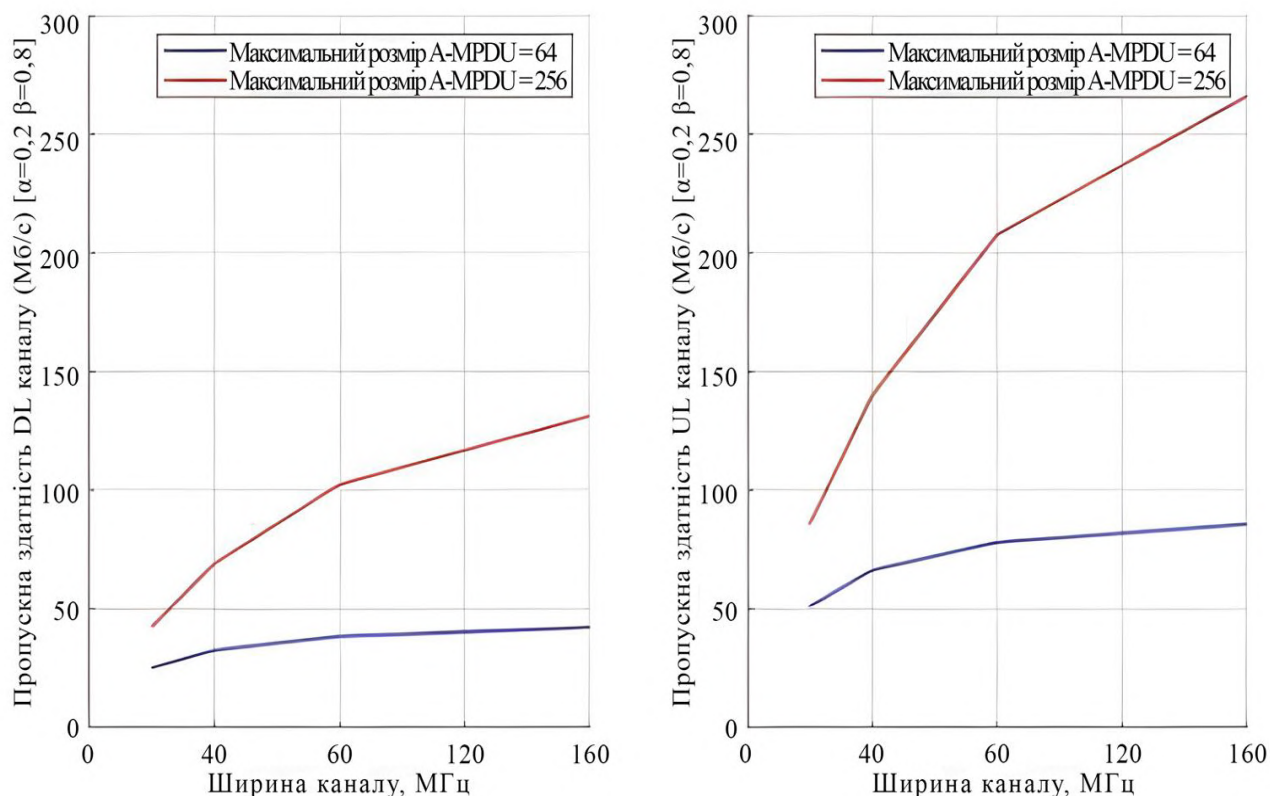


Рисунок 2.2 – Пропускна здатність в залежності від ширини каналу

Збільшення кількості антен в ТД збільшує кількість просторових потоків, що використовуються для однокористувацьких та багатокористувацьких передач.

Як показано на рисунку 2.3, кількість станцій, мультиплексованих в кожному RU, збільшується пропорційно кількості просторових потоків, виділених кожному користувачеві при однокористувацьких передачах, тому пропускна здатність низхідної лінії збільшується зі збільшенням кількості антен в ТД.

Однак кількість антен, які можуть бути встановлені на абонентській станції, обмежена двома. Зауважимо, що виграш від збільшення кількості антен зростає пропорційно ширині каналу [17].

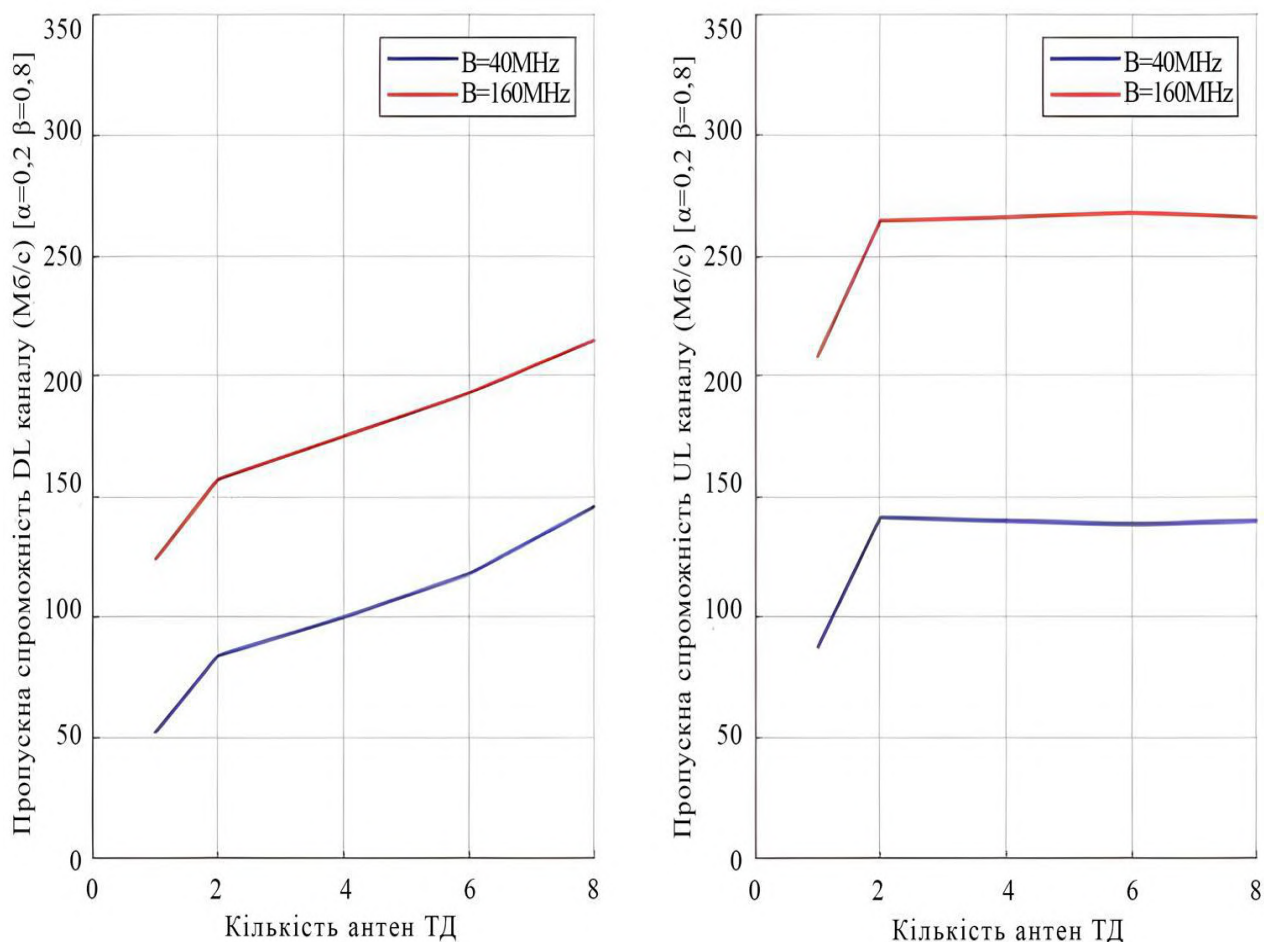


Рисунок 2.3 – Пропускна здатність в залежності від кількості антен

Отримані результати показують, як працюють мережі на основі стандарту IEEE 802.11ax в різних конфігураціях, в тому числі вплив швидкості прослуховування каналу, максимального розміру A-MPDU, ширини каналу і кількості антен на точку доступу на пропускну здатність мережі. Доведено необхідність правильної розстановки пріоритетів при плануванні багатокористувацьких передач DL і UL, щоб уникнути колізій з користувацькими станціями і оптимізувати пропускну здатність WLAN. Запропоновано модель, яка враховує часові витрати фізичного та каналного рівнів доступу до каналу для сегментів мережі IEEE 802.11ax. Модель також враховує необхідність врахування як однокористувацьких, так і багатокористувацьких сценаріїв передачі на низхідних і висхідних каналах при розрахунку пропускну здатності каналу мережі IEEE 802.11ax. Недоліком цієї роботи є те, що вона не враховує вплив фізично

генерованих втрат і гетерогенного трафіку. Крім того, ряд припущень, таких як рівновіддаленість всіх станцій, відсутність прихованих вузлів і насиченість мережі, також можуть змінити загальну пропускну здатність мережі.

Постійне збільшення кількості пристроїв призвело до появи концепції бездротових локальних мереж високої щільності. Іншими словами, мережа Wi-Fi високої щільності - це бездротове середовище з високою концентрацією активних користувачів. Сюди відносяться, наприклад, мережі у великих аудиторіях, конференц-залах, торгових залах, на стадіонах тощо. Крім того, мережа високої щільності також може бути мережею, розгорнутою між кількома периферійними сусідніми мережами або зонами обслуговування, які перекривають зони покриття одна одною.

У таких ситуаціях часто виникають додаткові проблеми у вигляді інших мереж, розгорнутих в зоні покриття розглянутої мережі, клієнтів інших мереж, зона покриття сигналу яких знаходиться в зоні покриття мережі, та інших джерел сигналу в частотному діапазоні, що використовується. У цьому випадку навіть добре спроектована Wi-Fi мережа на базі традиційного стандарту IEEE 802.11, що забезпечує хороший рівень сигналу і співвідношення сигнал/шум, не може забезпечити адекватну продуктивність через недостатнє робоче середовище. Основним обмежуючим фактором є час, протягом якого середовище передачі зайняте.

Це пов'язано з тим, що середовище передачі необмежене і має бути спільним для всіх клієнтів і точок доступу. Цей обмежувальний фактор також пов'язаний з основним механізмом розподілу доступу до середовища CSMA/CA (багатостанційний доступ з контролем несучої та уникненням колізій). Хоча цей механізм не є оптимальним з точки зору досягнення максимально можливої швидкості передачі, саме завдяки йому мережі Wi-Fi здатні повністю розкрити свій потенціал [18].

CSMA/CA - це мережевий протокол канального рівня (MAC), в якому вузли намагаються уникати колізій. Загальний алгоритм проілюстровано на рисунку 2.4.

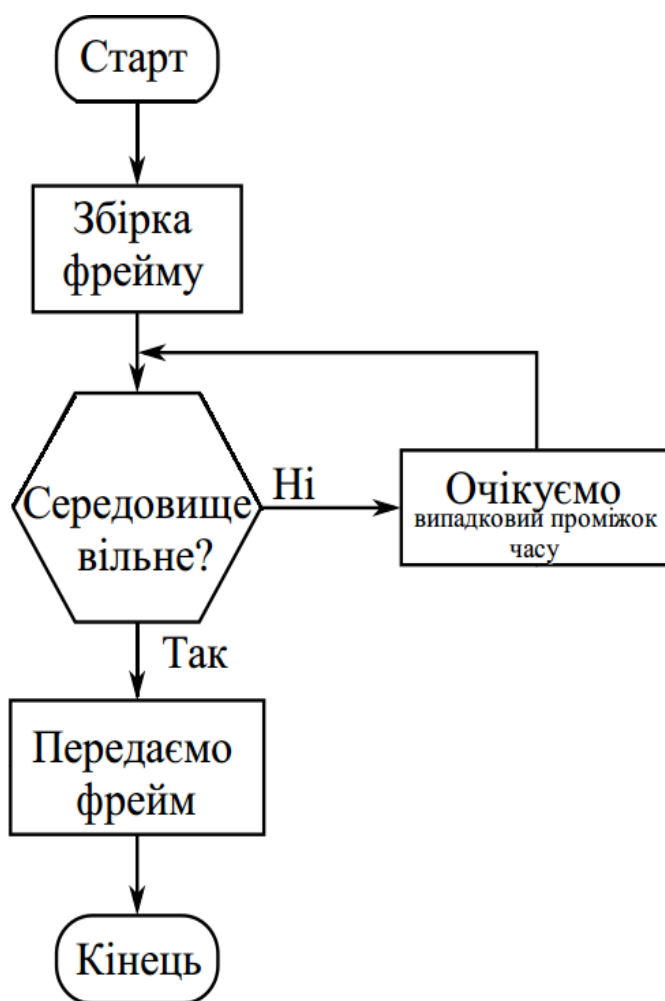


Рисунок 2.4 –Алгоритм роботи CSMA/CA

Однак цей алгоритм схильний до проблеми так званих прихованих вузлів, коли один вузол може спілкуватися з точками доступу, але не безпосередньо з іншими вузлами, і незахищених вузлів, коли один вузол помилково вважає, що він не може передавати через активність сусідніх передавачів.

