

Національний університет «Полтавська політехніка імені Юрія Кондратюка»  
(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки  
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій  
(повна назва кафедри (предметної, циклової комісії))

## Пояснювальна записка

до кваліфікаційної роботи

магістр  
(ступінь вищої освіти)

на тему Розробка безпроводової мережі абонентського доступу на основі протоколу IEEE 802.11

Виконав: студент 2 курсу, групи 601ТТ  
спеціальності 172 «Електронні комунікації та радіотехніка»  
(шифр і назва напряму підготовки, спеціальності)

Сілін І.О.  
(прізвище та ініціали)

Керівник Лисечко В.П.  
(прізвище та ініціали)


Рецензент Жученко О.С.  
(прізвище та ініціали)

Полтава - 2025 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»  
Інститут Навчально-науковий інститут інформаційних технологій і  
робототехніки  
Кафедра Автоматики, електроніки та телекомунікацій  
Ступінь вищої освіти Магістр  
Спеціальність 172 «Електронні комунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри  
автоматики, електроніки та  
телекомунікацій

  
О.В. Шефер  
“ 02 ” 09 2024 р.

## З А В Д А Н Н Я

### НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Сіліну Івану Олександровичу

1. Тема проекту (роботи) «Розробка безпроводової мережі абонентського доступу на основі протоколу IEEE 802.11»

керівник проекту (роботи) Лисечко Володимир Петрович, доктор техн. наук, професор

затверджена наказом вищого навчального закладу від “09” серпня 2024 року № 818-ф.а

2. Строк подання студентом проекту (роботи) 19.12.2024 р.

3. Вихідні дані до проекту (роботи) Технічна документація на протокол IEEE 802.11. Географічне розміщення – Україна.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз сімейства протоколів IEEE 802.11. Математичне моделювання безпроводових мереж. Розробка безпроводової мережі абонентського доступу. Висновки по роботі.

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

- 1) Вступ: актуальність, мета, завдання.
- 2) Огляд стандартів безпроводових мереж IEEE 802.11.
- 3) Планування архітектури локальної мережі.
- 4) Вибір обладнання та технічні характеристики.
- 5) Моделювання радіохвиль усередині будівель.
- 6) Аналіз пропускної здатності безпроводових мереж.
- 7) Проблеми та оптимізація продуктивності.

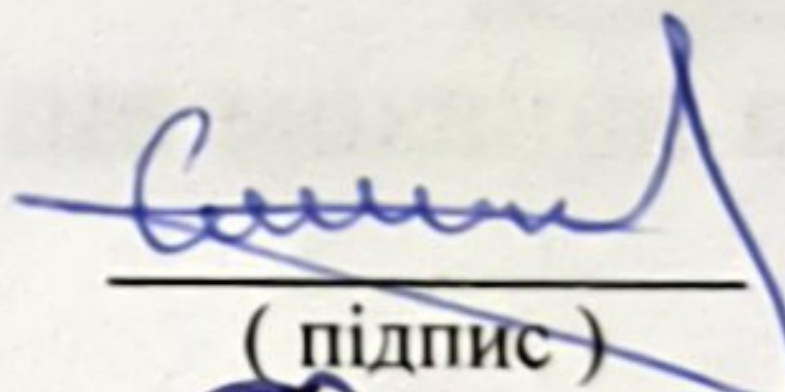
- 8) Рекомендації щодо безпеки та енергоефективності.  
9) Висновки та практичні рекомендації.

6. Дата видачі завдання 02.09.2024 р.

### КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін та обсяг виконання етапів роботи			Примітка (плакати)
		Термін	Категорія	Обсяг	
1	Отримання завдання у консультанта розділу з техніко-економічного обґрунтування	07.10.24		15%	Пл. 1
2	Підготовка матеріалів до оглядово-аналітичної частини дипломної роботи	16.10.24	I	25%	Пл. 2
3	Розробка розділу оглядово-аналітичного характеру	05.11.24		40%	Пл. 4
4	Розробка розділів спеціальної частини	12.11.24		50 %	Пл. 5
5	Розробка розділу з техніко-економічного обґрунтування	19.11.24	II	60%	Пл. 6
6	Оформлення пояснювальної записки	11.12.24		90%	Пл. 9
7	Підготовка демонстраційного матеріалу, доповіді, подання роботи на рецензію та затвердження	19.12.24	III	100%	Пл. 10

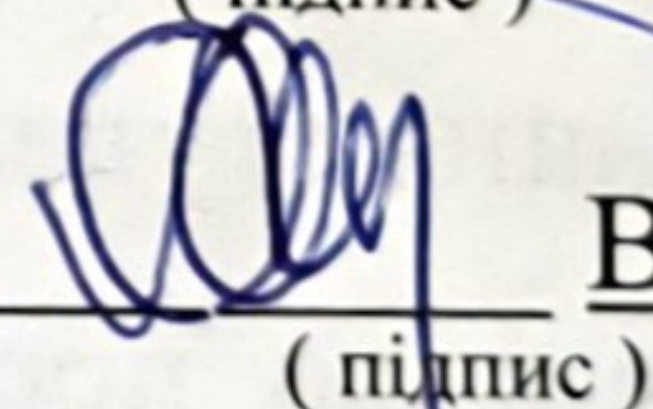
Магістрант

  
(підпис)

Іван СІЛІН

(прізвище та ініціали)

Керівник роботи

  
(підпис)

Володимир ЛИСЕЧКО

(прізвище та ініціали)

## Зміст

<b>ВСТУП</b> .....	<b>5</b>
<b>1. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ МЕРЕЖ ДОСТУПУ НА ОСНОВІ WI-FI</b> .....	<b>8</b>
1.1 Основні елементи мережі .....	8
1.2 Архітектура IEEE 802.11 .....	8
1.3 Стандарти протоколу 802.11.....	11
1.4 Фізичний рівень стандарту IEEE 802.11.b.....	19
<b>2. ПЛАНУВАННЯ ЛОКАЛЬНОЇ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ</b> .....	<b>28</b>
2.1. Чинники, які потрібно враховувати при проектуванні безпроводної мультисервісної мережі 802.11.g. ....	28
2.2. Архітектурна фаза проектування.....	28
2.3. Телекомунікаційна фаза проектування. ....	29
2.4. Вибір устаткування. ....	31
2.4.1. Ресурс точки доступу. ....	34
2.5. Переваги безпроводних мереж передачі даних.....	35
2.6. Недоліки безпроводних мереж передачі даних. ....	36
<b>3. МЕТОДИКА РОЗРАХУНКУ</b> .....	<b>38</b>
3.1 Моделі, використовувани для опису умов розповсюдження радіохвиль усередині будівель .....	38
3.2 Порівняння результатів вимірювань і розрахунків.....	52
3.3 Оцінка пропускної спроможності.....	54
3.4 Моделювання безпроводової локальної мережі в умовах високого навантаження .....	59
<b>ВИСНОВКИ</b> .....	<b>74</b>
<b>ПЕРЕЛІК ПОСИЛАНЬ</b> .....	<b>76</b>
<b>ДОДАТКИ</b> .....	<b>79</b>

## ВСТУП

### Актуальність теми магістерської роботи

Актуальність теми магістерської роботи зумовлена стрімким розвитком безпроводових технологій передачі даних, які сьогодні є важливим елементом телекомунікаційних систем. Безпроводові мережі забезпечують мобільний доступ до інформації у різних середовищах, що є ключовою умовою для функціонування сучасного суспільства, орієнтованого на цифровізацію. Одним із найперспективніших стандартів, які забезпечують такі потреби, є IEEE 802.11 (Wi-Fi), що дозволяє створювати високошвидкісні мережі абонентського доступу. Його широке застосування охоплює офісні приміщення, житлові будинки, торговельні та навчальні заклади, а також громадські простори.

В ході підготовки та виконання роботи автором була використана інформація, у тому числі текст, алгоритми, методики проведення аналізу, досліджень, визначення певних характеристик, параметрів та вихідних даних, розрахунків тощо, які містяться у джерелах [1 – 30], наведених у переліку посилань, а також інформація, отримана в результаті консультування з керівником роботи, науковими, науково-педагогічними працівниками та іншими особами, яка є неопублікованими авторськими напрацюваннями (найсучасніша інформація дослідницького, інноваційного характеру), дозволеними для використання автору цієї роботи виключно при виконанні тільки цієї дипломної роботи. Результатами роботи автора є розробка безпроводової мережі абонентського доступу на основі протоколу IEEE 802.11 на визначеній ділянці.

Аналіз сучасного стану проблеми показав, що, незважаючи на популярність та значні досягнення в розробці безпроводових мереж, існують проблеми, які потребують вирішення. Зокрема, йдеться про зниження ефективності роботи мережі в умовах підвищеного навантаження,

забезпечення стабільності зв'язку в складних архітектурних умовах, а також мінімізацію впливу зовнішніх перешкод на якість сигналу. Крім того, питання безпеки даних і захисту мережі від несанкціонованого доступу залишаються актуальними, оскільки значна кількість мереж використовує застарілі стандарти шифрування або зовсім не застосовує засобів захисту.

Досвід провідних компаній у галузі телекомунікацій, таких як Cisco, D-Link, TP-Link, а також аналіз зарубіжних та вітчизняних науково-технічних публікацій і патентного пошуку, свідчить про необхідність впровадження нових рішень для удосконалення існуючих мереж. Зокрема, акцент робиться на використанні покращених алгоритмів маршрутизації, застосуванні високопродуктивного обладнання та впровадженні технологій, які дозволяють підвищити пропускну здатність мережі.

**Метою** цієї магістерської роботи є розробка безпроводової мережі абонентського доступу на основі протоколу IEEE 802.11, що забезпечить стабільність, високу швидкість передачі даних та надійний захист інформації.

Для досягнення поставленої мети визначено такі задачі:

1. Провести аналіз існуючих стандартів безпроводових мереж і їхніх технічних характеристик.
2. Вивчити принципи проектування та побудови мереж абонентського доступу в умовах багатоповерхових житлових будинків.
3. Виконати моделювання роботи мережі в умовах високого навантаження.
4. Розробити проект оптимальної мережі, враховуючи технічні, економічні та безпекові аспекти.
5. Надати рекомендації щодо впровадження розробленої мережі у практичне використання.

У роботі використано методи моделювання, розрахунково-аналітичні підходи, а також технічний аналіз рішень, що застосовуються у сучасних безпроводових системах. Основні проєктні рішення базуються на виборі обладнання, що відповідає сучасним вимогам до пропускнуої здатності та енергетичної ефективності, а також на розробці структурної схеми мережі з урахуванням географічних, архітектурних і функціональних особливостей об'єкта проектування.

Запропоновані результати є основою для впровадження ефективних та економічно доцільних рішень, спрямованих на вдосконалення безпроводових мереж, що відповідають сучасним вимогам до надійності, безпеки та швидкості передачі даних.

## ***1. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ МЕРЕЖ ДОСТУПУ НА ОСНОВІ WI-FI.***

### ***1.1 Основні елементи мережі***

Стандарт IEEE 802.11, як і всі стандарти комітету IEEE 802, охоплює два нижні рівні моделі OSI: фізичний рівень і рівень канального зв'язку (Data Link Layer). Канальний рівень, у свою чергу, поділяється на два підрівні. Верхній підрівень, відомий як Logical Link Control (LLC), описується в стандарті IEEE 802.2. Нижній підрівень, Medium Access Control (MAC), відповідає за управління доступом до середовища передачі даних.

Фізичний рівень визначає, як пристрої працюють із середовищем передачі, а також швидкість і методи модуляції сигналів. На рівні MAC стандартизовано правила доступу до загального каналу, способи підключення пристроїв до точок доступу, механізми аутентифікації та захисту даних.

Стандарт IEEE 802.11 був створений як «безпроводовий Ethernet» і використовує пакетну передачу з 48-бітовими адресами, подібно до Ethernet-мереж. Значна увага приділялася забезпеченню сумісності всіх стандартів комітету IEEE 802, що дозволяє провідним і безпроводовим мережам цього сімейства легко взаємодіяти одна з одною.

### ***1.2 Архітектура IEEE 802.11***

Стандарт IEEE 802.11 передбачає два основні підходи до організації локальних мереж. Перший базується на принципі «рівний з рівним» (ad-hoc-мережа) і передбачає пряме з'єднання між двома станціями без необхідності централізованого адміністрування. Другий підхід реалізується у вигляді структурованих мереж, які є основним способом побудови мереж IEEE 802.11 на практиці. У таких мережах обов'язковим елементом є точка доступу (Access Point, AP), що є стаціонарним пристроєм, налаштованим на фіксований канал. Зв'язок між клієнтськими пристроями здійснюється виключно через точки

доступу, які також забезпечують вихід у зовнішні провідні мережі, такі як Ethernet.

Структуровані мережі можуть включати декілька точок доступу, з'єднаних між собою провідною мережею, створюючи набір базових станцій із перекривними зонами покриття. Стандарт підтримує функцію роумінгу, що дозволяє пристроям переміщуватися між зонами покриття різних точок доступу без втрати з'єднання, забезпечуючи тим самим мобільність користувачів. Важливою складовою є спеціальний протокол керування енергоспоживанням, який дає змогу передавальному пристрою переводити приймач у режим очікування під час бездіяльності, що є критичним для мобільних станцій із обмеженим ресурсом живлення.

Керування мережею зазвичай здійснюється в режимі розподіленого управління (Distributed Coordination Function, DCF), де функції координації розподілені між усіма пристроями мережі. Проте для структурованих мереж можливе використання режиму централізованого керування (Point Coordination Function, PCF), за якого управління передається одній із точок доступу. Такий режим застосовується для передачі даних, чутливих до затримок, наприклад, потокового відео.

Більшість мереж IEEE 802.11 використовують конкурентний доступ до каналу без пріоритетів, однак із впровадженням стандарту IEEE 802.11e очікується можливість реалізації розподіленого керування із встановленням пріоритетів для критично важливого трафіку. Важливо зазначити, що режим PCF функціонує лише в певні, заздалегідь визначені інтервали часу, які періодично повторюються.

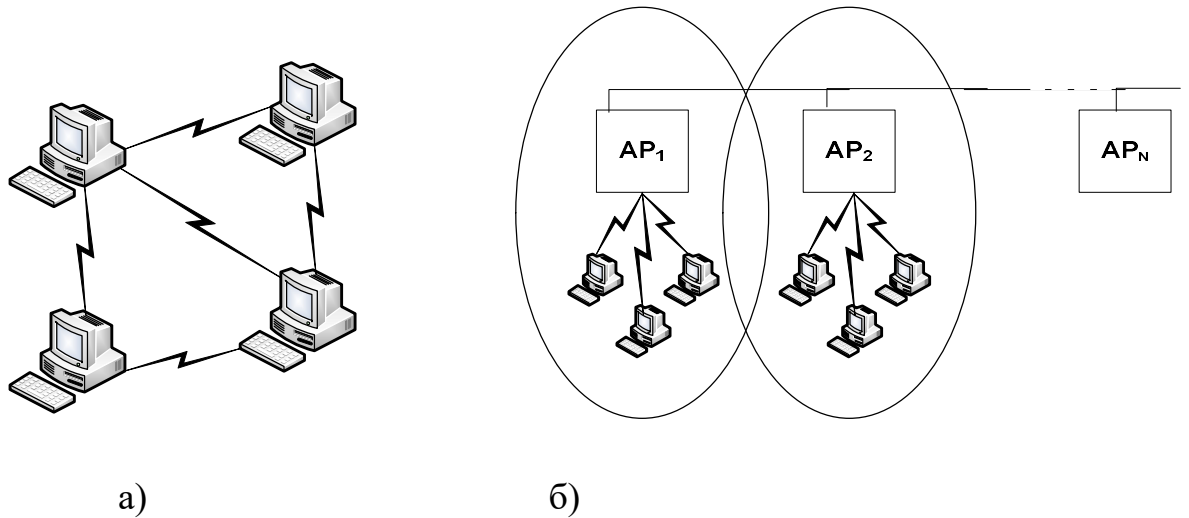


Рисунок 1.1 Архітектура мережі 802.11: а — ad-hoc-мережа, б — структуровані мережі

Однією з головних вимог до стандартів безпроводового зв'язку є забезпечення безпеки передавання даних. На рівні управління доступом до середовища (MAC-рівні) реалізовано механізм захисту, який включає процедури аутентифікації пристроїв і шифрування інформації. Цей механізм був розроблений для забезпечення рівня захисту, порівняного зі звичайними провідними мережами Ethernet, і отримав назву WEP (Wired Equivalent Privacy — «еквівалент провідної конфіденційності»).

Основою роботи WEP є використання чотирьох спільних для однієї мережі секретних ключів довжиною 40 біт. Для шифрування даних застосовується алгоритм RC4, розроблений компанією RSA Security. Цей алгоритм працює на основі перемноження блоків вихідних даних на псевдовипадкову послідовність, довжина якої відповідає розміру блоку даних для шифрування. Генерація псевдовипадкової послідовності здійснюється за допомогою 64-розрядного числа, яке включає 24-розрядний вектор ініціалізації (IV — Initialization Vector) і 40-розрядний секретний ключ.

Особливістю цього підходу є те, що вектор ініціалізації (IV) змінюється з кожним пакетом, навіть якщо секретний ключ залишається постійним. Це

знижує ризики компрометації даних. Для додаткового захисту кожен шифрований пакет супроводжується 32-розрядною контрольною сумою (ICV — Integrity Check Value), яка забезпечує виявлення змін у переданих даних. У результаті до кожного пакета додається 8 байт службової інформації: 4 байти для ICV, 3 байти для IV і 1 байт для ідентифікації використаного ключа.

Варто зазначити, що хоча стандарт допускає використання ключів більшої довжини (наприклад, 64 або 128 біт), законодавчі обмеження США на експорт пристроїв із довжиною ключа понад 40 біт змушують виробників дотримуватись цього ліміту. Таким чином, пристрої, що підтримують WEP, зазвичай обмежуються 240 варіантами ключів.

### ***1.3 Стандарти протоколу 802.11***

Стандарт IEEE 802.11.a був представлений майже одночасно зі стандартом IEEE 802.11b у вересні 1999 року. Його специфікація орієнтована на роботу в діапазоні частот 5 ГГц і базується на принципово іншому механізмі кодування даних — частотному мультиплексуванні з використанням ортогональних несучих (OFDM). У цьому стандарті кожен кадр передається за допомогою 52 ортогональних несучих, кожна з яких має ширину смуги приблизно 300 кГц (20 МГц/64). Ширина каналу в стандарті становить 20 МГц. Модуляція несучих здійснюється за допомогою методів BPSK, QPSK, а також квадратурної амплітудної модуляції з 16 та 64 рівнями (QAM). Залежно від типу модуляції і швидкості кодування (1/2, 3/4, для 64-QAM — 2/3 і 3/4) доступні швидкості передачі даних: 6, 9, 12, 18, 24, 36, 48 та 54 Мбіт/с.

Із 52 ортогональних несучих 48 використовуються для передавання інформаційних символів, а решта 4 виконують службові функції. Хоча структура заголовків фізичного рівня стандарту IEEE 802.11.a дещо відрізняється від стандарту IEEE 802.11.b, ці відмінності не є суттєвими (рисунок 1.2). Кадр складається з преамбули (12 символів синхронізації), заголовка фізичного рівня (PLCP-заголовок) та інформаційного поля,

сформованого на MAC-рівні. Заголовок містить відомості про швидкість кодування, тип модуляції та довжину кадра. Преамбула і заголовок передаються з мінімально можливою швидкістю (BPSK, швидкість кодування  $r = 1/2$ ), тоді як інформаційне поле передається із максимальною швидкістю, вказаною в заголовку, залежно від умов передачі.

OFDM-символи передаються кожні 4 мкс, із яких 3,2 мкс припадає на тривалість символу, а 0,8 мкс відводиться на захисний інтервал. Цей інтервал забезпечує стійкість до багатопроменевого поширення сигналу, оскільки відбитий сигнал, що приймається із затримкою, потрапляє у захисний інтервал і не впливає на наступний символ.

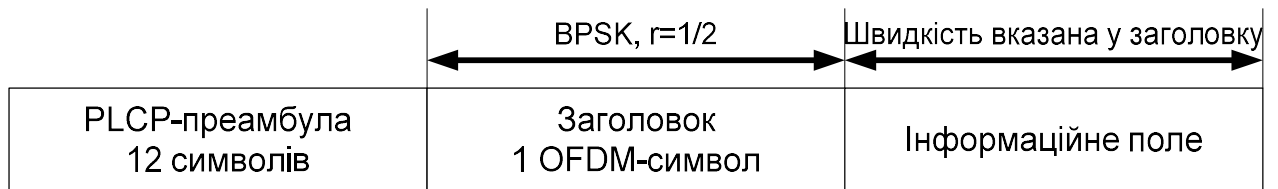


Рисунок 1.2 Структура заголовка фізичного рівня стандарту IEEE 802.11.a

Процес формування та декодування OFDM-символів реалізується із застосуванням швидкого перетворення Фур'є (прямого або зворотного, БПФ/ОБПФ). Типова схема трактів приймання і передачі (рисунок 1.3) є стандартною для цього методу і включає такі компоненти, як згортковий кодер, механізм перемежування (перерозподілу) для захисту від помилок у пакетах, а також процесор ОБПФ.

Фур'є-процесор об'єднує сигнал у єдину послідовність, додає захисний інтервал до символу, після чого формує OFDM-символ, який за допомогою квадратурного модулятора/конвертера переноситься у необхідний частотний діапазон. При прийманні сигналу всі операції виконуються у зворотному порядку.

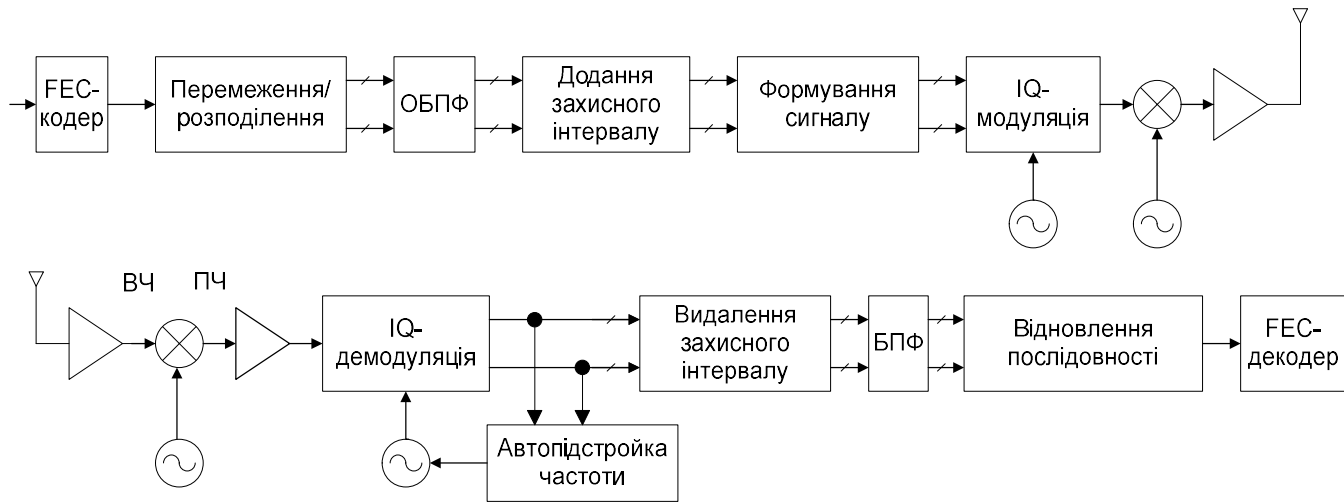


Рисунок 1.3 Функціональна схема трактів приймання/передачі стандарту IEEE 802.11a

Стандарт IEEE 802.11g, по суті, адаптує механізм модуляції OFDM, успішно використаний у стандарті 802.11a, для роботи в діапазоні 2,4 ГГц, зберігаючи при цьому сумісність із пристроями стандарту 802.11b. Така адаптація стала можливою завдяки схожості ширини каналів у діапазонах 2,4 та 5 ГГц, які становлять 22 МГц при рівнях потужності  $-30$  дБ та  $-20$  дБ відповідно. У діапазоні 5 ГГц стандарт 802.11a допускає ширину спектральної смуги до 40 МГц при рівні  $-28$  дБ.