Приймальні вузли R1 і R2 перебувають поза зоною дії один одного, а зони дії передавальних вузлів S1 і S2 перетинаються. У цій ситуації S1 передає сигнал на R1, а вузол S2 помилково вважає, що передача на R2 неможлива, оскільки середовище зайняте S1, що призводить до колізії. Однак R2 перебуває поза зоною дії S1 і тому може прийняти передачу S2, не викликаючи інтерференції (об'єднання хвиль при їх складанні з результатом зміни амплітуди).

У прикладі, показаному на рисунку 2.5, вузол S2 не захищений.

Проблема незахищеного вузла



Рисунок 2.5 – Затримка в роботі незахищеного вузла

Для вирішення цих проблем у звичайних мережах IEEE 802.11 може бути використаний протокол RTS/CTS (Request To Send/Clear To Send).

У протоколі RTS/CTS замість надсилання кадру даних станція, яка бажає зайняти середовище, повинна спочатку відправити станції призначення короткий службовий кадр RTS. Станція призначення повинна відповісти службовим повідомленням CTS(free to transmit), після чого відправник може передати кадр даних; кадр CTS повинен бути надісланий станції, яка перебуває поза зоною дії передавальної станції, але в зоні дії приймальної станції, тобто прихованому терміналу передавальної станції, якому про зайняття середовища необхідно повідомити. Після передачі даних передавальна станція очікує кадру ACK (Acknowledgement) для підтвердження того, що дані були отримані і що пакет був переданий правильно. Якщо протягом певного часу ACK не отримано, пакет вважається втраченим через колізію. Тоді станція збільшує затримку і повторює спробу надсилання пакета.

Цей протокол підходить у тому випадку, коли всі учасники однаково ділять канал у межах загальної зони покриття, однак зі збільшенням кількості пристроїв у мережі збільшується і кількість службових кадрів, що призводить до нелінійного зростання затримки доступу.

3 МОДЕЛЮВАННЯ МЕРЕЖІ

Планування і проєктування є ключовими факторами при розгортанні мережі Wi-Fi. Через особливості технології для забезпечення високої пропускну здатності, низької затримки і високої стабільності з'єднання необхідно враховувати наявність інших мереж у зоні покриття, передбачувану кількість активних пристроїв, а також планування і характеристики будівлі. У традиційних мережах IEEE 802.11 не реалізовано механізмів ефективного розподілу ресурсів радіочастотного спектра для сценаріїв із великою кількістю клієнтів. Крім того, в традиційних мережах IEEE 802.11 суворо дотримується правило, згідно з яким у зоні покриття активний тільки один пристрій. Це означає, що в таких мережах немає механізму, що дає змогу використовувати середовище одночасно з іншою зоною обслуговування, що перекривається, за умови дотримання умов, що виключають можливість шкідливого мовлення в інших зонах. У результаті традиційні мережі IEEE 802.11 не підходять для щільного розгортання, і для забезпечення оптимальної продуктивності в таких середовищах потрібні спеціальні методи проєктування.

3.1 Радіообстеження місцевості розгортання

Радіочастотні дослідження є важливою частиною як етапу планування, так і етапу проєктування. Вони проводяться з метою збору емпіричних даних про радіочастотний діапазон конкретного об'єкта. Основна перевага проведення радіочастотного обстеження порівняно з традиційним плануванням полягає в тому, що можна отримати найточніші дані для конкретного об'єкта. Хоча ця процедура актуальна як до, так і після розгортання мережі, дані, отримані під час планування,

можуть бути використані для уникнення багатьох проблем, пов'язаних із перешкодами сигналу та покриттям, а також для мінімізації переміщення точок доступу.

Радіообстеження перед розгортанням проводяться насамперед для визначення характеристик об'єкта. Якщо існуюча мережа відсутня, ця процедура дозволяє зібрати дані про радіочастотні характеристики об'єкта, такі як загасання сигналу через стіни та інші перешкоди, а також виявити інші мережі та джерела сигналу в сусідніх діапазонах. Якщо існуюча мережа потребує модернізації, цей метод може виявити недоліки та проблеми мережі, які можна врахувати вже на етапі проєктування.

Метод AP-on-a-Stick також може бути використаний на цьому етапі. У цьому методі для імітації покриття мережі використовується тестова точка доступу. Ця тестова точка доступу встановлюється на штатив і розміщується в передбачуваному місці розташування точки доступу. Потім тестується фактична зона покриття приміщення, щоб виявити фактори, які послаблюють сигнал. Процес повторюється, при необхідності точку переміщують на нове місце.

Після збору даних створюється карта покриття, що імітує вже розгорнуту мережу.

Основна перевага цього методу полягає в тому, що дослідження можна проводити за допомогою точок доступу, які будуть встановлені в приміщеннях під час фактичного розгортання мережі. Це забезпечує найбільш точну характеристику майбутнього покриття в конкретній будівлі.

Верифікаційне обстеження можна проводити одразу після розгортання мережі. Після того, як мережа на об'єкті спроектована і точки доступу встановлені, необхідно перевірити, чи працює мережа належним чином. На цьому етапі можна виявити багато проблем з мережею, наприклад, якщо встановлені точки доступу були неправильно налаштовані або орієнтовані під час встановлення. У таких випадках карта покриття може суттєво відрізнятися від тієї, що була отримана під час планування та попередніх досліджень. Дослідження після встановлення також можуть виявити особливості середовища, які були недоступні на етапі планування,

наприклад, вплив сусідніх точок доступу, обладнання, що заважає, меблів , тощо.

Радіообстеження також може бути прямим інструментом діагностики під час експлуатації вже розгорнутої та функціонуючої мережі. Воно дозволяє виявити проблеми або обмеження, які виникли з моменту останнього обстеження.

Процедура радіообстеження не замінює планування мережі, а скоріше доповнює і покращує його. Попереднє планування дозволяє уточнити характеристики середовища, а перевірка - підтвердити правильність розгортання. У мережах високої щільності вартість розгортання без попереднього планування, ймовірно, буде значно вищою, оскільки розміщення точок і їх конфігурація можуть потребувати коригування. Радіорозвідка сама по собі не може замінити комплексне проєктування, так само як і планування не може повністю виключити радіорозвідку.

Радіообстеження можна розділити на два типи: пасивні та активні.

Під час пасивного обстеження досліджуються всі точки доступу і канали, що використовуються на об'єкті, щоб визначити оптимальну конфігурацію мережі. Під час пасивного обстеження збирається вся інформація про навколишнє середовище, включаючи сусідні та цільові точки доступу і джерела сигналу. Це дозволяє отримати інформацію про всі канали і рівень сигналу в досліджуваному діапазоні. Внутрішньо і міжканальні перешкоди та інтерференція сигналів є основними причинами зниження пропускної здатності і нестабільної роботи обладнання.

Пасивні дослідження можна проводити до або після розгортання мережі. Якщо вони проводяться до розгортання, результати використовуються для оптимізації вибору каналів точок доступу, щоб мінімізувати міжканальні перешкоди від сусідніх передавачів. У випадку, якщо дослідження проводиться після розгортання мережі, воно допомагає переконатися у відсутності проблем або в тому, що проблеми були оптимально вирішені [19].

Активне обстеження дозволяє дослідити характеристики і зону покриття розгорнутої мережі. Активне обстеження досліджує зону покриття на рівні окремих точок доступу або мережі в цілому. В основному воно використовується як метод перевірки для визначення відповідності проєктним вимогам до пропускної

здатності та покриття. Проведення активного обстеження перед розгортанням мережі дозволяє краще спланувати розміщення та орієнтацію точок доступу.

Спектральний аналіз навколишнього середовища може бути частиною процедури радіообстеження. Перешкоди на сусідніх частотах, не пов'язаних з бездротовою мережею, можуть значно підвищити загальний рівень шуму і зробити смугу практично непридатною для передачі даних. Джерелами таких перешкод можуть бути як незалежні пристрої, такі як мікрохвильові печі, Bluetooth-пристрої, бездротові клавіатури і передавачі маніпуляторів в діапазоні 2,4 ГГц, так і компоненти інших технічних рішень, наприклад, метеорологічні радіолокаційні станції в діапазоні 5 ГГц.

3.2 Проєктування мереж із зменшенням домену колізій

При необхідності розгортання мереж в умовах високої щільності застосовується методика проєктування зі зменшенням домену колізій.

Зазвичай основну частину інтерференції становлять перешкоди від сторонніх мереж Wi-Fi або суміжних точок доступу. На великих площах, на кшталт торгових центрів, дуже містких навчальних аудиторій, конференц-залів, стадіонів тощо, зазвичай спостерігається висока інтерференція у спектрі, який використовується Wi-Fi. Часто це пов'язано з відсутністю численних перешкод поширенню радіосигналу та велику кількість користувачів середовища передачі. Якщо в зоні покриття точки доступу виявляється інша точка, що працює на тому ж каналі, виникають ефекти внутрішньоканальної інтерференції CCI (Co-Channel Interference). Як правило, в мережах високої щільності розміщується велика кількість точок доступу, багато з яких можуть працювати на одному каналі. Чим більше таких точок, тим більше буде спостерігатися ефект внутрішньоканальної інтерференції.

Виразність ефекту CCI залежить від багатьох факторів, таких як: тип точки

доступу, тип і характеристики антен, розташування та орієнтація точки та інші, залежно від кількості клієнтів. При цьому, слід тримати можливу інтерференцію на мінімальному рівні. Ефекти внутрішньоканальної інтерференції є основною причиною проблем експлуатації мереж з високою щільністю. У цьому сенсі метою планування бездротової локальної мережі є забезпечення того, щоб загальна пропускна здатність мережі залишалася незмінною навіть при подальшому збільшенні кількості точок доступу.

Міжканальна інтерференція сигналів (ACI, Adjacent Channel Interference) проявляється, коли у спектрі перетинаються смуги сигналів, що передаються у різних каналах. У бездротових локальних мережах це явище зустрічається дуже часто і є неминучим через використання коміркового принципу їх побудови, що передбачає перетин зон покриття точок доступу, що працюють на різних каналах.

На рисунку 3.1 зображена структура мережі із традиційним методом проєктування, в якому спостерігається надмірна потужність передавачів і перекриття зон обслуговування [17].

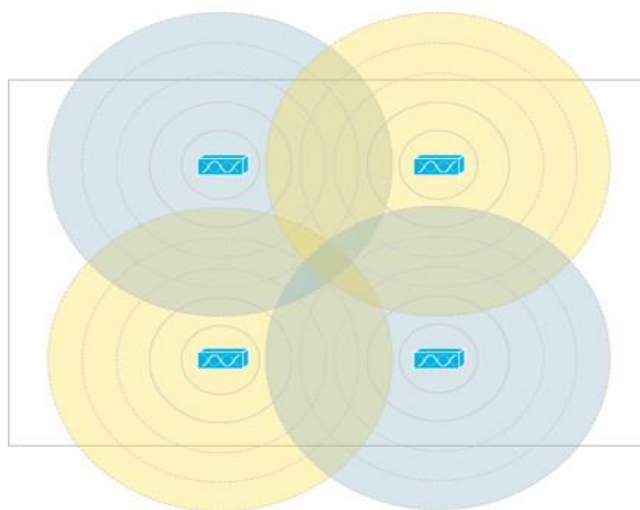


Рисунок 3.1 – Традиційне розміщення

Збільшивши кількість використовуваних точок доступу і зменшивши рівень їхнього сигналу, можна розмістити клієнтів фізично ближче до точки доступу, яка їх обслуговує. На рисунку 3.2 зображена структура мережі із використанням

методу зменшення доменів колізій.

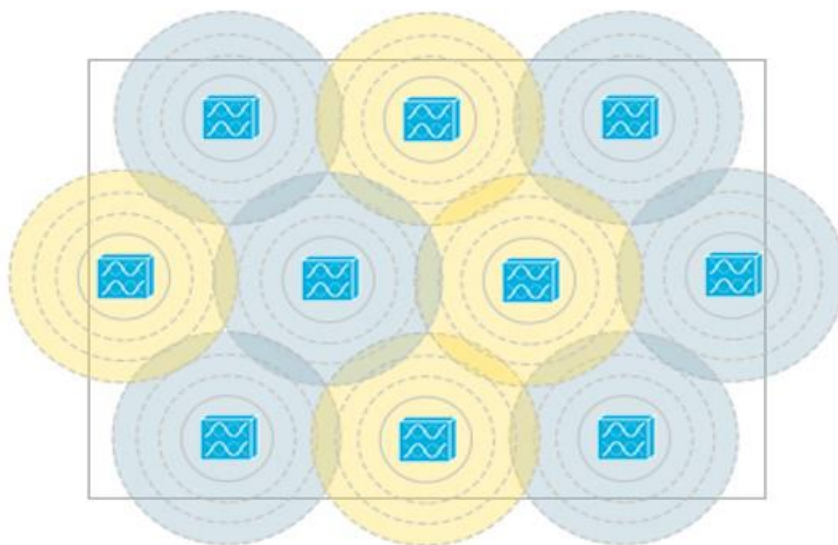


Рисунок 3.2 – Зменшення домену колізій

Для зменшення впливу описаних ефектів застосовують метод проєктування мереж із зменшенням доменів колізій. Сенс методу полягає у розміщенні більшої кількості точок доступу на тій же площі та обмеження потужності їхніх передавачів для забезпечення мінімального оптимального перекриття зон обслуговування для забезпечення роумінгу клієнтів

Зменшення кількості клієнтів на одну точку доступу також може значно зменшити вплив інтерференції сигналів між клієнтами. Крім того, можлива більш ефективна модуляція і більш швидкісні канали. Варто також відзначити, що магістральна дротова мережа завантажується більш рівномірно, зменшуючи інтерференцію з сусідніми бездротовими мережами.

Використовуючи описані методи, наприклад, каналного і фізичного розділення точок доступу, можна не тільки зменшити проблеми, пов'язані з перешкодами, але і практично повністю усунути вплив обмежуючих факторів, таких як потужність бездротових клієнтських передавачів. У багатьох випадках потужність передавача клієнта значно (в рази) нижча за потужність передавача точки доступу. Якщо не враховувати цей фактор належним чином і орієнтуватися

переважно на покриття передавачів точок доступу, то ймовірно виникнення ситуації, коли клієнт бачить точку доступу може приймати від неї сигнал, однак точка доступу не бачить сигнал клієнта через малу потужність його передавача.

3.3 Коефіцієнт ослаблення сигналу Wi-Fi

У бездротових каналах зв'язку спостерігаються два основні типи загасання сигналу: загасання відстані та загасання множинних шляхів. Загасання відстані (Path Loss) виникає внаслідок поширення сигналу в просторі. Зі збільшенням відстані між передавачем і приймачем сигнал втрачає енергію через розповсюдження в середовищі, а також через поглиблення та відбиття від перешкод, таких як будівлі, гори, дерева тощо. Чим далі сигнал подорожує, тим менше його потужність на приймачі. Загасання множинних шляхів (Multipath Fading) виникає внаслідок того, що сигнал може досягти приймача за різними шляхами, наприклад, прямим і відбитим від стін або інших перешкод. Коли ці різні екземпляри сигналу досягають приймача з різних напрямків і в різний час, вони можуть між собою інтерферувати, що призводить до зниження якості сигналу.

Для бездротового підключення Wi-Fi важливо враховувати, які перешкоди перебувають на шляху поширення сигналу. Наявність капітальних стін, листового металу, штукатурки на стінах, і інших матеріалів може впливати на якість сигналу та суттєво погіршувати функціональність Wi-Fi-пристроїв (рис. 3.3) [18].

Всередині приміщення радіосигнал може зазнавати перешкод внаслідок наявності дзеркал та тонованих вікон. Важливо зазначити, що послаблення сигналу в діапазоні 2,4 ГГц та 5 ГГц при проходженні через різні види перешкод значно відрізняється, але очікувано для 5ГГц сигнал значно більше втрачає потужність. Різниця в загасанні цих двох діапазонів в більшості матеріалів складає 1-3 дБ, проте в міжкімнатних стінах, стелях, шахтах ліфтів може досягати більше 10 дБ.

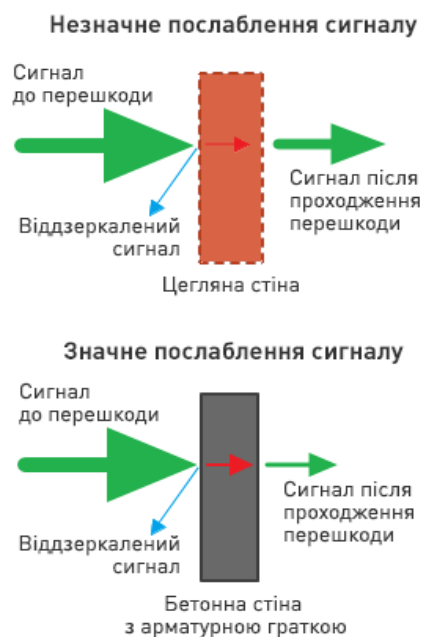


Рисунок 3.3 – Загасання сигналу під час проходження перешкод

У таблиці 3.1 наведено значення загасання типових перешкод, узагальнені на основі історичних емпіричних даних. Фактичні значення загасання залежать від результатів обстеження місця [19].

Таблиця 3.1 – Загасання сигналу через різні види перешкод

Перешкода	Товщина (мм)	Загасання сигналу 2,4 ГГц (дБ)	Загасання сигналу 5 ГГц (дБ)
Міжкімнатна стіна	120	10	20
Несуча стіна	240	15	25
Бетонна підлога/стеля	240	25	30
Азбест	8	3	4
Шахта ліфту	80	30	35
Спінені матеріали	8	3	4
Деревина пустотіла	20	2	3
Міжкімнатні дерев'яні двері	40	3	4
Двері з масиву дерева	40	10	15
Звичайне скло	8	4	7
Товсте скло	12	8	10
Броньоване скло	30	25	35
Несучий стовп	500	25	30

3.4 Вибір програмного та апаратного комплексу для дослідження

Для досягнення високої ефективності в мережах, розгорнутих на підприємствах, необхідні різноманітні візуальні та професійні інструменти, оскільки бездротові перешкоди мають непередбачуваний та невидимий характер.

На ринку програмного забезпечення (ПЗ) для моделювання зони покриття бездротових точок доступу Wi-Fi мереж є таке ПЗ:

- Ekahau Site Survey;
- TamoGraph Site Survey;
- D-link Wi-Fi Planner PRO;
- NetAlly AirMagnet Survey Pro.

Ekahau Pro Site Survey – це програмне забезпечення, спрямоване на менеджерів, інженерів і фахівців у сфері бездротових мереж, а також на професіоналів Wi-Fi. Воно призначене для планування, розгортання та підтримки життєздатних мереж 802.11. Цей програмний продукт надає інструменти для зручного планування, швидкого дослідження, візуального представлення даних, а також функції розширеного аналізу, оптимізації та звітності. Усі ці функції можуть використовуватися одночасно завдяки єдиному та простому в управлінні інтерфейсу, спрямованому на користувача. Недоліком є висока вартість ліцензії 12085 USD.

TamoGraph Site Survey – це потужне та зручне програмне забезпечення для бездротового обстеження сайтів для збору, візуалізації та аналізу даних Wi-Fi 802.11 a/b/g/n/ac/ax. Для розгортання та обслуговування бездротової мережі потрібне використання професійного радіочастотного інструменту обстеження місця, який полегшує виконання трудомістких і дуже складних завдань, таких як поточний аналіз і звітність про силу сигналу, шум і перешкоди, розподіл каналів, швидкість передачі даних тощо [12].

Використовуючи TamoGraph, можливо значно скоротити час і витрати, які потрібні для розгортання та підтримки мереж Wi-Fi, а також покращити

продуктивність мережі та покриття в будь-якому середовищі: офісні будівлі, аеропорти, кафе, торгові центри або відкриті простори. Для некомерційного використання існує версія Evaluation з деякими обмеженнями.

D-link Wi-Fi Planner PRO – це інструмент моделювання радіочастот, призначений для спрощення розгортання бездротових мереж (WLAN) [13]. Це простий і ефективний інструмент для планування Wi-Fi-мереж перед їх фактичним впровадженням. Wi-Fi Planner PRO надає комплексну візуалізацію обстановки Wi-Fi перед реальним розгортанням, що в значній мірі спрощує планування та взаємодію з клієнтами щодо впровадження WLAN..

NetAlly AirMagnet Survey – це професійне програмне рішення для проектування та планування локальних бездротових мереж стандартів 802.11a/b/g/n/ac/ax. Воно дозволяє розрахувати необхідну кількість, розміщення та конфігурацію точок доступу під час проектування та впровадження WLAN. AirMagnet Survey виконує завдання, пов'язані з вивченням мереж Wi-Fi, включаючи створення карт покриття, аналіз шумів і визначення продуктивності в завданнях користувачів з підтримкою стандарту 802.11ax.. Недолік - немає підтримки в Україні.

Оскільки більшість програмного забезпечення вимагає придбання дорогої ліцензії, серед усіх зазначених програм для моделювання зони покриття точки доступу для проведення навчальних та наукових досліджень обираємо TamoGraph Site Survey, оскільки воно має безкоштовну версію Evaluation.

Розглянемо основні функції TamoGraph:

- радіочастотне планування - створення віртуальних моделей і планування майбутніх WLAN;
- комплексне оцінювання бездротової мережі (WLAN) з супровідною візуалізацією сигналу, перешкод, областей покриття точок доступу та швидкості передачі даних, виявлення можливих проблем у мережі.;
- автоматичне визначення місця розташування точок доступу;
- детальна інформація про кожну точку доступу (канал, максимальна швидкість передачі даних, провайдер, тип шифрування) для кожної точки доступу;

– повна підтримка мереж 802.11ах.

Система дає змогу проводити пасивні, активні та прогнозні дослідження.

Для визначення експлуатаційних характеристик мереж у ході експериментального дослідження будемо використовувати застосунок iPerf3[17].

iPerf — програма для вимірювання швидкості передачі даних у мережах, розроблена The Energy Sciences Network/Lawrence Berkeley National Laboratory.

Ця програма дозволяє вимірювати максимально досяжну пропускну здатність мережі в обох напрямках передачі.

Платформа iPerf3 для Windows розроблена як консольна програма.

Нижче наведено набір ключів, які дозволяють налаштувати параметри завантаження, список найважливіших параметрів та їх функції:

- iperf в режимі сервера ключ «s»;
- режим клієнта ключ «c»;
- налаштування часу для передачі або отримання ключ «t»;
- налаштування розміру вікна TCP, більші вікна можуть розвинути більшу пропускну здатність ключ «w»;
- реверсивний режим, де сервер надсилає, а клієнт отримує ключ «r»;
- встановлення інтервалу звітів ключ «i».

Як клієнтський пристрій для експериментального вимірювання продуктивності будемо використовувати ноутбук Lenovo ThinkBook 15. Найбільш важливим технічним критерієм даного пристрою в тестах є наявність модуля Wi-Fi Intel AX201, що підтримує стандарт IEEE 802.11ах. Ноутбук має антену 2x2, тобто підтримує MU-MIMO 2x2.

Такі параметри ноутбука повністю забезпечують можливість проведення необхідних тестів та дозволяють легко масштабувати проєкт. Наявність накопичувача SSD дозволить без перешкод задавати максимальну необхідну швидкість.

Зовнішній вид ноутбука представлено на рисунку 3.4.



Рисунок 3.4 – Ноутбук Lenovo ThinkBook 15

Технічні характеристики ноутбука:

- процесор – i3-1115G4 (3.0 –4.1 ГГц);
- графічний процесор – Intel UHD Graphics Xe;
- оперативна пам'ять – 16ГБ, DDR4;
- накопичувач SSD 256 ГБ;
- Wi-Fi модуль Intel AX201;
- 1 Гбіт/с Ethernet.

Технічні характеристики мережевого контролеру Intel AX201:

- підтримка антени 2x2;
- MU-MIMO;
- підтримка IEEE 802.11ax;
- максимальна швидкість –2,4 Гбіт/с (160 МГц на 5 ГГц).

В якості точки доступу використовуємо маршрутизатор TP-Link Archer AX1500. Цей пристрій підтримує роботу як в якості маршрутизатору так і точки доступу. Чотири антени охоплюють більше напрямків та розширюють зону покриття. Зовнішній вид представлено на рисунку 3.5.



Рисунок 3.5 –Маршрутизатор TP-Link Archer AX1500

Для з'єднання із дротовою мережею має інтерфейс Ethernet 1 Гбіт/с. Для підтримки роботи багатьох користувачів оснащений 1,5 ГГц трьох'ядерним процесором Broadcom BCM6750. Пристрій підтримує такі засоби мережевої безпеки:

- міжмережевий екран SPI;
- контроль доступу;
- прив'язка IP і MAC;
- шлюз прикладного рівня.

Бездротові характеристики наведені в таблиці 3.2.