Однією з основних вимог до специфікації 802.11g була забезпечення зворотної сумісності з пристроями 802.11b. Це викликало суперечки між компаніями Intersil та TI. У стандарті 802.11b основною технологією модуляції є ССК (Complementary Code Keying), а додатково підтримується PBSS. Розробники стандарту 802.11g вирішили залишити ССК-модуляцію для швидкостей до 11 Мбіт/с і застосувати OFDM для вищих швидкостей.

Незважаючи на це, мережі 802.11 працюють на основі принципу CSMA/CA (множинний доступ із контролем несучої та уникненням колізій). Це означає, що пристрої повинні переконатися у відсутності активного трафіку перед початком передачі.

Якщо в зоні дії знаходяться пристрої 802.11b та 802.11g, останні використовують OFDM, що може бути "незрозумілим" для пристроїв 802.11b. У таких випадках пристрої 802.11b можуть намагатися розпочати передачу, створюючи конфлікти.

Для уникнення подібних ситуацій у стандарті 802.11g передбачено режим змішаної роботи ССК-OFDM. У цьому режимі кадри передаються у двох частинах: преамбула та заголовок кодуються методом ССК, а інформаційне поле – методом OFDM. Це дозволяє пристроям 802.11b розпізнавати заголовки кадрів і утримуватися від передачі, коли передається трафік пристроїв 802.11g. Однак цей підхід знижує пропускну здатність мережі, оскільки преамбула та заголовок передаються на швидкості лише 1 Мбіт/с.

Для усунення обмежень, пов'язаних із використанням технології ССК, в стандарті 802.11g передбачено необов'язковий режим PBSS, як і в 802.11b. У цьому режимі заголовок і преамбула передаються так само, як і при ССК, а інформаційне поле модулюється PBSS зі швидкостями 22 або 33 Мбіт/с. Завдяки цьому пристрої 802.11g залишаються сумісними з усіма версіями 802.11b, зводячи до мінімуму ризику виникнення конфліктів. Підтримувані швидкості для різних типів модуляції наведено в таблиці 1.1, а залежність швидкості передачі від методу модуляції зображено на рисунку 1.4.

Таблиця 1.1 Можливі швидкості й типи модуляції в специфікації IEEE 802.11g

Швидкість, Мбіт/с	Тип модуляції	
	Обов'язково	Допустимо
1	2	3
1	Послідовність Баркера	
2	Послідовність Баркера	
5,5	ССК	PBSS
6	OFDM	ССК-OFDM

Продовження таблиці 1.1

1	2	3
9		OFDM, CCK-OFDM
11	CCK	PBCC
12	OFDM	CCK-OFDM
18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM

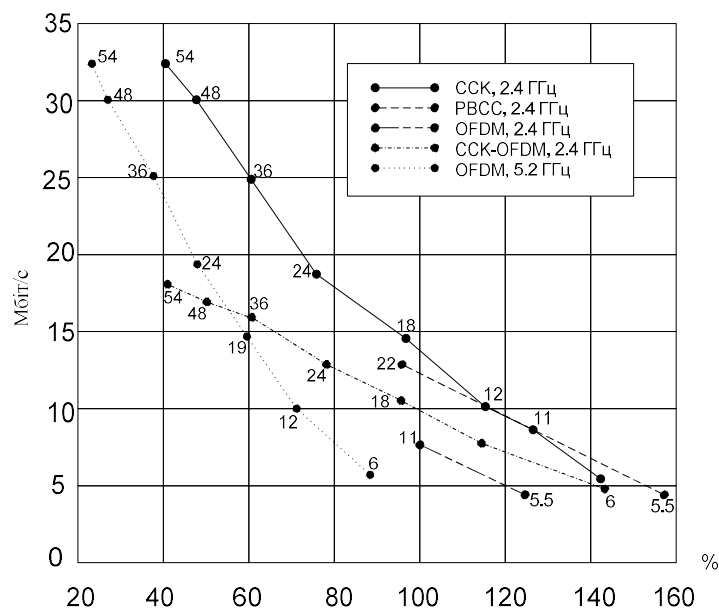


Рисунок 1.4 Залежність швидкості передачі від відстані для різноманітних технологій передачі. Відстань наведена у відсотках, 100% -дальність передачі з модуляцією CCK на швидкості 11Мбіт/с.

Очевидно, що пристрої стандарту IEEE 802.11g будуть змушені ще тривалий час працювати у спільних мережах із обладнанням, яке підтримує лише стандарт 802.11b. При цьому варто зазначити, що більшість виробників

неохоче впроваджуватимуть режими ССК-OFDM і PBSS, оскільки вони не є обов'язковими, а собівартість пристроїв часто визначає кінцеву ціну. Одним із ключових завдань нового стандарту було забезпечення безконфліктної роботи змішаних мереж 802.11b/g.

Основний принцип роботи мереж 802.11 — це концепція «слухати перед тим, як передавати». Проте пристрої стандарту 802.11b не здатні розпізнати трафік, створений обладнанням 802.11g, що працює в OFDM-режимі. Це створює ситуацію, подібну до проблеми «схованих станцій»: коли два пристрої, які не знаходяться в зоні чутності один одного, намагаються передати дані третій станції, створюючи конфлікт. Для уникнення таких ситуацій у стандарті 802.11 було впроваджено механізм захисту на основі кадрів RTS/CTS («запит на передачу» та «підтвердження передачі»). Цей механізм працює і в змішаних мережах 802.11b/g, дозволяючи пристроям уникати одночасної передачі. При цьому кадри RTS/CTS передаються за допомогою ССК-модуляції, зрозумілої для всіх пристроїв.

Однак захисний механізм значно знижує пропускну здатність мережі. Наприклад, у мережах 802.11g із фізичною швидкістю 54 Мбіт/с реальна пропускну здатність через накладні витрати становить близько 32 Мбіт/с, а для пристроїв звичайного обладнання — близько 24 Мбіт/с. У змішаних мережах із використанням RTS/CTS цей показник падає до 12 Мбіт/с, що майже вдвічі більше, ніж пропускну здатність мереж 802.11b (~6 Мбіт/с), але все ще нижче очікуваного. Як альтернативу можна використовувати тільки кадри CTS, які передаються перед кожним OFDM-кадром, що дозволяє підвищити пропускну здатність до 14,5 Мбіт/с. Втім, цей підхід має обмеження, якщо не всі пристрої мережі перебувають у зоні прямої чутності.

Щоб вирішити цю проблему, виробники почали впроваджувати власні технології для підвищення швидкості в рамках існуючих стандартів. Наприклад, компанія Atheros розробила режим Turbo Mode, який дозволяє

подвоїти швидкість передачі до 108 Мбіт/с, використовуючи два канали одночасно. Для цього компанія створила чипсет AR5001X+, оснащений модернізованим процесором AR5212.

Корпорація Intersil обрала інший підхід, запропонувавши технологію PRISM Nitro. Ця технологія включає два основні елементи: механізм захисту та метод групової передачі OFDM-кадрів. Захисний механізм, аналогічний RTS/CTS, передбачає передавання кадру CTS перед кожним OFDM-кадром. Водночас групова передача дозволяє значно збільшити пропускну здатність як у змішаних, так і в однорідних мережах. Наприклад, у змішаних мережах кожному пристрою пропонується рівний часовий інтервал для передачі. Для кадру ССК, що передається на швидкості 11 Мбіт/с, витрачається приблизно стільки ж часу, скільки для шести OFDM-кадрів на швидкості 54 Мбіт/с, включаючи всі накладні витрати. Таким чином, пристрої 802.11b і 802.11g можуть ефективно розподіляти час передачі, мінімізуючи втрати пропускну здатності. Наприклад, для двох пристроїв із розміром інформаційного поля 1500 байт передача може зайняти 2143 мкс (рисунок 1.5).

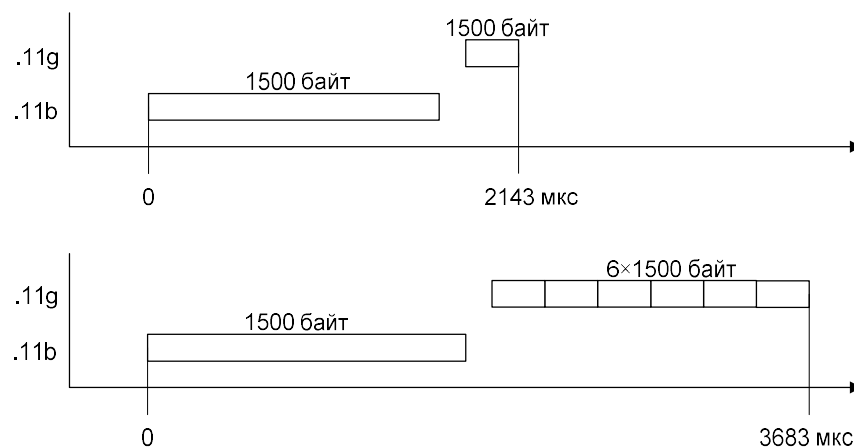


Рисунок 1.5 Групова передача OFDM-Пакетів за технологією PRISM Nitro у змішаній мережі.

У разі використання однорідної мережі стандарту 802.11g групова передача пакетів також забезпечує значний приріст ефективності. Це

досягається завдяки тому, що всередині групи пакетів немає потреби у передачі кадрів CTS або очікуванні міжкадрових інтервалів між окремими передачами. Усі накладні витрати скорочуються до передачі лише короткого кадру підтвердження приймання (ACK), що значно знижує час простою мережі (рисунок 1.6).

Цей підхід дозволяє значно підвищити пропускну здатність мережі, особливо за умов високого навантаження, забезпечуючи більшу ефективність використання каналу передачі даних. Таким чином, групова передача пакетів стає важливим елементом оптимізації продуктивності мереж 802.11g, як для змішаних, так і для однорідних середовищ.

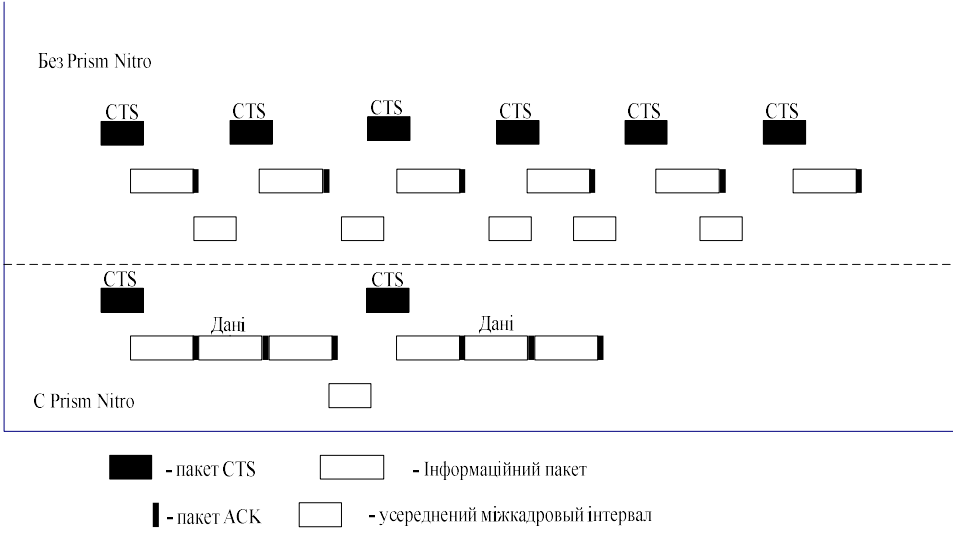


Рисунок 1.6 Групова передача OFDM-Пакетів за технологією PRISM Nitro в однорідній мережі.