Таблиця 3.2 – Бездротові характеристики TP-Link Archer AX1500

Бездротова мережа	Характеристики
Стандарти	IEEE 802.11ax/ac/n/a 5 ГГц IEEE 802.11n/b/g 2,4 ГГц
Швидкість Wi-Fi	AX1500 5 ГГц – 1201 Мбіт/с (802.11ax) 2,4 ГГц – 300 Мбіт/с (802.11n)

Продовження таблиці 3.2

Бездротова мережа	Характеристики
Технології Wi-Fi	OFDMA Одночасно обмінюється даними з декількома підключеними пристроями з підтримкою стандарту Wi-Fi 6
	Airtime Fairness Підвищує ефективність мережі за рахунок обмеження надмірного навантаження
	Target Wake Time зменшує споживання енергії підключеними пристроями.
Шифрування WiFi	WEP WPA WPA2 WPA/WPA2-Enterprise (802.1x)

4 ОЦІНЮВАННЯ ПРОДУКТИВНОСТІ МЕРЕЖІ ПРИ ЗМІНІ ПАРАМЕТРІВ

4.1 Налаштування програмно-апаратного комплексу

4.1.1 Налаштування програми TamoGraph Site Survey

Одним із підходів до дослідження обрано метод моделювання. Тестова мережа спроектована в середовищі TamoGraph Site Survey, в цьому ж середовищі змодельовані її робочі характеристики. Для моделювання обрано перший поверх офісного приміщення. Бездротове покриття потрібно забезпечити в приміщеннях 1-17, тому на них і зосереджена основна увага.

Висота між поверхами будівлі становить 2,8 метри, при цьому кожне перекриття має висоту 2,8 метра. Загальна товщина перекриттів будівлі складає 30 см і виготовлена з залізобетону. Зовнішні стіни мають товщину приблизно 25 см, а внутрішні - 9 см. Загальний план приведено на рисунку 4.1.

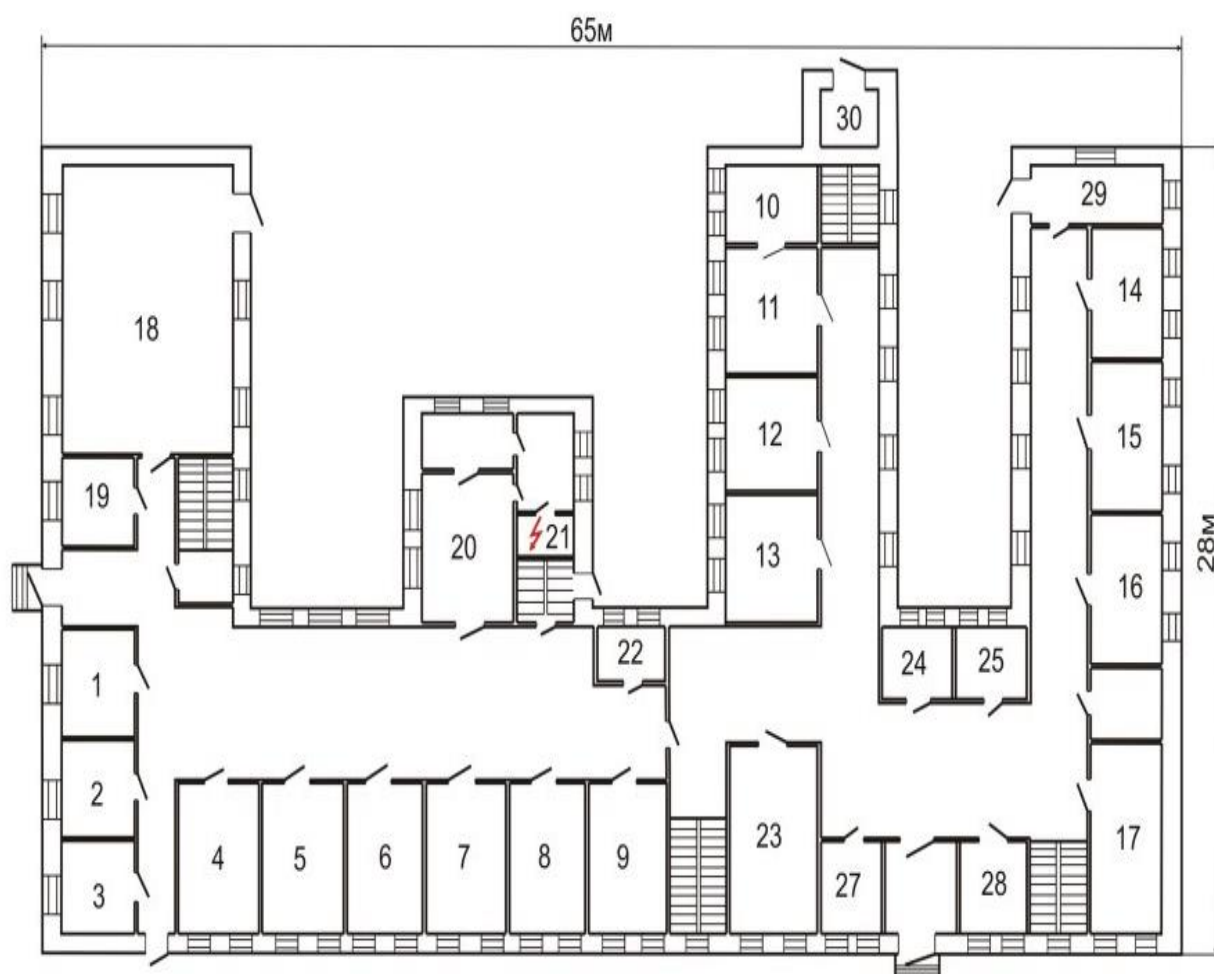


Рисунок 4.1 – План приміщення

Бездротові мережі можуть зазнавати негативного впливу з боку пристроїв Wi-Fi, неї може впливати обладнання (маршрутизатори, точки доступу). Це спричиняє падіння рівня мережі, а в деяких випадках і повне згасання сигналу Wi-Fi. Тому спочатку проведемо радіообстеження об'єкта. Для цього необхідно завантажити план приміщення, вказати радіус зони покриття для кожної точки доступу та розмістити їх відповідно до плану розташування. Важливо внести зміни у план приміщення, відповідно до матеріалів, з яких виготовлена будівля, та її розмірів, таких як стіни, перегородки, вікна, двері тощо. Обираємо тип середовища для вимірювання параметрів. У вікні "Майстер проєкту" у списку "Обрати тип середовища" вибираємо приміщення із середнім загасанням сигналу, як показано на рисунку 4.2.

Project Wizard

Environment and Measurement Units

Select environment type

Indoor with high attenuation (enclosed office, apartment) ▾

Recommended guess range: 3 m

Guess range: 3 m

☐ Extrapolate data beyond the guess range

Measurement units: ▾

Help **Back** **Next** **Cancel**

Select an environment that best describes the site to be surveyed. For each environment, the application recommends a guess range, which is the diameter of the circle inside which the application predicts the WLAN characteristics with a high degree of certainty. The application also can compute WLAN characteristics outside the guess range, although such computations have a lower degree of accuracy. Check the "Extrapolate data beyond the guess range" box to enable such

Рисунок 4.2 – Тип середовища

Далі завантажуюємо план будівлі і проводимо калібрування об'єкта. Процес калібрування показано на рисунку 4.3.

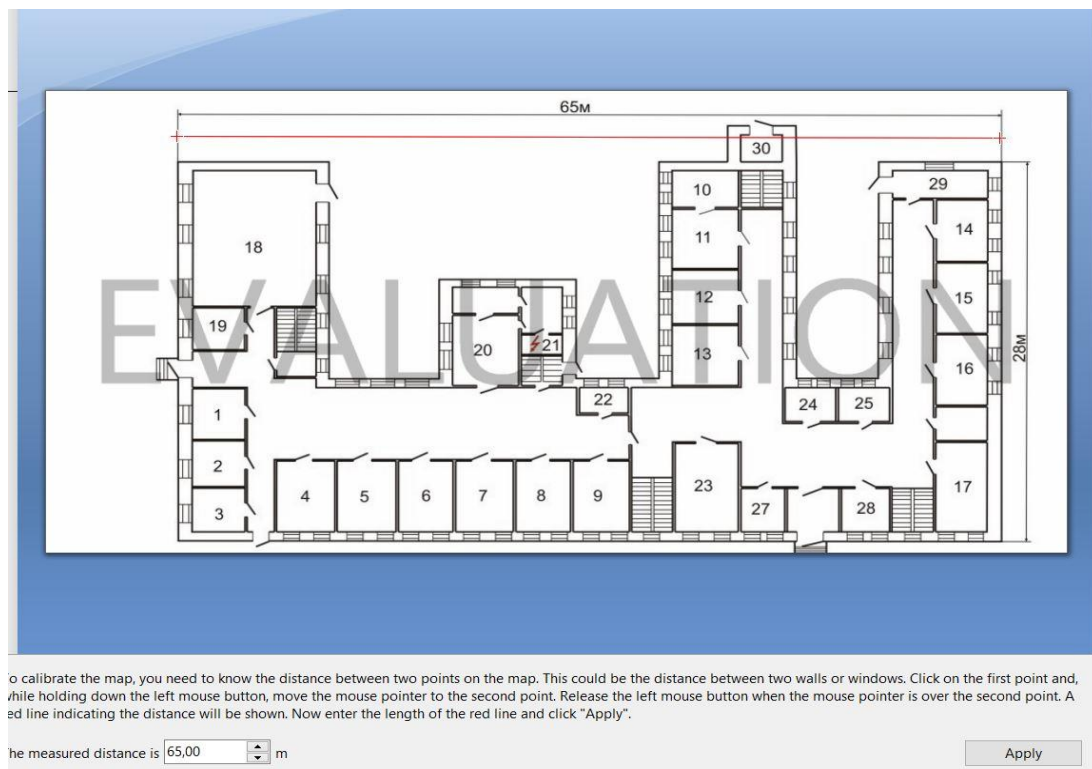


Рисунок 4.3 – Калібрування карти

Процес калібрування необхідний для налаштування масштабу карти в програмі. У режимі калібрування потрібно визначити відстань між будь-якими двома точками на карті, щоб програма могла правильно відобразити розташування об'єктів на карті. Задаємо довжину 65 м, яка вказана на схемі. Щоб додати стіни, двері, перекриття до плану поверху, скористаємося випадаючим меню для вибору перешкод. Виберемо попередньо встановлений тип, наприклад, цегляну стіну або капітальну стіну. Програмне забезпечення для обстеження об'єктів Tamograph пропонує безліч варіантів матеріалів і товщин для кожного зі своїми рівнями поглинання на стінах, вікнах і дверях. Можна вказати власне значення зниження рівня сигналу. Його можна знайти, вимірявши силу сигналу по обидва боки перешкоди та обчисливши різницю. Вимірювання можна проводити за допомогою TamoGraph або аналізатором Wi-Fi, наприклад CommView for WiFi. Для спрощення моделювання застосуємо чотири типи перешкод: зовнішні стіни, внутрішні стіни, двері, сходові клітки. Товщина внутрішньої цегляної стіни становить 9 см (позначена червоним кольором), для стандартного фасаду використана цегляна стіна товщиною 25 см (позначена світло-зеленим кольором), а міжкімнатні двері є стандартними пустотілими (позначено зеленим кольором). Остаточний результат розташування перешкод відображено на рисунку 4.4.

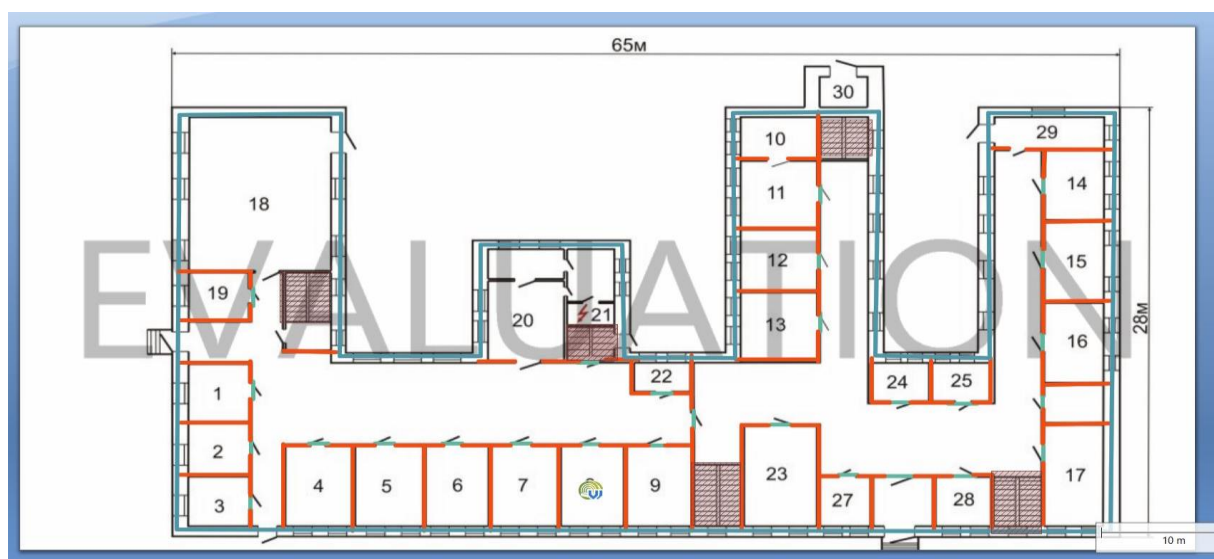


Рисунок 4.4 – План перешкод

4.1.2 Налаштування апаратного комплексу

Для налаштування маршрутизатора TP-Link Archer AX1500 можливо використовувати застосунок TP-Link Tether. Цей застосунок забезпечує найпростіший спосіб доступу та керування мережею за допомогою пристроїв з операційними системами iOS або Android. Tether - це мобільний додаток, що дозволяє переглядати стан пристрою, статус підключення користувачів, привілеї доступу, а також встановлювати батьківський контроль. Перевага застосунку це можливість доступу до основних налаштувань та звітів маршрутизатора з будь якої точки світу де є інтернет. Для забезпечення більш розширених налаштувань пристрою використовуємо підключення через дротову мережу за допомогою операційної системи Windows 10.

Під'єднаємо ноутбук Lenovo ThinkBook 15 до будь-якого вільного LAN-порту на маршрутизаторі TP-Link Archer AX1500.. Зовнішній вид веб-інтерфейсу та схема підключення до мережі відображені на рисунку 4.5.

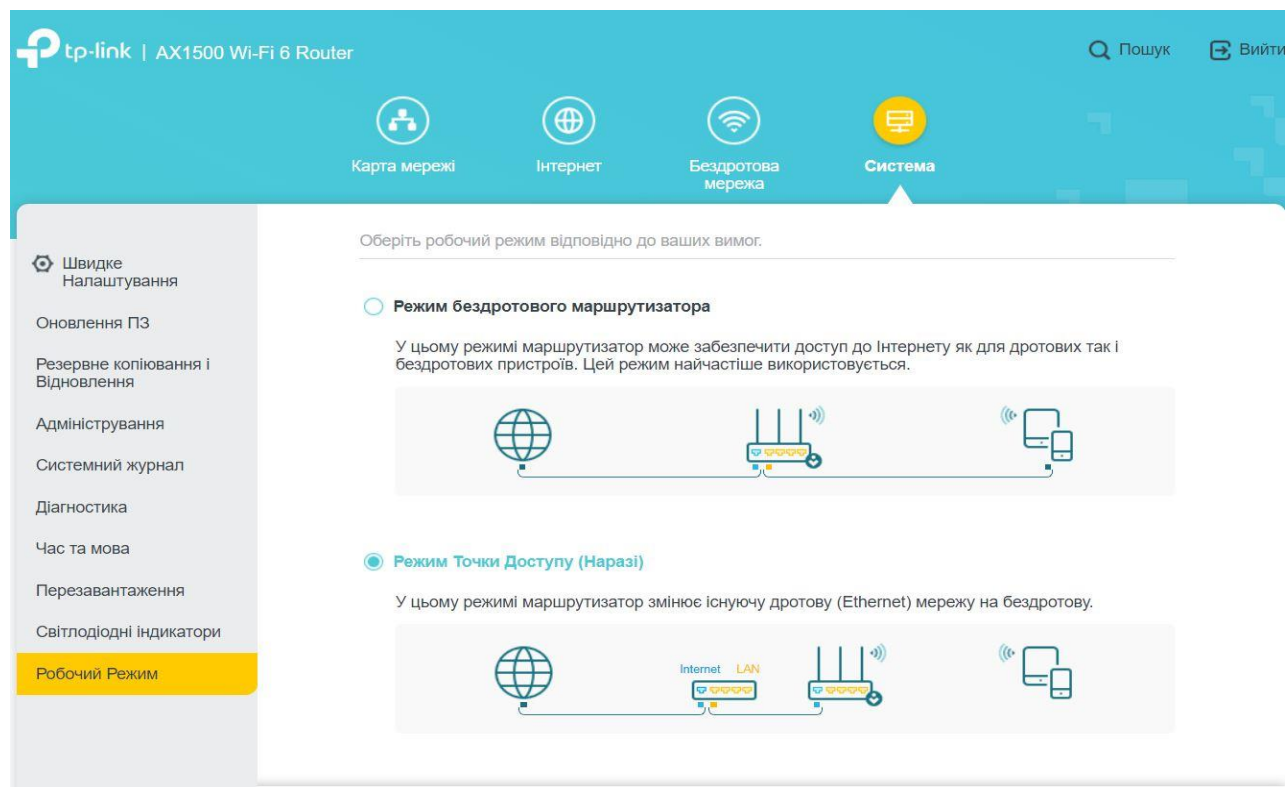


Рисунок 4.5 – Встановлення режиму точки доступу

За допомогою веб-інтерфейсу встановимо нові паролі для адміністратора та переведемо маршрутизатор в режим точки доступу. Переходимо до налаштування бездротової мережі. При налаштуванні є можливість вмикати режими роботи в діапазонах 2,4 ГГц та 5 ГГц, вибирати ширину каналу, протокол безпеки та підтримку OFDMA та TWT(Target Wake Time).

Вказуємо параметри Wi-Fi точки доступу. Для мережі 2,4 ГГц встановимо ім'я бездротової мережі (SSID) AX1500-24. Для мережі 5 ГГц встановимо ім'я бездротової мережі (SSID) AX1500-24_5G. Протокол безпеки для обох мереж використовуємо WPA2. Параметри підключення Wi-Fi мережі відображені на рисунку 4.6.

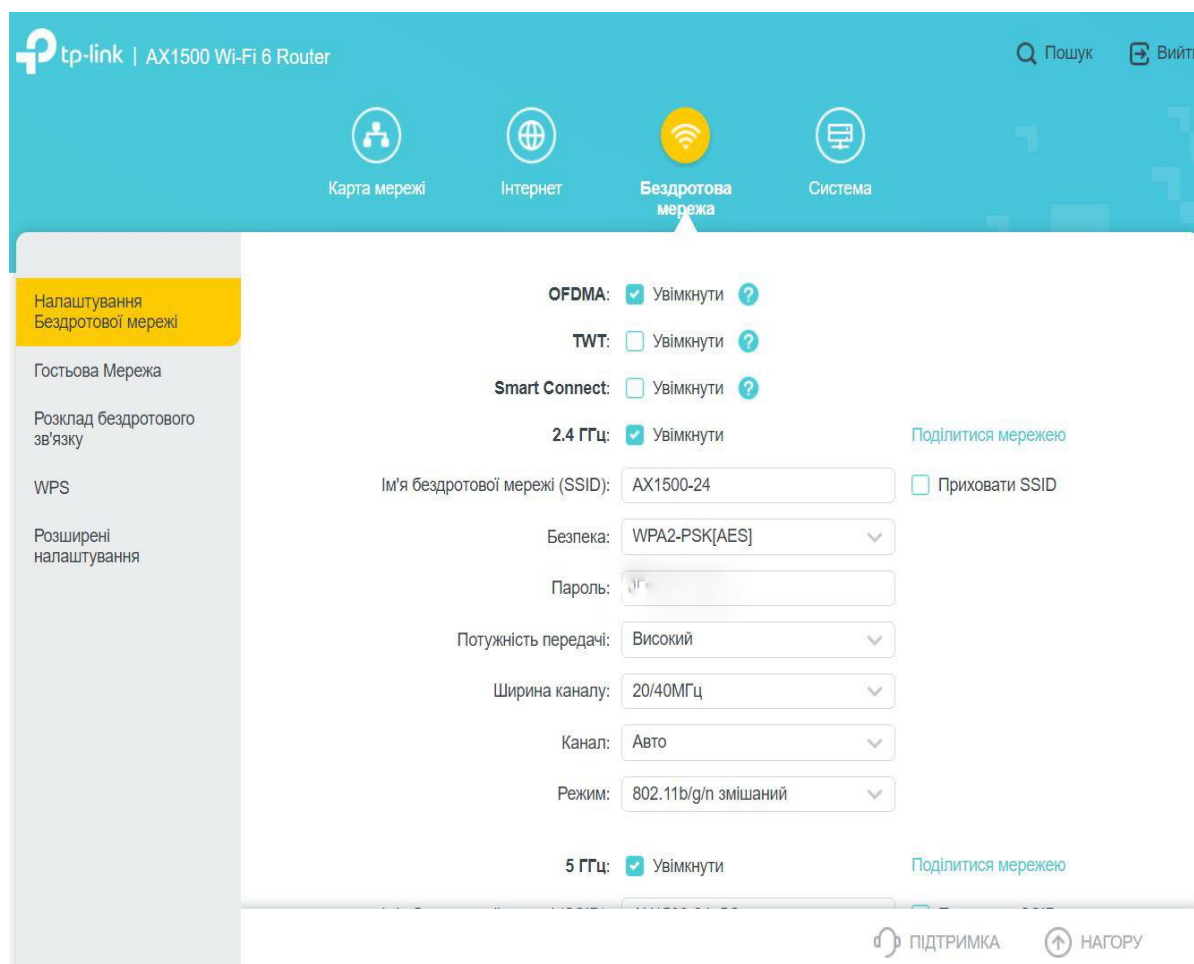


Рисунок 4.6 – Параметри підключення Wi-Fi мережі

4.2 Результати моделювання

4.2.1 Моделювання в програмному комплексі

Під час проведення дослідження аналізуються наступні параметри для кожного діапазону частот:

- рівень сигналу;
- відношення сигнал/шум;
- рівень інтерференції;
- прогнозована фізична швидкість.

Давайте розглянемо сценарій, де активовано лише одну точку доступу в діапазоні 2,4 ГГц, і порівняємо його з діапазоном 5 ГГц, щоб візуально оцінити відмінності в рівні сигналу.

На рисунках 4.7 та 4.8 видно різницю в площі покриття та рівні сигналу в двох діапазонах.