Технологія PRISM Nitro була реалізована на рівні системного програмного забезпечення і створена для інтеграції з чипсетами PRISM Duette та PRISM GT. Її розробники стверджують, що ця технологія повністю відповідає вимогам стандарту IEEE 802.11g, забезпечуючи високу ефективність і продуктивність у безпроводових мережах. PRISM Nitro вже

знайшла застосування в низці сучасних пристроїв, зокрема в маршрутизаторі CONNECT2AIR, а також у мережевих картах компанії Fujitsu Siemens Computers.

Примітно, що Fujitsu Siemens Computers першою впровадила новітній процесор ISL3893, розроблений фірмою Intersil, для точок доступу та маршрутизаторів безпроводових мереж. Цей процесор побудований на основі мікропроцесорного ядра ARM9, що дозволяє йому виконувати функції як мережного процесора для безпроводової мережі, так і процесора для мереж Ethernet. Така багатофункціональність забезпечує ефективну інтеграцію провідних і безпроводових компонентів мережі.

Процесор ISL3893 спеціально оптимізований для роботи з чипсетами PRISM GT і PRISM Duette, що робить його ідеальним рішенням для створення високопродуктивних безпроводових мереж. Його архітектура дозволяє забезпечити високу швидкість обробки даних, стабільність з'єднань і підтримку сучасних вимог до телекомунікаційного обладнання.

#### ***1.4 Фізичний рівень стандарту IEEE 802.11.b***

На фізичному рівні до MAC-кадрів (MPDU) додається заголовок фізичного рівня, який складається з преамбули та PLCP-заголовка (див. рисунок 1.7). Преамбула включає стартову синхропослідовність (SYNC), яка використовується для налаштування приймача, а також 16-бітний код початку кадра (SFD), що має значення F3A016. PLCP-заголовок містить кілька ключових полів: SIGNAL (містить інформацію про швидкість передачі та тип модуляції), SERVICE (містить додаткові дані, зокрема про застосування високошвидкісних розширень або PBSS-модуляції) і LENGTH (визначає час у мікросекундах, необхідний для передачі решти кадра після заголовка). Усі ці три поля PLCP-заголовка захищені 16-бітною контрольною сумою CRC, що гарантує цілісність переданих даних.

Стандарт IEEE 802.11b передбачає два види заголовків фізичного рівня: довгий і короткий (рисунок 1.8). Основні відмінності між ними полягають у довжині синхропослідовності (128 біт для довгого та 56 біт для короткого), методах генерації цих послідовностей, а також у порядку передавання символу початку кадра. У короткому заголовку символ початку кадра передається у зворотному порядку.

Ще однією важливою різницею є швидкість передачі даних у заголовках. Для довгого заголовка всі поля передаються зі швидкістю 1 Мбіт/с. У випадку короткого заголовка преамбула також передається на швидкості 1 Мбіт/с, але решта полів заголовка передається зі швидкістю 2 Мбіт/с. Основна частина кадра може передаватися на будь-якій із швидкостей, дозволених стандартом, які визначаються у полях SIGNAL та SERVICE.

Введення коротких заголовків у стандарті IEEE 802.11b було спрямоване на підвищення пропускної здатності мережі. Це дозволяє знизити накладні витрати на обробку кадрів і, відповідно, підвищити ефективність використання доступного радіоканалу, особливо в умовах високого навантаження.

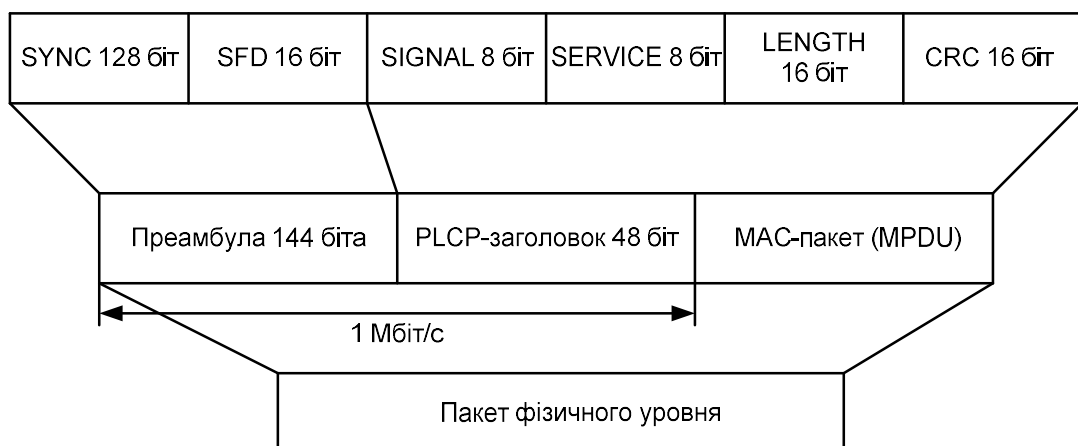


Рисунок 1.7 Структура кадрів мережі 802.11 MAC – рівня

З опису процедур зв'язки мережі IEEE 802.11 видно, що «накладні витрати» у цьому стандарті вище, ніж у провідній мережі Ethernet. Тому надто важливо забезпечити високу швидкість передачі даних у каналі. Підвищити

пропускну здатність каналу із заданою шириною смуги частот можна, розробляючи й застосовуючи більш досконалі методи модуляції. Цим шляхом пішла група розроблювачів IEEE 802.11.b. Нагадаємо, що споконвічно стандарт IEEE 802.11 передбачав роботу в режимі DSSS з використанням так званої Баркеровської послідовності (Barker) довжиною 11 біт:  $B_i = (10110111000)$ . Кожний інформаційний біт заміщається своїм добутком по модулю 2 (операція «, що виключає АБО») з даною послідовністю, тобто кожна інформаційна одиниця замінюється на  $B_i$ , кожний нуль — на інверсію  $B_i$ . У результаті біт замінюється послідовністю 11 чіпів. Далі сигнал кодується за допомогою диференціальної двох- або чотирьохпозиційної фазової модуляції (DBPSK або DQPSK, один або два чіпи на символ відповідно). При частоті модуляції несучої 11 МГц загальна швидкість становить залежно від типу модуляції 1 і 2 Мбіт/с.



Рисунок 1.8 Короткий заголовок кадрів мережі 802.11.b

Стандарт IEEE 802.11b додатково забезпечує можливість передачі даних на швидкостях 11 та 5,5 Мбіт/с. Для досягнення цих швидкостей використовується метод модуляції, відомий як ССК-модуляція (Complementary Code Keying, кодування комплементарним кодом). Цей підхід базується на наукових розробках фахівців компаній Intersil (раніше — Harris Semiconductor) та Agere Systems, які входили до складу Lucent Technologies. У цьому методі для передачі даних застосовується DQPSK-модуляція в радіотракті, а сама ССК-модуляція виконується шляхом розбиття вхідного потоку даних на групи по 8 біт (d0-d7).

Ці вісім біт формують інформаційний символ із восьми комплексних чіпів  $Z = [z_0, \dots, z_7]$ , кожен із яких визначає I- та Q-квадратурні складові

сигналу для DQPSK. Модуляція здійснюється з використанням несучої частоти 11 МГц. Кожен чип у складі символу є сигналом несучої частоти з фазовим зсувом, обчисленим для всього символу відповідно до формули:

$$Z[c_0, \dots, c_7] = [j_1 + j_2 + j_3 + j_4; j_1 + j_3 + j_4; j_1 + j_2 + j_4; -(j_1 + j_4); j_1 + j_2 + j_3; j_1 + j_3; -(j_1 + j_2); j_1]$$

Значення елемента  $j_1$  присутнє у кожному чипі символу, впливаючи на фазу всього символу. Фазова модуляція є диференціальною, оскільки значення  $j_1$  поточного символу обчислюється на основі значення  $j_1$  попереднього символу. Фазовий зсув  $j_1$  визначається формулою  $\Delta j_1 = (d_0 d_1)\pi/2$  для парних символів, де  $(d_0 d_1)$  — двобітєве двійкове число в діапазоні від 0 до 3. Для непарних символів до  $j_1$  додається додатковий зсув на  $\pi$ .

У стандарті IEEE 802.11b ССК-модуляція застосовується лише до MAC-кадрів. Перший ССК-символ, який з'являється після заголовка фізичного рівня, має номер «0», тобто вважається парним. Фаза останнього символу заголовка кадра, модульованого за допомогою QPSK, використовується як опорна для визначення початкового значення  $j_1$  першого символу інформаційного поля, до якого додається фазовий зсув  $\Delta j_1$ . Інші три параметри символу визначаються за формулами:

$$j_2 = (d_2 d_3)\pi/2; j_3 = (d_4 d_5)\pi/2; j_4 = (d_6 d_7)\pi/2, \quad (1.1)$$

де  $(d_x d_{x+1})$  — двобітєві двійкові числа.

Для передачі на швидкості 5,5 Мбіт/с застосовується DBPSK-модуляція. У цьому випадку ССК-символ кодується чотирма бітами даних  $(d_0-d_3)$ , що й зумовлює зниження швидкості вдвічі порівняно зі швидкістю 11 Мбіт/с. При цьому  $j_1$  обчислюється за тією ж формулою, тоді як інші параметри визначаються так:  $j_2 = d_2\pi/2$ ;  $j_3 = 0$ ;  $j_4 = d_3\pi$ .

Головною перевагою ССК-модуляції є її ефективність. Як показує формула, чипи символу визначаються на основі послідовностей Уолша-Адамара, що забезпечують гарні кореляційні властивості. Для швидкості 11 Мбіт/с вхідний вектор даних  $D = [d_0, \dots, d_7]$  можна представити як послідовність четверичних чисел  $m_1 \dots m_4$ , де  $m_1 = (d_0d_1)$ ,  $m_2 = (d_2d_3)$ , ...,  $m_4 = (d_6d_7)$ . Тоді вектор  $Z$  обчислюється як:

$$Z = (M \times (WH + V))\pi/2, \quad (1.2)$$

де  $WH$  — верхня половина матриці Уолша-Адамара, а  $V$  — вектор, що забезпечує корекцію фазових зсувів.

$$\{WH\} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Вектор  $V = [0, 0, 0, 2, 0, 0, 2, 0]$ , що фізично відповідає фазовому зсуву чипів  $c_3$  та  $c_6$  на  $180^\circ$  (зміна знаку на «мінус» у формулі (1.1)), відіграє важливу роль у покращенні кореляційних властивостей кодових послідовностей. Послідовності Уолша-Адамара, на основі яких працює цей підхід, добре досліджені та мають відмінні автокореляційні характеристики. Їх важливою особливістю є низький рівень самокореляції навіть за умови фазового зсуву, що робить їх ефективними для боротьби з перевідбитими сигналами в радіотрактах.

Теоретичне операційне посилення ССК-модуляції становить 3 дБ (що відповідає подвоєнню потужності сигналу). Це пояснюється тим, що без застосування кодування QPSK-модульований сигнал на частоті 11 МГц здатен

передавати дані зі швидкістю 22 Мбіт/с. Завдяки своїй простоті ССК-модуляція розглядається як блоковий код, що забезпечує її легкість в апаратній реалізації. Саме цей набір властивостей зробив ССК-модуляцію обов'язковим методом кодування в стандарті IEEE 802.11b.