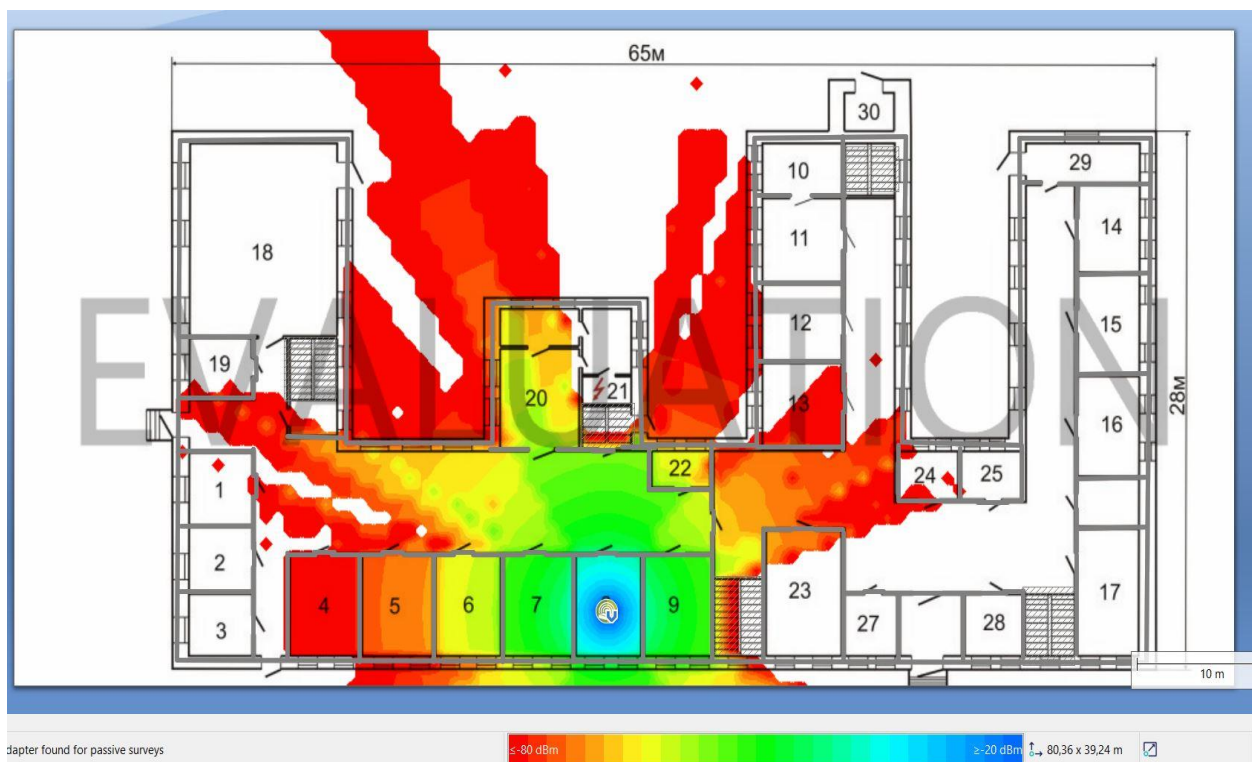


Рисунок 4.7 – Рівень сигналу однієї точки доступу в діапазоні 2,4 ГГц

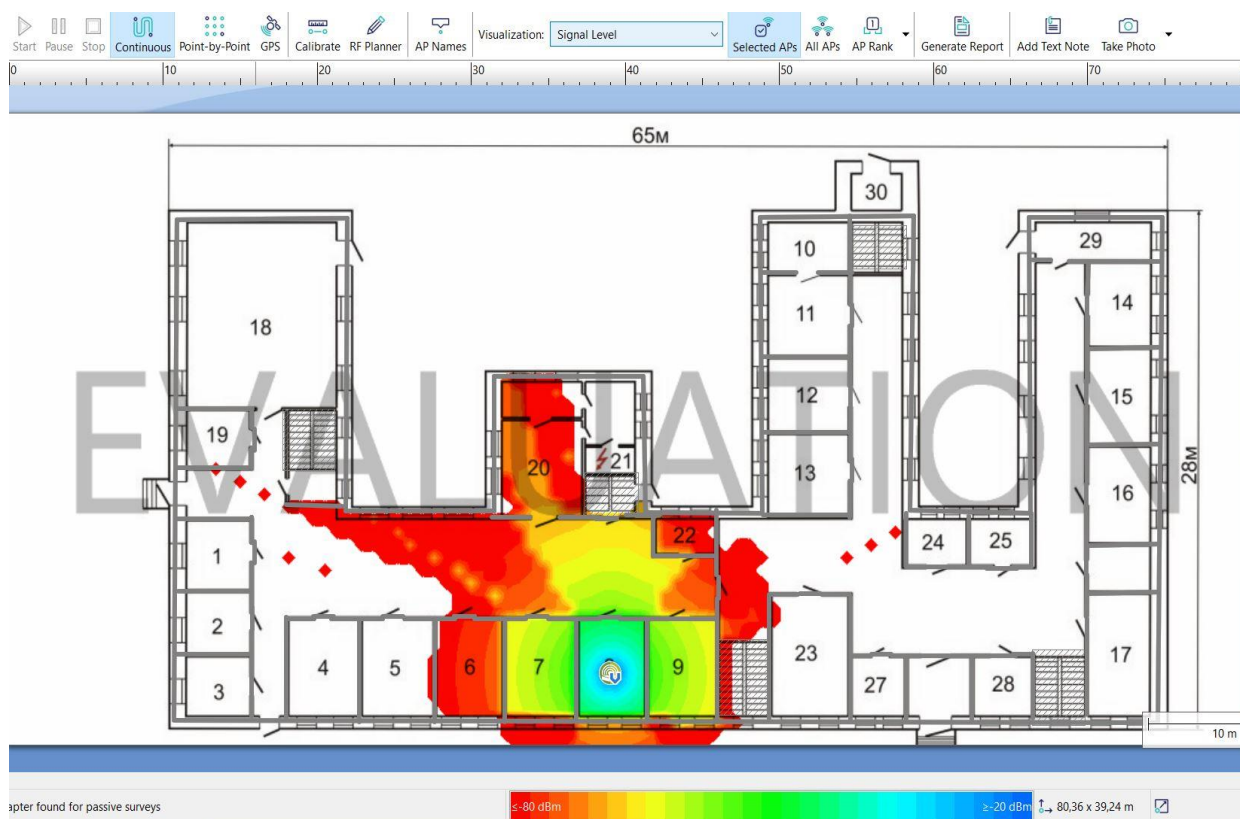


Рисунок 4.8 – Рівень сигналу однієї точки доступу в діапазоні 5 ГГц

Різними кольорами позначено рівень сигналу в децибелах (dB). Числові значення отримаємо за допомогою графічної шкали, розташованої у нижній частині зображення, або наводячи курсор на мапі в місці виміру.

За даними рисунків добре видно як швидко загасає сигнал на частоті 5 ГГц. Перевага використання частоти 2,4 ГГц часто зменшується через сильну конкуренцію від інших випромінювачів у цьому діапазоні. З іншого боку, можна легко розширити покриття мережі в діапазоні 5 ГГц, додаючи додаткові точки доступу. Рівень сигналу або карта покриття - це одна з найважливіших характеристик, що впливає на продуктивність мереж Wi-Fi.

Далі розташуємо всі точки доступу згідно нашого плану та розглянемо різницю в рівні сигналу в двох діапазонах. Згідно завдання, бездротову мережу потрібно забезпечити в приміщеннях 1-17, тому на них і зосереджена основна увага. На рисунках 4.9 та 4.10 видно значну різницю рівнів сигналу що знаходяться в діапазонах 2,4 ГГц та 5 ГГц.



Рисунок 4.9 – Рівень сигналу восьми точок доступу в діапазоні 2,4 ГГц

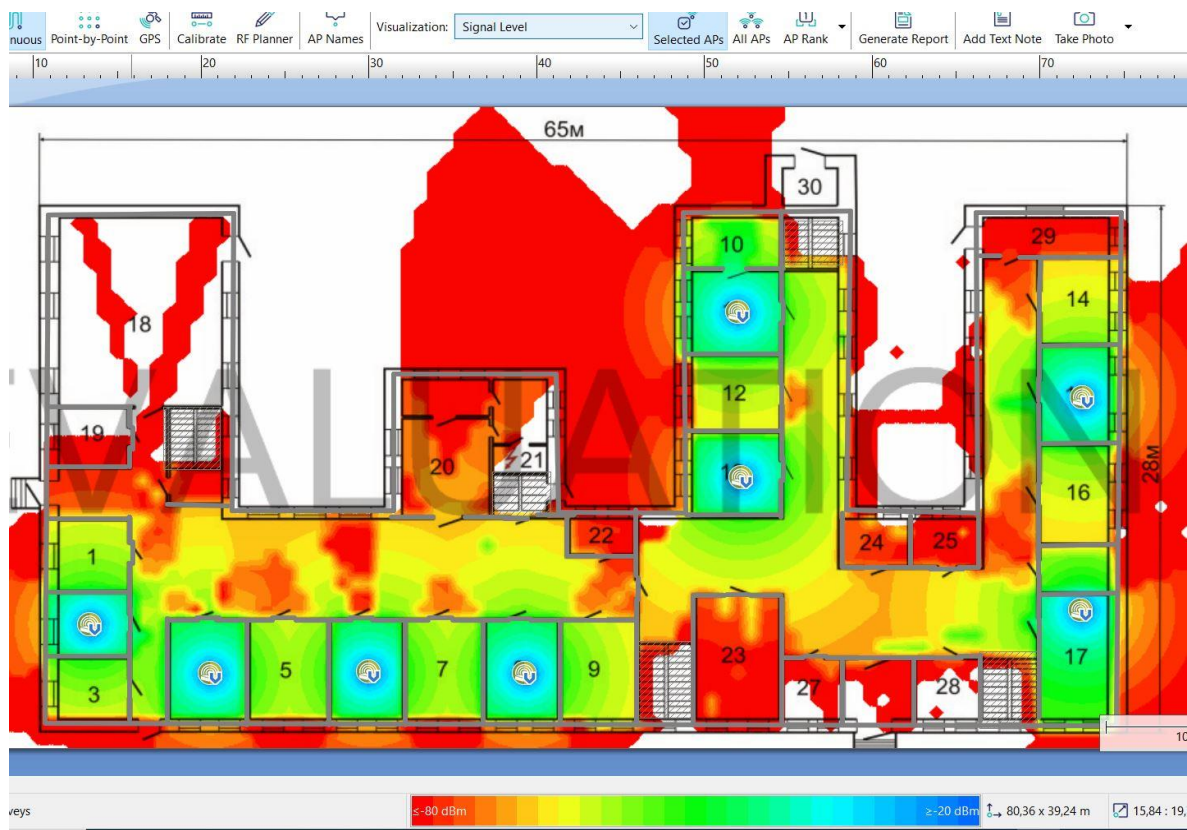


Рисунок 4.10 – Рівень сигналу восьми точок доступу в діапазоні 5 ГГц

Після прогнозування рівня сигналу, перевіримо рівень сигнал/шум (SNR). Ця характеристика теж вимірюється в децибелах і показує, наскільки рівень сигналу вищий за рівень шуму. Під шумом розуміють джерела радіовипромінювання, не включені до стандарту 802.11. Рівень сигнал/шум (SNR) є критичним показником для якості і надійності бездротового зв'язку в мережах Wi-Fi. SNR визначає відношення потужності корисного сигналу до рівня шуму в каналі передачі даних. Високий рівень SNR дозволяє використовувати більше високошвидкісних режимів передачі даних та зберігати стабільне з'єднання на великій відстані від точки доступу. У типових умовах рівень шуму становить приблизно -90 dB. На рисунках 4.11 та 4.12 показано відношення сигнал/шум для даних точок. На цих рисунках добре видно що при перетинанні декількох перешкод сигнал в діапазоні 5 ГГц втрачає потужність і практично не в змозі забезпечити з'єднання.

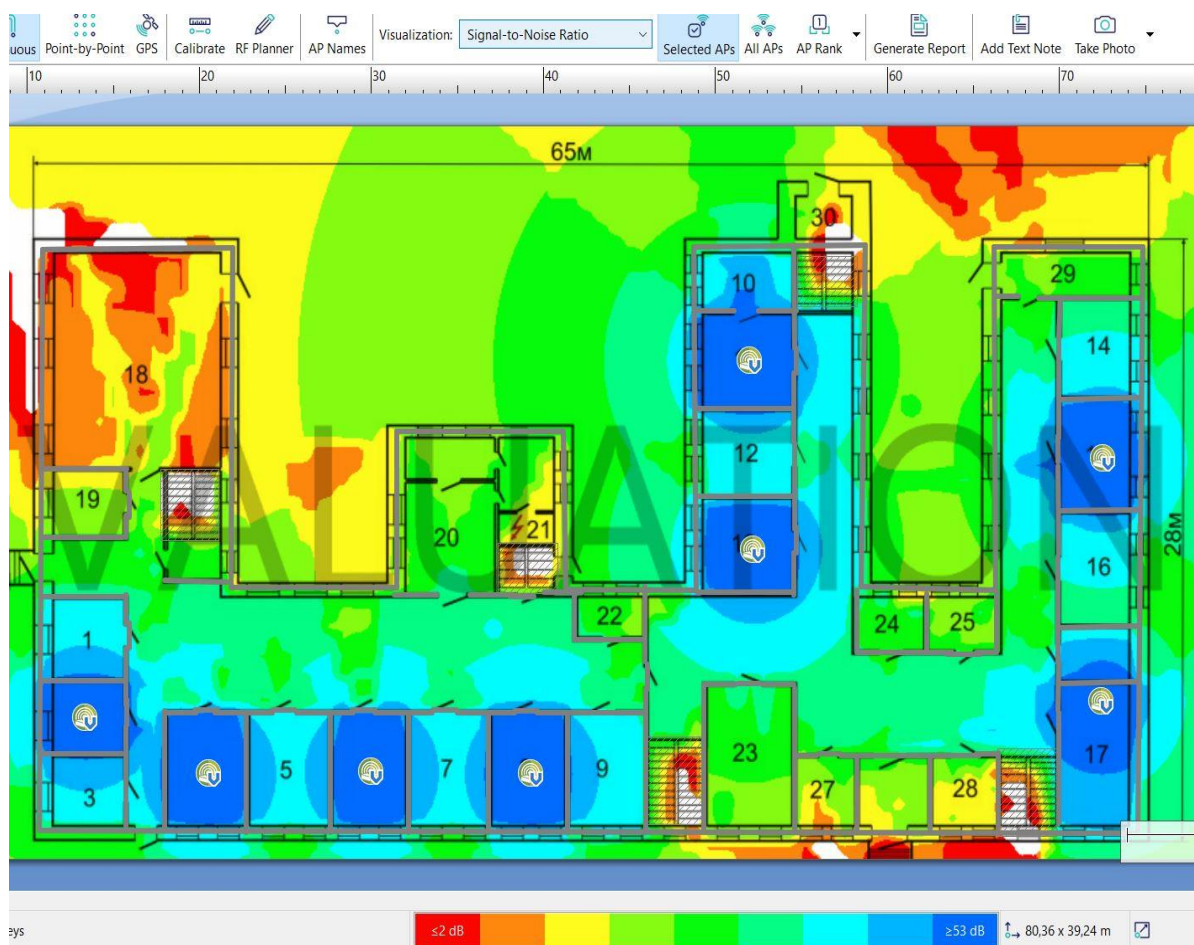


Рисунок 4.11 – Рівень сигнал/шум в діапазоні 2,4 ГГц



Рисунок 4.12 – Рівень сигнал/шум в діапазоні 5 ГГц

Важливим показником при оцінюванні продуктивності мережі є рівень інтерференції. На рисунку 4.13 зображено рівень інтерференції в діапазоні 2,4 ГГц.



Рисунок 4.13 – Рівень інтерференції діапазоні 2,4 ГГц, один канал
Зменшення пропускної здатності мережі є показником інтерференції,

оскільки конфлікти між сигналами можуть призводити до зниження швидкості передачі даних Розглянемо як зміна параметрів вплине на цей показник. Для більшої наочності приведемо рівень інтерференції в діапазоні 2,4 ГГц. В першому випадку всі точки доступу працюватимуть на першому каналі. Розподілимо точки доступу по вільним каналам. В діапазоні 2,4 ГГц використовується 13 каналів шириною 20 МГц. Виберемо для точок доступу канали 1, 5, 9, 13. Точки доступу які використовують однакові канали розташуємо якнайдалі одна від одної. Тепер мапа покриття буде виглядати так як зображено на рисунку 4.14.

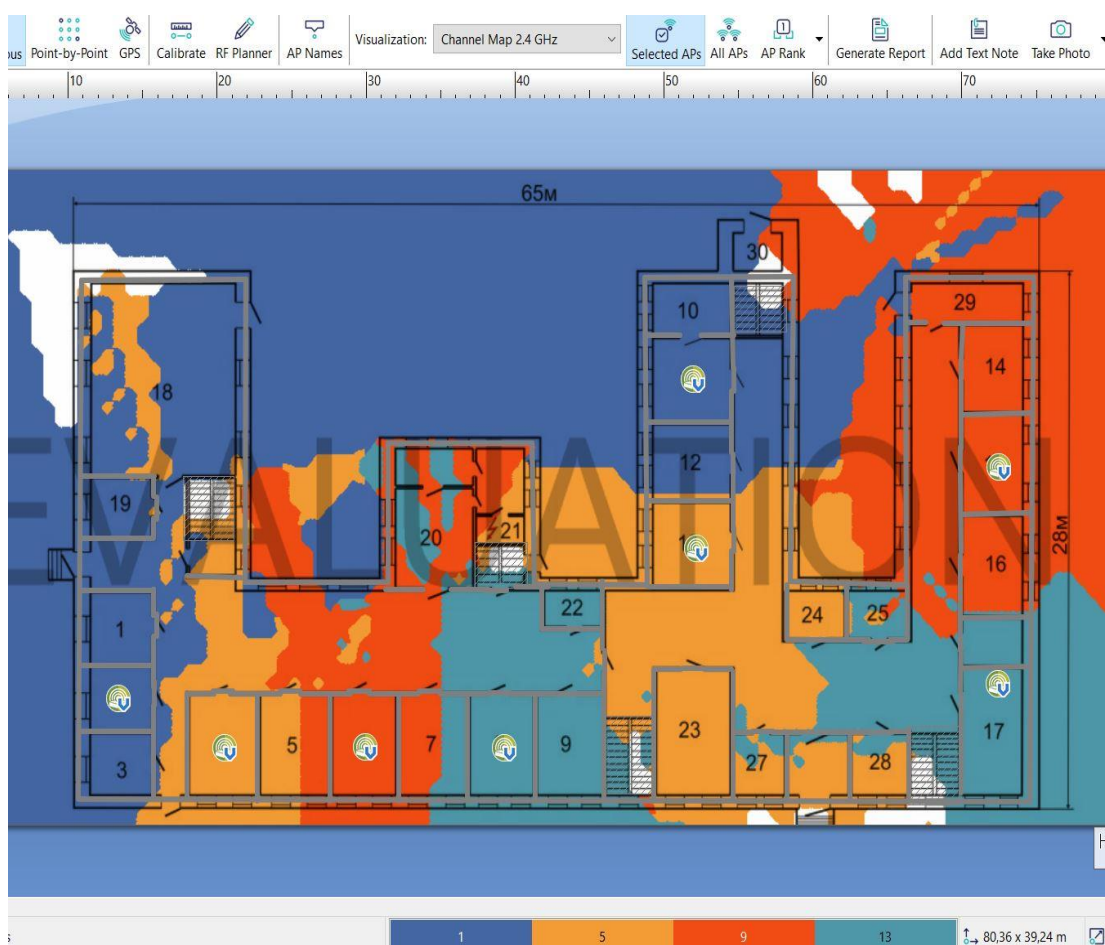


Рисунок 4.14 – Мапа покриття в діапазоні 2,4 ГГц, чотири канали

Як можна бачити з рисунка 4.15 використання каналів, що віддалені по смузі пропускання значно зменшила рівень інтерференції, що в свою чергу покращує пропускну здатність мережі.



Рисунок 4.15 – Рівень інтерференції в діапазоні 2,4 ГГц, чотири канали

На рисунках 4.16 та 4.17 відображено прогнозовану фізичну швидкість для даних точок доступу в обох діапазонах.

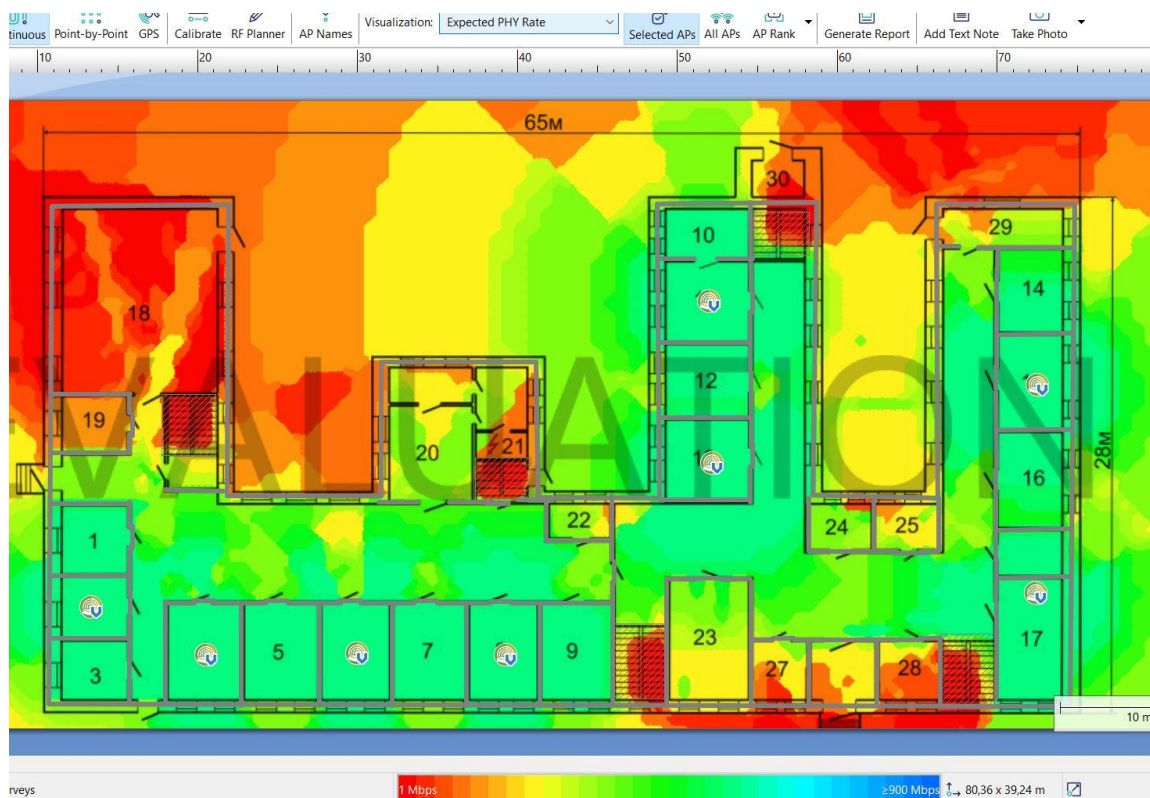


Рисунок 4.16 – Очікувана фізична швидкість в діапазоні 2,4 ГГц

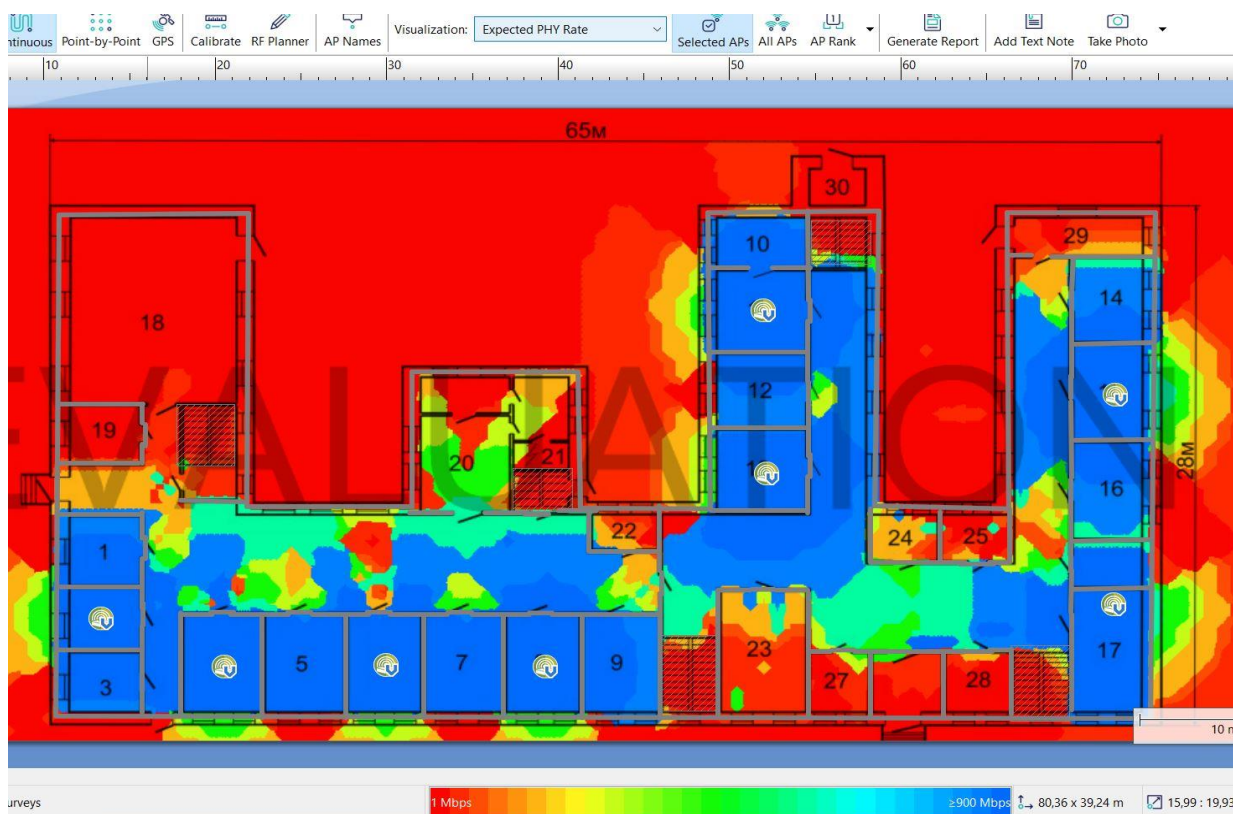


Рисунок 4.17 – Очікувана фізична швидкість в діапазоні 5 ГГц

Фізична швидкість напряму корелює із пропускнуою здатністю, яка визначає середню швидкість обміну даними клієнтом із точкою доступу на рівні застосунків (наприклад, передача файлів). Пропускна здатність завжди менша за фізичну швидкість і, як правило, не перевищує 50% через різні причини, такі як повторна передача даних і відправлення технічної інформації, яка не несе корисного навантаження (заголовки пакетів, параметри протоколів передачі даних). Знижена фізична швидкість завжди вказує на обмежену пропускну здатність, що призводить до зниженої продуктивності мережі. При використанні діапазону 5 ГГц очікувана фізична швидкість в обстежуваних приміщеннях згідно рисунка 4.17 складає в межах від 1200 Мбіт/с до 576 Мбіт/с.

4.2.2 Експериментальне дослідження

Перевіримо наскільки співпадає очікувана фізична швидкість та реальні показники бездротової мережі. Для проведення експериментального дослідження було розгорнуто тестову мережу. Для проведення вимірів пропускнуої здатності

скористуємось застосунком iPerf3 для Windows. Перший ноутбук Lenovo ThinkBook під'єднаємо за допомогою кабелю типу «звита пара» Cat5e до гігабітного порту Ethernet точки доступу. На першому ноутбуці запустимо Iperf в режимі сервера. Другий буде з'єднуватися через Wi-Fi модуль Intel AX201, на ньому Iperf запустимо в режимі клієнту. Виміри будемо проводити для однієї точки доступу та із збільшенням відстані. Максимальна кількість перешкод складатиме дві стіни. Перед початком тесту було визначено деякі необхідні фізичні параметри модельованого приміщення. Зокрема, ослаблення сигналу при проходженні стіни становить 7 дБ, а рівень шуму на частоті 5 ГГц - 91 дБм. При початковому тестуванні відстань між точкою доступу та ноутбуком з Wi-Fi модулем дорівнювала 2 метри, без додаткових перешкод.