На практиці, однак, важливими є не лише теоретичні показники посилення. Рівномірність розподілу символів у фазовому просторі також відіграє ключову роль: чим більша відстань між символами, тим нижчою є ймовірність помилок під час їх детектування. У цьому аспекті ССК-модуляція має певні недоліки. Її реальне операційне посилення, як правило, не перевищує 2 дБ, що поступається теоретичному показнику. Через ці обмеження спочатку розглядали альтернативні підходи.

Одним із таких підходів стало пакетне бінарне згорткове кодування (PBCC – Packet Binary Convolutional Coding). Ця технологія була запропонована фахівцями компанії Alantro Communications, яка у 2000 році увійшла до складу Texas Instruments. PBCC увійшло до стандарту IEEE 802.11b як додатковий (необов'язковий) метод модуляції. Його впровадження дозволило досягати пропускної здатності в мережах IEEE 802.11b на рівні 5,5, 11 та 22 Мбіт/с (рисунок 1.9), розширюючи можливості застосування цього стандарту.

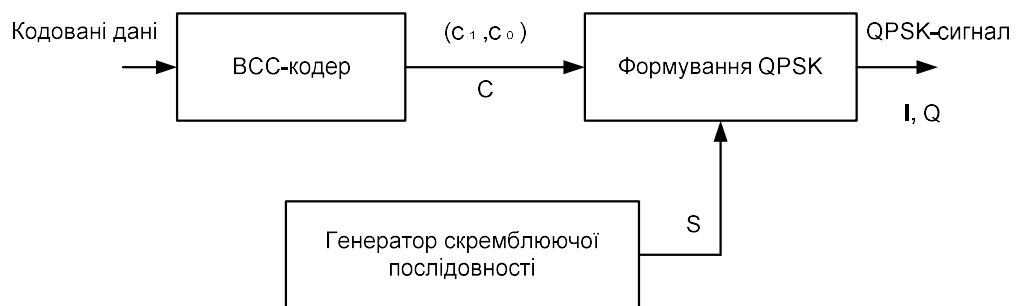


Рисунок 1.9 Загальна схема PBSS-Модуляції

Як випливає з назви, метод пакетного бінарного згорткового кодування (PBCC) базується на принципі згорткового кодування. Для швидкостей

передачі 5,5 і 11 Мбіт/с потік інформаційних бітів обробляється за допомогою шістирозрядного зсувного регістра, оснащеного суматорами (рисунок 1.10.а). На початковому етапі роботи всі тригери регістра ініціалізуються нулями. У результаті кожен вхідний біт інформації  $d$  замінюється двома бітами кодової послідовності  $c_0$  і  $c_1$ .

При швидкості передачі 11 Мбіт/с біти  $c_0$  і  $c_1$  формують один символ, що відповідає чотиріпозиційній QPSK-модуляції. Для швидкості 5,5 Мбіт/с застосовується двопозиційна BPSK-модуляція, яка послідовно передає біти  $c_0$  і  $c_1$ . Якщо необхідно досягти швидкості 22 Мбіт/с, схема кодування стає складнішою (рисунок 1.10.б): у цьому випадку три кодові біти  $c_0$ ,  $c_1$  та  $c_2$  визначають один символ у восьмипозиційній PSK-модуляції.

Після формування PSK-символів здійснюється процес скремблювання. Це змінює послідовність бітів для забезпечення рівномірності статистичного розподілу сигналу. У залежності від значення сигналу  $s$  (див. рисунок 1.9) символ залишається без змін ( $s = 0$ ) або його фаза збільшується на  $\pi/2$  ( $s = 1$ ). Значення  $s$  визначається 256-бітовою циклічно повторюваною послідовністю  $S$ , яка формується на основі початкового вектора  $U = 338B16$ .

Цей початковий вектор має рівну кількість нулів і одиниць, що сприяє оптимальному розподілу фазових зсувів. Послідовність  $S$  генерується у вигляді 16 векторів  $U_i$  (де  $i = 0 \dots 15$ ), причому кожен вектор  $U_i$  є циклічним зсувом попереднього  $U_{i-1}$  на кілька розрядів. Завдяки цьому підходу сигнал стає більш стійким до радіозавад і забезпечується стабільна передача даних навіть у складних умовах [1].

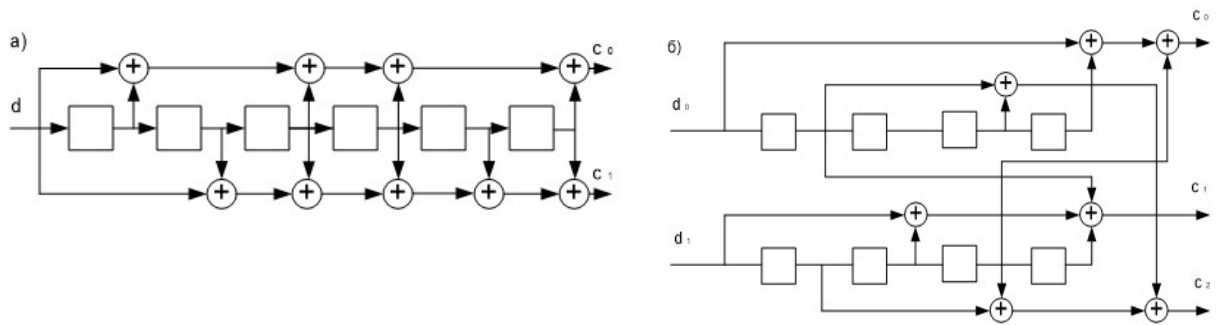


Рисунок 1.10 Схема зверточного ВСС-Кодування: а – для швидкостей 5,5 і 11 Мбіт/с; б – для швидкості 22 Мбіт/с

У шістирозрядного здвигового регістру, застосовуваного у РВСС для швидкостей 11 і 5,5 Мбіт/с, 64 можливих вихідних стану. Так що при модуляції РВСС інформаційні біти у фазовому просторі виявляються набагато далі друг від друга, чніж при СКК-Модуляції. Тому РВСС і дозволяє при тих самих співвідношенні сигнал/шум і рівні помилок вести передачу з більшою швидкістю, ніж у випадку СКК.

### ***Висновок по розділу***

Технологія Wi-Fi є надзвичайно гнучкою і пропонує широкий спектр режимів для організації та розгортання мереж. Незважаючи на те, що одним із основних недоліків цієї технології залишаються низький рівень безпеки та недостатній захист даних, стандарт IEEE 802.11 стає дедалі популярнішим у місцях великого скупчення людей, таких як кафе, аеропорти, ресторани. Однак його використання для організації масового доступу до Інтернету в житлових будинках все ще залишається рідкісним явищем.

Цьому сприяють два ключові чинники. По-перше, у багатьох користувачів досі не сформувалося чітке розуміння переваг технології Wi-Fi, а також способів її ефективного використання у побутових умовах. По-друге,

недостатньо розвинена інфраструктура, яка дозволила б забезпечити якісне підключення в житлових районах, обмежує поширення цієї технології.

Для подолання зазначених проблем необхідно зосередитися на кількох напрямках. Зокрема, важливим є активне рекламне просування переваг Wi-Fi, орієнтоване на широку аудиторію, яке допоможе підвищити обізнаність користувачів про можливості цієї технології. Також важливу роль відіграє інвестування у розвиток інфраструктури, що дозволить створити надійну основу для масштабного впровадження Wi-Fi у житлових будинках. Лише за умови комплексного підходу можна досягти значного розширення застосування цієї технології та забезпечити її ефективне використання у різних сферах.

## **2. ПЛАНУВАННЯ ЛОКАЛЬНОЇ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ**

### **2.1. Чинники, які потрібно враховувати при проектуванні безпроводної мультисервісної мережі 802.11g.**

При ухваленні рішень щодо розгортання безпроводних LAN (WLAN) необхідно враховувати:

- особливості роботи протоколу 802.11g;
- поведінка мобільних вузлів;
- питання захисту;
- якість зв'язку (QOS);
- додатки, використовувані безпроводними клієнтами.

Фізичний аспект виконання картування місця робіт дає можливість зрозуміти, яку зону покриття має кожна точка доступу, яка кількість точок доступу, необхідна для покриття заданої області, і встановити параметри кожного каналу і випромінювану потужність.

### **2.2. Архітектурна фаза проектування.**

Проектування мережі Wi-Fi виконується для дев'ятиповерхового житлового будинку. На кожному поверсі розташовано чотири квартири, кожна з яких має площу приблизно 50 квадратних метрів. Це створює потенційну абонентську базу з чотирьох користувачів на кожному поверсі.

Для забезпечення стабільного зв'язку точки доступу Wi-Fi встановлюються на 2-му, 5-му та 8-му поверхах. Кожна точка доступу підключається до маршрутизатора, розташованого на технічному поверсі будівлі, за допомогою окремого кабелю UTP категорії 5. Такий підхід дозволяє одній точці доступу обслуговувати три поверхи будівлі, що забезпечує

з'єднання для максимум 12 термінальних пристроїв. Ураховуючи, що висота одного поверху становить 3 метри, а загальна товщина міжповерхових перекриттів — 40 см, це рішення оптимізує покриття Wi-Fi сигналом, мінімізуючи втрати сигналу через будівельні матеріали.

Для прокладання горизонтальних кабельних систем передбачено використання таких типів каналів:

- ✓ металеві труби, що забезпечують захист кабелів при прокладанні між поверхами будівлі;
- ✓ декоративні коробки, виготовлені з негорючого пластику, що використовуються для розміщення точок доступу Wi-Fi.

Такий підхід забезпечує надійний захист кабелів від механічних пошкоджень і впливу навколишнього середовища, а також естетичний вигляд усієї інфраструктури. У цьому випадку кабельна система стає не лише функціональною, але й безпечною, відповідаючи сучасним вимогам протипожежної безпеки.

### ***2.3. Телекомунікаційна фаза проектування.***

На момент виконання проєктних робіт основним стандартом для створення локальних мереж є Fast Ethernet. Для реалізації горизонтальної підсистеми передбачено використання елементної бази категорії 5e, яка забезпечує передачу сигналів через структуровану кабельну систему (СКС) для всіх поширених протоколів Ethernet, включно з високошвидкісним Gigabit Ethernet 802.3ab. Це рішення дозволяє створити резерв пропускну здатності горизонтальних трактів СКС, достатній для підтримки не лише існуючих, але й перспективних видів додатків.

Згідно з початковими вимогами, інформаційно-обчислювальна система не передбачає передачу конфіденційних даних. Тому для побудови СКС було

обрано неекрановану елементну базу, яка є дешевшою та простішою в реалізації.

Кабелі категорії 5 спеціально розроблені для підтримки високошвидкісних протоколів. Їх характеристики відповідають частотному діапазону до 100 МГц, що забезпечує роботу протоколів зі швидкістю передачі даних до 100 Мбіт/с, таких як FDDI (з фізичним стандартом TR-PMD), Fast Ethernet і 100VG-Any LAN. Крім того, вони підтримують швидші протоколи, наприклад, АТМ зі швидкістю 155 Мбіт/с і Gigabit Ethernet зі швидкістю 1000 Мбіт/с.

*Основні електромагнітні характеристики кабелів категорії 5:*

- Повний хвильовий опір у діапазоні частот до 100 МГц становить 100 Ом (стандарт ISO 11801 також допускає опір 120 Ом).
- Загасання сигналу: від 0,8 дБ (на частоті 64 кГц) до 22 дБ (на частоті 100 МГц).
- Сумарне перехідне загасання на ближньому кінці (PS NEXT) — не менше 27,1 дБ.
- Захищеність на дальньому кінці (ELFEXT) — не менше 17 дБ.
- Активний опір не перевищує 9,4 Ом на 100 метрів.

Кабелі категорії 5е (покращені) розроблені для підтримки протоколу Gigabit Ethernet, який передає дані одночасно по всіх чотирьох парах кабелю. Частотний діапазон для категорії 5е залишається тим самим, що й для категорії 5 — до 100 МГц.