При тестуванні у висхідному напрямку будемо застосовувати ключ "R". Для зміни кількості потоків використовується ключ "P". Подивимось як зміна параметрів розміру вікна та числа потоків вплине на продуктивність мережі. Мережа працюватиме в режимі IEEE 802.11ax зі смугою пропускання у 40 МГц. Виміри будемо проводити у низхідному і висхідному напрямках передачі.

Результат виконання програми Iperf при кількості потоків 2 наведено на рисунку 4.18.

```
C:\iperf>iperf3.exe -c 192.168.0.107 -t 5 -P 2 -w 524288000
Connecting to host 192.168.0.107, port 5201
[ 4] local 192.168.0.116 port 10434 connected to 192.168.0.107 port 5201
[ 6] local 192.168.0.116 port 10435 connected to 192.168.0.107 port 5201
```

ID	Interval	Transfer	Bandwidth	
[4]	0.00-1.00 sec	518 MBytes	4.34 Gbits/sec	
[6]	0.00-1.00 sec	518 MBytes	4.33 Gbits/sec	
[SUM]	0.00-1.00 sec	1.01 GBytes	8.68 Gbits/sec	
[4]	1.00-2.00 sec	18.6 MBytes	156 Mbits/sec	
[6]	1.00-2.00 sec	18.8 MBytes	157 Mbits/sec	
[SUM]	1.00-2.00 sec	37.4 MBytes	313 Mbits/sec	
[4]	2.00-3.00 sec	19.6 MBytes	165 Mbits/sec	
[6]	2.00-3.00 sec	19.6 MBytes	165 Mbits/sec	
[SUM]	2.00-3.00 sec	39.2 MBytes	330 Mbits/sec	
[4]	3.00-4.01 sec	18.9 MBytes	158 Mbits/sec	
[6]	3.00-4.01 sec	19.0 MBytes	159 Mbits/sec	
[SUM]	3.00-4.01 sec	37.9 MBytes	316 Mbits/sec	
[4]	4.01-5.00 sec	19.5 MBytes	164 Mbits/sec	
[6]	4.01-5.00 sec	19.9 MBytes	167 Mbits/sec	
[SUM]	4.01-5.00 sec	39.4 MBytes	331 Mbits/sec	
ID	Interval	Transfer	Bandwidth	
[4]	0.00-5.00 sec	595 MBytes	997 Mbits/sec	sender
[4]	0.00-5.00 sec	96.9 MBytes	162 Mbits/sec	receiver
[6]	0.00-5.00 sec	595 MBytes	997 Mbits/sec	sender
[6]	0.00-5.00 sec	97.0 MBytes	163 Mbits/sec	receiver
[SUM]	0.00-5.00 sec	1.16 GBytes	1.99 Gbits/sec	sender
[SUM]	0.00-5.00 sec	194 MBytes	325 Mbits/sec	receiver

Рисунок 4.18 – Продуктивність мережі зі смугою пропускання у 40 МГц

Загальні результати наведені в таблиці 4.1.

Таблиця 4.1 – Пропускна здатність зі смугою пропускання у 40 МГц

Розмір вікна	1 МБ		512 МБ	
Пропускна здатність(Мбіт/с)	DL	UL	DL	UL
1 потік	226	215	323	229
2 потоки	288	262	325	259
4 потоки	322	304	332	308

Як видно з таблиці при застосуванні смуги пропускання у 40 МГц у низхідному і висхідному напрямку передачі та збільшенні кількості потоків до 4 пропускна здатність досягає 304-322 Мбіт/с. Прогнозована швидкість знаходиться в межах 400 Мбіт/с. Для забезпечення розвинення максимальної швидкості з'єднання, розмір вікна в застосунку iPerf3 (ключ w) встановлюємо рівним 512МБ.

Протестуємо мережу в режимі IEEE 802.11ax зі смугою пропускання у 20 МГц. Результати наведені в таблиці 4.2.

Таблиця 4.2 – Пропускна здатність зі смугою пропускання у 20 МГц

Розмір вікна	512 МБ	
Пропускна здатність (Мбіт/с)	DL	UL
1 потік	236	184
2 потоки	237	214
4 потоки	237	225

Як видно з таблиці, при застосуванні смуги пропускання у 20 МГц у низхідному напрямку передачі та збільшенні кількості потоків до 4 пропускна здатність досягає 237 Мбіт/с і зостається на одному рівні. Прогнозована швидкість знаходиться в межах 287 Мбіт/с.

Проведемо тестування з максимально можливою смугою пропускання для точки доступу TP-Link Archer AX1500 в 80 МГц. Залишимо відстань на незмінною – два метри, розмір вікна -512МБ. Результати наведені в таблиці 4.3.

Таблиця 4.3 – Пропускна здатність зі смугою пропускання у 80 МГц

Пропускна здатність (Мбіт/с)	DL	UL
1 потік	813	429
2 потоки	873	567
4 потоки	883	739

Як ми бачимо з таблиці при застосуванні смуги пропускання у 80 МГц у низхідному напрямку передачі та збільшенні кількості потоків до 4 пропускна здатність досягає 883 Мбіт/с. Прогнозована швидкість знаходиться в межах 1200 Мбіт/с.

В наступному тесті вимірювання проведено в двох діапазонах – 5 ГГц та 2,4 ГГц. Смуги пропускання максимальні для цих діапазонів, 80 МГц та 40 МГц відповідно, по 4 потоки. Виміри проведемо на відстані 2 та 5 метрів без перешкод, 5 метрів та 1 стіна, 8 метрів 2 стіни. Результати тестування наведені в таблиці 4.4.

Таблиця 4.4 – Пропускна здатність при наявності перешкод

Діапазон (ГГц)	2,4		5	
Пропускна здатність (Мбіт/с)	DL	UL	DL	UL
2 метри, без перешкод	145	107	883	739
5 метрів, без перешкод	110	89	832	674
5 метрів, 1 стіна	84	38	691	569
8 метрів, 2 стіни	61	31	413	316

Аналіз проведених експериментальних вимірювань показує їх високу наближеність до модельованих результатів. Це дозволяє зробити висновок що моделювання в програмному забезпеченні TamoGragh Site Survey може значно

полегшити розгортання мереж та скоротити час на підготовку.

Основними параметрами, які впливають на продуктивність бездротових мереж стандарту IEEE 802.11 є: вибір частотного діапазону 2,4 ГГц або 5 ГГц; вибір ширини каналу; фізичні перешкоди; відстань до точки доступу та наявність інших електронних пристроїв.

ВИСНОВКИ

У ході виконання роботи всі завдання виконані. Проведено дослідження експлуатаційних параметрів мереж стандарту IEEE 802.11 при його розгортанні в сучасних умовах та вплив цих параметрів на ефективність застосування стандарту в процесі побудови бездротових сегментів. Проаналізовано сучасні методи та алгоритми оптимізації технологій передавання даних у бездротових локальних мережах та вимоги до систем доступу на базі IEEE 802.11ах. В переважній більшості випадків мережа на базі стандарту IEEE 802.11ах демонструє перевагу в пропускній здатності та найвищу швидкість. Пристрої, які не підтримують стандарт IEEE 802.11ах, не можуть інтерпретувати новий формат кадру даних і працюють у режимі сумісності, як у звичайній мережі стандартів IEEE 802.11а/b/g/n/ac.

Застосоване програмне забезпечення TamoGragh Site Survey для обстеження об'єктів найкраще підходить для моделювання мереж стандартів IEEE 802.11. Воно має всі необхідні засоби для моделювання, починаючи від можливості попереднього радіообстеження і закінчуючи оцінкою фізичної швидкості готової мережі. Діапазони 2,4 ГГц і 5 ГГц мають різні експлуатаційні завдання: точки доступу в діапазоні 2,4 ГГц мають ширше покриття і відносно нижчу швидкість передачі даних, ніж точки доступу в діапазоні 5 ГГц. З іншого боку, точки доступу в діапазоні 5 ГГц більш чутливі до подолання перешкод, що призводить до зниження рівня сигналу і зменшення швидкості.

Загалом, за умови наявності більшої кількості клієнтів мережі, яка підтримує стандарт IEEE 802.11ах, використання апаратного забезпечення із підтримкою IEEE 802.11ах для побудови або модернізації такої мережі безумовно є доцільним.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Турчин Р. І., Сучасний рух науки: тези доп. IX міжнародної науково-практичної інтернет-конференції, 2-3 грудня 2019 р. Дніпро, 2019. Том 3. С. 463.
2. Мороз Ю.А., Киричек Г.Г. Дослідження впливу зміни параметрів на продуктивність бездротових мереж 802.11. XXVI Міжнародна науково-технічна конференція «Технологія-2023», Київ, 26 травня 2023 р., Східноукраїнський національний університет ім. В. Даля, 2023. С.117.
3. Киричек Г.Г., Тягунова М.Ю., Латишев А.В. Моделювання робочих характеристик безшовної мережі на базі технології Mikrotik CAPsMAN. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки Вплив технології AIRTIME FAIRNESS на продуктивність бездротової мережі стандарту 802.11 ас. 2023. Том 34 (73) №1. С.88-94.
4. Wi-Fi CERTIFIED 6 | Wi-Fi Alliance. Wi-Fi Alliance. URL: <https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6> (дата звернення: 22.10.2023).
5. Еволюція стандартів WiFi. URL: <https://lanmarket.ua/ua/stats/evolyutsiya-standartov-wifi-802-11> (дата звернення: 22.11.2023).
6. WiFi Standards: IEEE 802.11 Electronics Notes. Reference site for electronics, radio & wireless. URL: <https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/standards.php> (дата звернення: 22.11.2023).
7. Щербаненко, Г. О., Чебанюк О. В. Огляд сучасних бездротових технологій передачі даних для «Internet of things» та аналіз проблем їх безпеки в контексті використання у системі «розумний будинок». КПІ ім. Ігоря Сікорського 2021. С.181–184.
8. Макаренко В. С. 802.11 ах-нова версія стандарту високошвидкісної системи зв'язку Wi-Fi. Телекомунікації та зв'язок. 2017. Т. 2. С. 42-51.
9. Lazebnyi V. S. Estimation of probabilistic processes in wireless networks of 802.11 standard. Мікросистеми, електроніка та акустика. 2017. №5. С. 47-53.

10. Вишняк А.В., Лазебний В.С. Експериментальне дослідження параметрів каналу передавання мережі Wi-Fi. Тези доповідей студентів та аспірантів, 2018.

11. SignalBoosters.com. What are the WiFi IEEE 802.11 Standards? SignalBoosters. URL: <https://www.signalboosters.com/blog/what-are-the-wifi-ieee-80211-standards/> (дата звернення: 15.11.2023).

12. Wi-Fi Site Survey & Planning Software for 802.11 a/b/g/n/ac/ax WLANs - TamoGraph. Wired and Wireless Network Analysis Software by TamoSoft. URL: <https://www.tamos.com/products/wifi-site-survey/> (дата звернення: 21.11.2023).

13. Wi-Fi Planner PRO. Tools Welcome. URL: <https://tools.dlink.com/intro/wfp/#access> (дата звернення: 22.11.2023).

14. Deploying Very High Density Wi-Fi. Study documents, essay examples, research papers, course notes and other - studyres.com - StudyRes. URL: <https://studyres.com/doc/17812445/deploying-very-high-density-wi-fi> (дата звернення: 22.11.2023).

15. iPerf - Download iPerf3 and original iPerf pre-compiled binaries. iPerf - The TCP, UDP and SCTP network bandwidth measurement tool. URL: <https://iperf.fr/iperf-download.php> (дата звернення: 28.11.2023).

16. IEEE Journal on Selected Areas in Communications | IEEE Xplore. IEEE Xplore. URL: <https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=49> (дата звернення: 22.11.2023).

17. Ultra-Dense Networks: A Survey. IEEE Xplore. URL: <https://ieeexplore.ieee.org/document/7476821> (дата звернення: 28.11.2023).

18. Підпалій О.І. Аналіз роботи протоколу захисту безпроводових мереж 4G. Міжнародна науково-практична конференція. Modern science: problems and innovations. Збірник матеріалів конференції. 5-7 квітня 2020 р. Стокгольм. 2020. С. 229.

19. Signal Attenuation Caused Common URL: <https://forum.huawei.com/enterprise/en/Signal-Attenuation-Caused-by-Common-Obstacles/thread/667271400337063936> (дата звернення: 25.11.2023).