Всі кабелі UTP випускаються в чотирипарному виконанні, причому кожна пара має свій колір і певний крок скручування. Зазвичай дві пари використовуються для передачі даних, а інші дві — для передачі голосу.

Довжина ліній зв'язку також є критичним параметром під час проектування мережі. Для великих відстаней може знадобитися дороге обладнання або додаткові засоби захисту від зовнішніх радіозавад. Зі збільшенням відстані значно зростає вплив таких чинників на швидкість передачі даних, що вимагає ретельного вибору між Ethernet і Fast Ethernet. Рекомендується передбачати запас довжини (близько 10%) для врахування непередбачуваних обставин.

Для забезпечення майбутньої масштабованості мережі слід вибирати комутатори та маршрутизатори із запасом портів (10-20% більше, ніж потрібно на момент проектування). Це дозволить легко додати нові сегменти мережі в разі необхідності.

#### ***2.4. Вибір устаткування.***

Під час вибору мережевого обладнання необхідно враховувати низку важливих чинників, зокрема:

- ❖ відповідність стандартам і сумісність обладнання з найпоширенішими програмними рішеннями;
- ❖ швидкість передачі даних та можливість її збільшення у майбутньому;
- ❖ підтримувані топології мережі (шина, пасивна зірка, пасивне дерево) та їх комбінації;
- ❖ методи керування обміном у мережі (наприклад, CSMA/CD, повний дуплекс, маркерний метод);
- ❖ дозволені типи кабелів, їх максимальну довжину та стійкість до радіозавад;
- ❖ вартість та технічні характеристики обладнання (мережеві адаптери, трансивери, репітери, концентратори, комутатори).

На сучасному етапі для організації локальних мереж широко використовується неекранована вита пара (UTP) категорії 5e. Її популярність пояснюється такими перевагами:

1. Доступна ціна;
2. Наявність інструментів для швидкої та простої установки роз'ємів (RJ45);
3. Зручність під час прокладки кабелю в різних умовах;
4. Легкість ремонту у разі пошкодження;
5. Підтримка високошвидкісних протоколів (Fast Ethernet, Gigabit Ethernet) при використанні кабелів категорії 5e або вищої.

Для вибору точок доступу у цьому проєкті було обрано обладнання компанії D-Link, яке широко використовується у локальних мережах міста Харкова. Це обладнання характеризується високою надійністю, доступною ціною і здатністю ефективно задовольняти потреби як невеликих офісних мереж, так і житлових будинків. Зважаючи на ці переваги, для планування та вимірювань було обрано саме це устаткування.



Рисунок 2.1 Точка доступу Wi-Fi. D-Link DIR-415

Таблиця 2.1 Характеристика точки доступу D-Link DIR-415

Частота	2.412 - 2.484 ГГц
Потужність передавача (802.11b)	18dBm
Потужність передавача (802.11g)	16dBm
Швидкість передачі даних Super G:	108 Мбіт/сек;
802.11g:	54, 48, 36, 24, 18, 12, 9, 6 Мбіт/сек
802.11b:	11, 5.5, 2, 1 Мбіт/сек
Чутливість приймача (802.11b) 10 – 5 BER @	85 dBm
Чутливість приймача (802.11g) 10 – 5 BER @	75 dBm
Режими	Access Point, WDS Bridge (до 6 пристроїв)
Відповідність стандартам	IEEE 802.11g, IEEE 802.11b, 802.3 (Ethernet), 802.3u (Fast Ethernet)
Модуляція 802.11b:	ССК (11 і 5.5 Мбіт/сек), Barker Modulations (1, 2 Мбіт/сек)
802.11g:	OFDM (6, 9, 12, 18, 24, 36, 48, 54 Мбіт/сек)
Радіус дії	150 метрів в приміщенні
	400 метрів на відкритій місцевості

Продовження таблиці 2.1

Управління	Веб-сервер-інтерфейс
Порти	1 порт 10/100 Мбіт/сек LAN з підтримкою AUTO-MDIX
Безпека	WEP-кодування з 64- або 128-бітовим ключем; підтримка кодування WPA/WPA2 і WPA-PSK/WPA2-PSK; фільтрація по MAC-адресі
Антенa	2 зовнішніх незнімних дипольних антени 4dBi  2 внутрішніх антени
Посилення антени	4 dBi
Підтримка ОС	Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows 2003 Server; Linux; Mac.

#### ***2.4.1. Ресурс точки доступу.***

Кількість користувачів, які одночасно працюють із точкою доступу, значною мірою залежить від обсягу трафіку, який вони генерують (наприклад, розмір завантажуваних файлів). Пропускна спроможність безпроводової мережі, як і дротової, розподіляється між усіма активними користувачами. Ефективність роботи мережі зазвичай оцінюється за кількістю підключених пристроїв, які можуть одночасно працювати без помітного зниження якості зв'язку.

Для точки доступу, що працює за стандартом 802.11g, максимальна пропускна здатність становить до 54 Мбіт/с. Цього показника вистачає для обслуговування таких категорій користувачів:

– до 200 користувачів, які переважно перевіряють електронну пошту в текстовому форматі та мінімально використовують Інтернет;

– до 100 активних користувачів, які часто надсилають і отримують електронні листи, а також працюють із файлами середнього розміру;

– від 40 до 80 інтенсивно активних користувачів, які постійно завантажують і передають великі файли або використовують ресурсоємні додатки.

У нашому випадку одна точка доступу зможе легко обслуговувати 12 користувачів, забезпечуючи стабільний і якісний зв'язок. Такий підхід відповідає специфікаціям мережі та враховує обсяг середньостатистичного трафіку кожного абонента.

### ***2.5. Переваги безпроводних мереж передачі даних.***

Безпроводові локальні мережі (WLAN) мають низку суттєвих переваг у порівнянні з кабельними мережами (LAN):

- ✓ Мобільність: користувачі можуть вільно пересуватися в межах покриття мережі WLAN, зберігаючи доступ до інформаційних ресурсів та сервісів.
- ✓ Гнучкість інсталяції: WLAN легко розгортаються в умовах, де прокладка кабельної мережі є складною або неможливою, наприклад, у старовинних будівлях із архітектурними обмеженнями чи на відкритих просторах.

- ✓ Створення мобільних мереж: безпроводові технології дозволяють організувати тимчасові або пересувні локальні мережі для різноманітних задач.
- ✓ Швидкість розгортання: розгортання WLAN потребує значно менше часу, ніж створення кабельної інфраструктури.
- ✓ Низькі експлуатаційні витрати: витрати на підтримку безпроводових мереж є мінімальними, оскільки вони не потребують складного обслуговування кабельних систем.

Ці переваги роблять WLAN ідеальним рішенням для багатьох сценаріїв, де потрібен гнучкий, економічно вигідний та швидко впроваджуваний доступ до мережевих ресурсів.

## ***2.6. Недоліки безпроводних мереж передачі даних.***

Одним із головних недоліків технології Wi-Fi залишається низький рівень безпеки та недостатній захист даних і самих мереж. У багатоярусних міських умовах фізично відстежити та нейтралізувати зловмисника чи його обладнання, що працює в радіусі 100 і більше метрів, практично неможливо. Деякі власники мереж впроваджують додаткові заходи безпеки на вищих рівнях мережевої моделі, проте навіть це не робить Wi-Fi достатньо безпечним для використання в урядових установах чи ряді приватних компаній.

Більше того, значна частина діючих сьогодні мереж не використовує навіть базових засобів захисту, передбачених стандартом Wi-Fi. Наприклад, часто відсутні навіть елементарні паролі. Це створює ідеальні умови для злочинних дій кіберзловмисників. Хакери можуть безперешкодно проникати в зону покриття мережі, виконувати свої дії та залишати її. При цьому всі

докази, у разі розслідування, будуть вказувати на власника мережі, який може понести юридичну відповідальність за події.

Ще однією суттєвою проблемою технології Wi-Fi є високе енергоспоживання мобільних пристроїв через постійну роботу передавача. Це особливо помітно у невеликих пристроях, таких як смартфони чи КПК (PDA), через що багато виробників не поспішають впроваджувати Wi-Fi у свої моделі. Деякі компанії навіть закликають до введення режимів роботи на нижчих швидкостях передачі даних, які знижують витрати енергії, а також розробляють спеціальні енергоефективні чіпсети. Однак ці чіпсети часто не відповідають вимогам стандарту 802.11g, наприклад, щодо дальності дії.

Водночас розробляються нові покоління мікросхем, які дозволяють реалізувати енергозберігаючі функції, такі як "сплячий" режим для абонентських пристроїв. У цьому режимі базова станція мережі Wi-Fi може "розбудити" пристрій у разі необхідності, забезпечуючи баланс між енергозбереженням і функціональністю.

### **Висновки по розділу**

Зниження витрат на створення мережі можливе лише за умови ретельного аналізу всіх можливих варіантів її структури, включаючи сучасні технології безпроводового зв'язку, а також використання альтернативних методів підключення через електромережу або телефонні лінії. Таким чином, під час проєктування мережі особливо важливо уважно прорахувати всі аспекти, оскільки змінити або модернізувати вже прокладену кабельну систему в майбутньому буде досить складно. Ретельне планування на початковому етапі допоможе мінімізувати витрати та уникнути непотрібних фінансових і технічних втрат.

### **3. МЕТОДИКА РОЗРАХУНКУ**

#### **3.1 Моделі, використовувані для опису умов розповсюдження радіохвиль усередині будівель**

Останнім часом проблемі поширення радіохвиль усередині будівель і приміщень приділяється значна увага. Це зумовлено необхідністю створення локальних інформаційних мереж, а також забезпеченням надійного радіозв'язку для співробітників підприємств і установ з метою ефективного управління та підвищення рівня безпеки. Усередині будівель радіохвилі поширюються у складному середовищі, яке формується через наявність стін, перегородок, меблів, радіоелектронної апаратури, людей та інших об'єктів.

Умови поширення радіохвиль у приміщеннях значно відрізняються від їхнього поширення у відкритому просторі. Серед основних ефектів, які спостерігаються в таких умовах, можна виділити:

- ✓ багатопроменевість, що виникає внаслідок багаторазових відбиттів хвиль від стін і предметів;
- ✓ дифракцію, яка виникає на гострих краях об'єктів;
- ✓ розсіювання, що змінює напрямок і характер поширення хвиль.

Ці явища створюють складну інтерференційну структуру електромагнітного поля, яка суттєво змінюється під час руху людей або переміщення предметів. Як приклад, на рисунку 3.1 наведено графік залежності потужності прийнятого сигналу від відстані, виміряний усередині кімнати на частоті  $f = 914$  МГц. Він ілюструє складний інтерференційний характер поля з глибокими мінімумами (завмираннями) потужності сигналу.

Моделювання каналів зв'язку всередині будівель має певні особливості, що відрізняють їх від традиційних моделей мобільного зв'язку:

- зона покриття значно менша, ніж у міських умовах;
- умови поширення радіохвиль більш різноманітні через велику кількість перешкод та об'єктів.

Основними параметрами, що визначають поширення радіохвиль усередині будівель, є:

- планування приміщень;
- використані будівельні матеріали;
- тип будівлі.
- До явищ, характерних для поширення хвиль у приміщеннях, належать:
  - відбиття;
  - дифракція;
  - поглинання;
  - розсіювання.

На рівень сигналу впливають такі фактори, як відкриті чи закриті двері, висота розташування антен (на рівні столу чи під стелею), а також розташування стін і перегородок. Різноманітні об'єкти всередині будівлі, включаючи меблі, значно впливають на формування структури електромагнітного поля як у приміщенні, так і поза його межами.

Стіни та перегородки всередині приміщень зазвичай діляться на два типи:

- ✓ «тверді» стіни, які є конструктивними елементами будівлі;
- ✓ «м'які» перегородки, що можуть переміщуватися, зазвичай вони нижчі за висоту основних стін.

Матеріали, з яких виконані стіни та перегородки, мають різні електричні властивості, що значно ускладнює створення універсальної моделі для різних типів будівель.

Загасання сигналу між поверхами визначається:

- ❖ зовнішніми розмірами будівлі та її матеріалами;
- ❖ конструкцією міжповерхових перекриттів;
- ❖ зовнішнім середовищем (наявність сусідніх будівель чи об'єктів);
- ❖ кількістю вікон і характеристиками поверхонь стін.

Втрати сигналу всередині приміщень можуть бути описані математичними залежностями, що враховують вищезгадані фактори:

$$L(r) = L(r_0) + 10n \lg \frac{r}{r_0} + X_{\sigma}, \quad (3.1)$$

де  $n$  - залежить від типу будинку й навколишніх будівель;

$X_{\sigma}$  – випадкова величина, що підкоряється нормальному розподілу із дисперсією  $\sigma$ . Ця модель дає величину втрат, що відрізняється від обмірюваної в процесі експерименту не більше ніж на 4 дБ.

При поширенні радіохвиль між поверхами втрати описуються формулою

$$L(r) = L(r_0) + 10n_{SF} \lg \left( \frac{r}{r_0} \right) + FAF \quad (3.2)$$

де  $n_{SF}$  – показник ступеня, що характеризує поширення в межах одного поверху,  $FAF$  – фактор загасання між поверхами. Попередня формула може бути представлена в іншому виді

$$L(r) = L(r_0) + 10n_{MF} \lg \left( \frac{r}{r_0} \right) \quad (3.3)$$

де  $nmf$ – показник ступеня, що характеризує поширення між поверхами.

Більшість моделей, які використовуються для розрахунків поширення радіохвиль усередині будівель, базуються на формулі для відкритого простору. Однак у реальних умовах на характер поширення радіохвиль впливають численні чинники, такі як стіни, підлога, меблі, люди та інші об'єкти. Це різноманіття умов у приміщеннях вимагає застосування емпіричних моделей, розроблених на основі численних експериментальних досліджень.

У цій роботі розглянуто кілька моделей, які дозволяють оцінити втрати сигналу на трасі. Ці моделі базуються на співвідношеннях, що враховують вплив різних об'єктів та матеріалів на поширення радіохвиль у межах приміщень.

$$L(d) \approx L_p(d/d_0)^{-n}, \quad (3.4)$$

де  $L_p$ – втрати при поширенні на трасі прямої видимості довжиною  $d_0$ ,  $d$ – відстань між передавачем і приймачем. Причому, у деяких моделях значення  $n$  є постійною величиною, в інших – залежить від відстані. Наприклад, до відстаней близько 10м  $n=2$ , в інтервалі відстаней  $10 < d < 20$ м –  $n=3$ , для  $20 < d < 40$  м -  $n=6$ , при  $d > 40$ м -  $n=12$ . Збільшення значення  $n$  з ростом відстані, імовірно, пов'язане зі збільшенням числа стін, що відокремлюють прийомну антену від передавальної.

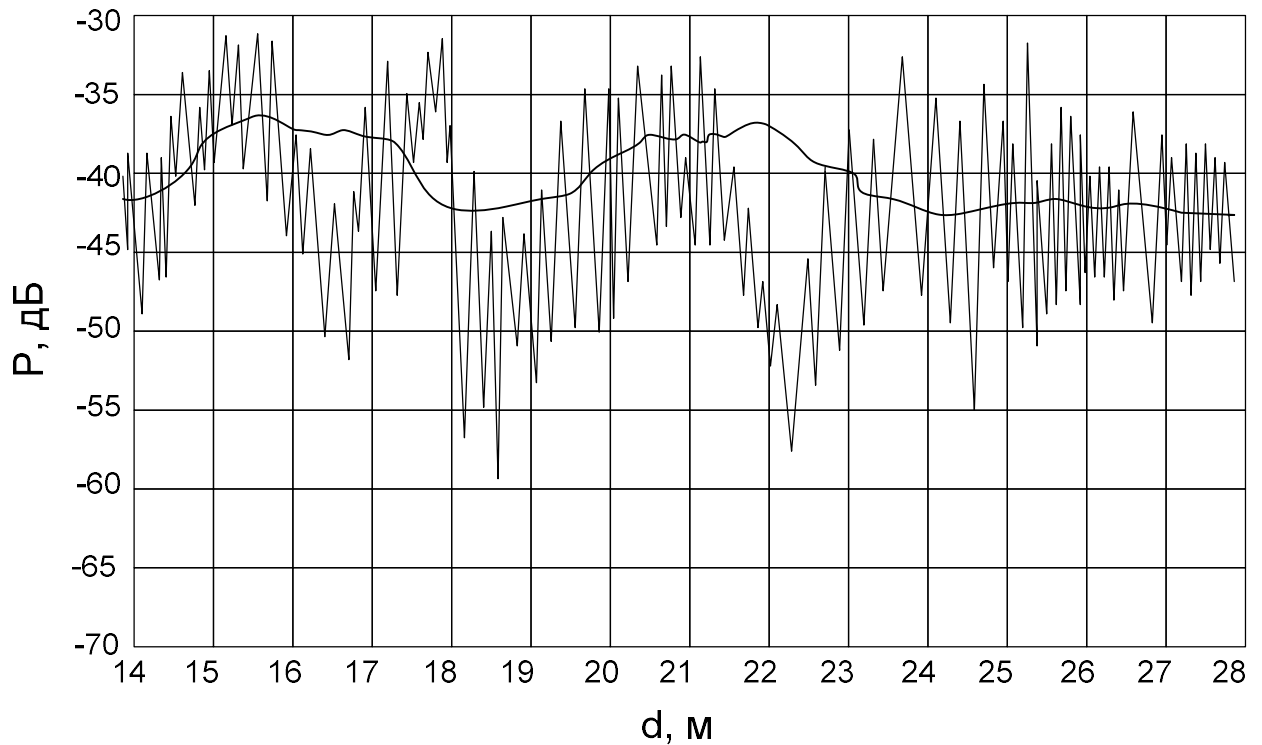


Рисунок 3.1 Залежність потужності прийнятого сигналу від відстані, обмірювана усередині кімнати на частоті  $f = 914$  МГц.

Коли передавальна антена розташована всередині кімнати, багаторазові відбиття радіохвиль від поверхонь приміщення, таких як стіни, підлога, стеля, меблі та інші об'єкти, сприяють збільшенню потужності прийнятого сигналу. Це явище схоже на реверберацію, добре вивчену у сфері акустики, де багаторазове відбиття звукових хвиль підсилює інтенсивність звуку в замкненому просторі.

Розглянемо невелику площу  $ds$ , довільно розташовану всередині кімнати. Якщо припустити, що радіохвилі поширюються рівномірно у всіх напрямках, то половина потужності хвилі, що розповсюджується, наприклад, ізліва направо, переноситься через цю площу за умови її нормального падіння. Однак, якщо хвиля падає під довільним кутом, середня переносна потужність зменшується приблизно вдвічі порівняно з нормальним падінням. Таким чином, через виділену площу проходить лише одна чверть загального потоку енергії.

Враховуючи ці обставини, щільність потоку енергії  $W$  на відстані  $d$  від джерела сигналу потужністю  $P_T$  у вільному просторі визначається відповідною формулою. Ця формула дозволяє оцінити розподіл енергії сигналу, зважаючи на специфічні умови поширення хвиль у приміщенні. При цьому вплив реверберації, відбиттів та інших факторів слід враховувати під час аналізу поширення радіохвиль.

$$W = \frac{P_T}{4\pi d^2}, \quad (3.5)$$

Уводячи середній коефіцієнт поглинання поверхні  $\bar{\alpha}$  та підсумовуючись по всій поверхні, можна записати співвідношення

$$\frac{W}{4} \sum S \bar{\alpha} P_T (1 - \bar{\alpha}). \quad (3.6)$$

Тоді для щільності потоку енергії ревербераційного поля маємо

$$W = \frac{4P_T}{R}, \quad R = \frac{\sum S \bar{\alpha}}{(1 - \bar{\alpha})}. \quad (3.7)$$

Комбінуючи потужність прямого сигналу й ревербераційного поля, а також враховуючи ефективну площу приймальної антени, отримуємо:

$$P_R = P_T \left( \frac{1}{4\pi d^2} + \frac{4}{R} \right) \left( \frac{\lambda^2}{4\pi} \right). \quad (3.8)$$

З (3.8) випливає вираження для втрат

$$L_P = \lg \left[ \left( \frac{1}{4\pi d^2} + \frac{4}{R} \right) \left( \frac{\lambda^2}{4\pi} \right) \right]. \quad (3.9)$$

Як приклад приведемо розраховані по формулі (3.9) залежності втрат від відстані для невеликої кімнати розмірами  $3,3 \times 5,1 \times 2,1$  м для різних значень коефіцієнта поглинання  $\alpha$  (Рисунок 3.2). Суцільною лінією для порівняння показані втрати при поширенні у вільному просторі.

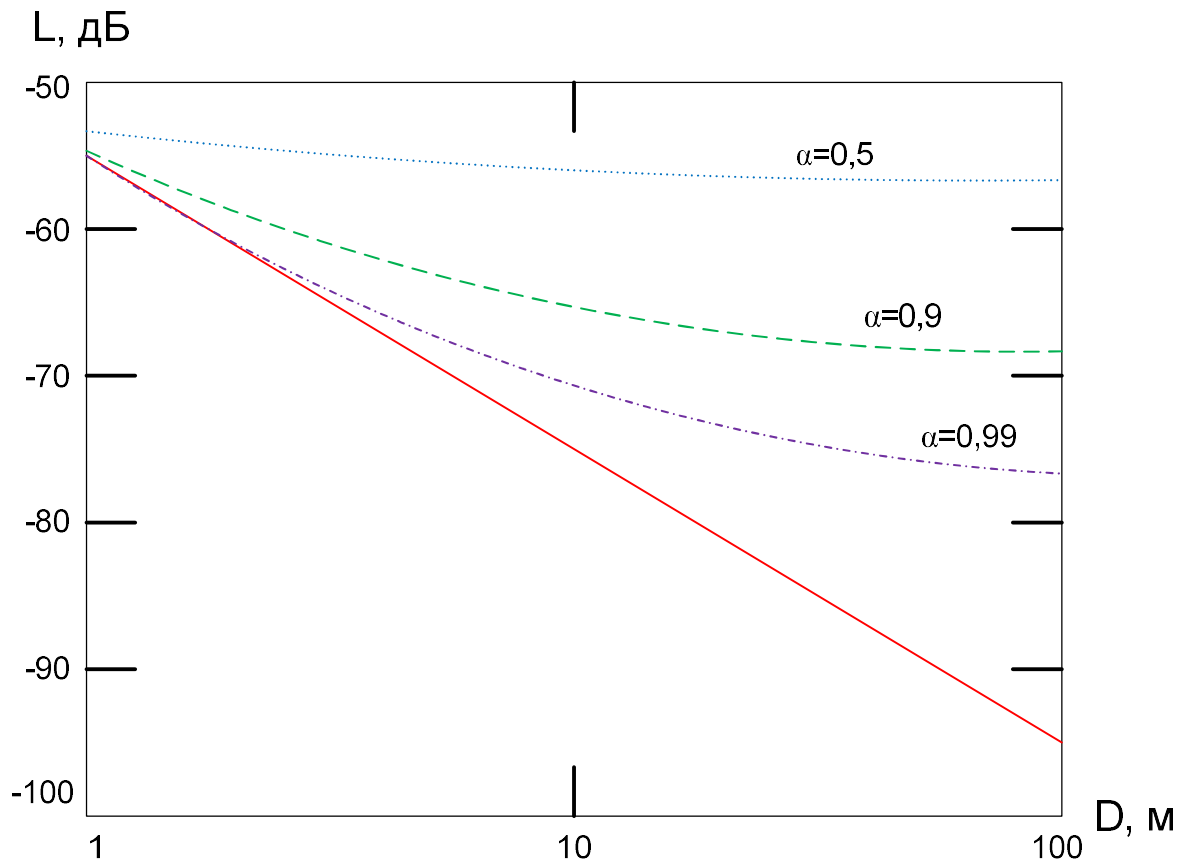


Рисунок 3.2 Залежності втрат від відстані для невеликої кімнати розмірами 3,3×5,1×2,1 м

На рисунку 3.3 представлені графіки залежності різниці втрат сигналу, обчислених за формулою (3.6), та втрат у вільному просторі залежно від відстані. Графіки побудовані для різних значень сумарної площі поглинаючої поверхні при ефективному коефіцієнті поглинання  $\alpha = 0,9$ . Цифри, зазначені біля кривих на графіку, вказують значення площі поглинаючої поверхні.

Аналіз графіків показує, що втрати сигналу в приміщенні суттєво залежать від властивостей будівельних матеріалів і покриттів. Зокрема, коефіцієнт відбиття та проходження радіохвиль, а також ефективний коефіцієнт поглинання  $\alpha$  будівельних матеріалів значно впливають на поширення радіосигналу. Ці параметри характеризують, наскільки сильно матеріали приміщення затримують, відбивають або поглинають радіохвилі.

Для конкретної частоти **60 ГГц** значення коефіцієнтів відбиття, проходження і поглинання для різних будівельних матеріалів наведено у таблиці 3.1. Ця інформація дозволяє оцінити вплив матеріалів на поширення сигналу, що є критичним для моделювання роботи безпроводових мереж у приміщеннях.

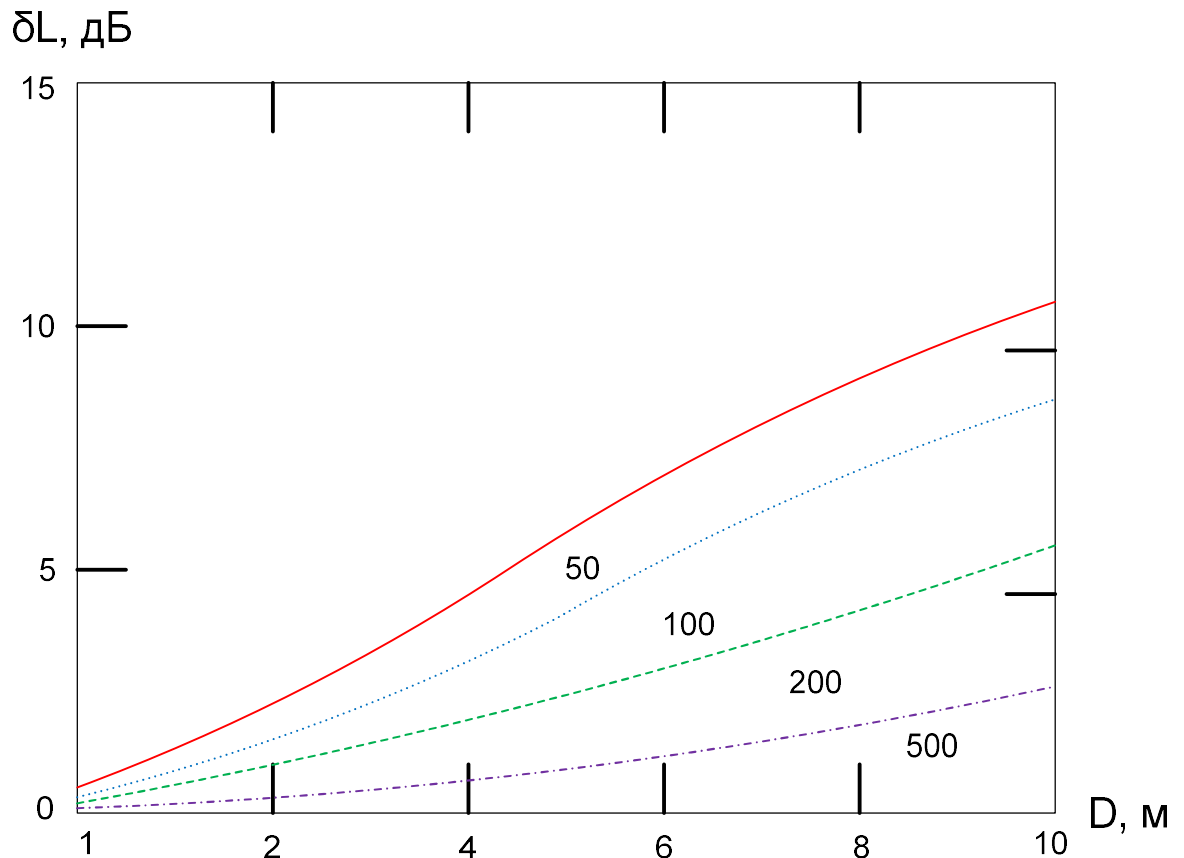


Рисунок 3.3 Залежності від відстані різниці втрат і втрат у вільному просторі при різних значеннях сумарної площі поверхні.

Під час вивчення поширення радіохвиль у міських умовах або всередині будівель і приміщень часто виникає потреба у визначенні коефіцієнта проходження хвилі через стіни, перегородки та інші багатоповітряні середовища. Для цього необхідно враховувати фізичні характеристики матеріалів, через які проходить хвиля.

Таблиця 3.1 Значення коефіцієнтів відбиття й проходження, а також ефективного коефіцієнта поглинання  $\bar{\alpha}$  для деяких матеріалів на частоті 60 ГГц

Матеріал	Коефіцієнт проходження, %	Коефіцієнт відбиття, %	$\bar{\alpha}$
Гіпсова панель (s=1 см)	42,5	2,0	0,98
Фіброліт (s=1,9 см)	4,5	20,0	0,8
Бетонна плита (s=10 см)	0,0001	16,0	0,84

Розглянемо випадок, коли електромагнітна хвиля падає на плоский шар товщиною  $\mathbf{d}$ , властивості якого визначаються відносною діелектричною проникністю  $\epsilon_2$  та магнітною проникністю  $\mu_2$ . У середовищі зліва від шару (для області  $\mathbf{z} < \mathbf{0}$ ) параметри середовища описуються величинами  $\epsilon_1$  та  $\mu_1$ , а для області справа від шару ( $\mathbf{z} > \mathbf{d}$ ) — параметрами  $\epsilon_3$  та  $\mu_3$ .

Для випадку ТЕ-поляризації електромагнітної хвилі (з поперечним електричним полем) компоненти електромагнітного поля можна описати за допомогою математичної моделі, яка враховує розподіл хвилі в кожній із трьох областей. Ця модель дозволяє визначити як коефіцієнт проходження хвилі, так і коефіцієнт відбиття залежно від властивостей матеріалів, кута падіння хвилі та її частоти.

Такі розрахунки є важливими для моделювання радіохвильового каналу в умовах багатоповерхових будівель і міської забудови, де хвиля проходить через різноманітні шари будівельних матеріалів із різними електромагнітними характеристиками:

в області  $z < 0$

$$E_y^{(1)} = e^{ik_1 \sin \vartheta_1 x} (e^{ik_1 \cos \vartheta_1 z} + R_d e^{-ik_1 \cos \vartheta_1 z}), \quad (3.10)$$

$$E - e^{ik_1 \sin \vartheta_1 x} \frac{\cos \vartheta_1}{\zeta_1} (e^{ik_1 \cos \vartheta_1 z} - R_d e^{-ik_1 \cos \vartheta_1 z}), \quad (3.11)$$

в області  $0 \leq z \leq d$

$$E_y^{(2)} = e^{ik_2 \sin \vartheta_2 x} (A e^{ik_2 \cos \vartheta_2 z} + B e^{-ik_2 \cos \vartheta_2 z}), \quad (3.12)$$

$$E - e^{ik_2 \sin \vartheta_2 x} \frac{\cos \vartheta_2}{\zeta_2} (A e^{ik_2 \cos \vartheta_2 z} - B e^{-ik_2 \cos \vartheta_2 z}), \quad (3.13)$$

в області  $z > d$

$$E_y^{(3)} = e^{ik_3 \sin \vartheta_3 x} T_d^\perp e^{ik_3 \cos \vartheta_3 z}, \quad (3.14)$$

$$E - e^{ik_3 \sin \vartheta_3 x} \frac{\cos \vartheta_3}{\zeta_3} T_d^\perp e^{ik_3 \cos \vartheta_3 z}. \quad (3.15)$$

У цьому контексті  $\vartheta_1$  позначає кут падіння хвилі на шар, а  $R_d^\perp$  і  $T_d^\perp$  — відповідно коефіцієнти відбиття та проходження для шару товщиною  $d$ . Для визначення цих коефіцієнтів необхідно враховувати умови поширення хвилі в багатошаровому середовищі.

Використовуючи умови безперервності тангенціальних компонентів електромагнітного поля на межах шарів (у точках  $z = 0$  і  $z = d$ ), можна вивести аналітичні вирази для коефіцієнтів відбиття та проходження. Ці умови гарантують, що значення електричного та магнітного полів є безперервними на границях шарів, що фізично відповідає збереженню енергії хвилі.

Отримані формули для  $R_d^\perp$  і  $T_d^\perp$  враховують такі параметри, як:

- кут падіння хвилі  $\vartheta_1$ ;
- діелектричну проникність та магнітну проникність середовищ;

- товщину шару  $d$ ;
- частоту хвилі.

Ці залежності є важливими для моделювання поведінки радіохвиль у багатошарових середовищах, таких як стіни будівель, міжповерхові перекриття або інші конструктивні елементи. Вони дозволяють оцінити рівень відбиття та частку енергії, що проходить крізь шар, забезпечуючи точність розрахунків у задачах проектування безпроводових мереж і систем зв'язку.

$$R_d^\perp = \frac{R_{23}^\perp e^{2i\delta} + R_{12}^\perp}{1 + R_{12}^\perp R_{23}^\perp e^{2i\delta}}, \quad (3.16)$$

$$R \frac{T_{12}^\perp T_{23}^\perp e^{i\delta}}{1 + R_{12}^\perp R_{23}^\perp e^{2i\delta}}, \quad (3.17)$$

де  $R_{12}^\perp$  і  $R_{23}^\perp$  – коефіцієнти відбиття Френеля плоскої хвилі, що падає ліворуч на границі розділа середовищ  $z = 0$  і  $z = d$ . Аналогічно  $T_{12}^\perp$  і  $T_{23}^\perp$  – коефіцієнти проходження плоскої хвилі через ці границі. Аналогічно можуть бути отримані відповідні коефіцієнти для Тм-Поляризації.

У низці наукових досліджень [29, 30] були ретельно вивчені властивості однорідних будівельних матеріалів, які впливають на поширення радіохвиль. Зокрема, були досліджені такі характеристики, як відносна діелектрична проникність і тангенс кута втрат у частотному діапазоні від 2 до 7 ГГц. Ці параметри дозволяють оцінити, наскільки матеріал впливає на загасання, відбиття та проходження радіосигналу, і є важливими для моделювання радіохвильового середовища всередині будівель.

Як приклад, у таблиці 3.2 наводяться типові значення відносної діелектричної проникності та тангенса кута втрат для деяких поширених будівельних матеріалів. Ці дані є основою для розрахунків ефективності роботи безпроводових мереж і оцінки втрат сигналу у реальних умовах.

Таблиця 3.2 Відносна діелектрична проникність і тангенс втрат

Матеріал	Відносна діелектрична проникність	Тангенс кута втрат
Оргскло	2,74	$3,2 \cdot 10^{-4}$
Жалюзі (закриті)	3,49	$5,96 \cdot 10^{-5}$
Жалюзі (закриті)	1,96	$5,96 \cdot 10^{-5}$
Червона цегла (суха)	5,86	$1,16 \cdot 10^{-5}$
Червона цегла (волога)	5,92	$1,17 \cdot 10^{-1}$
Килим	1,32	$5,96 \cdot 10^{-4}$
Стельове покриття	1,32	$1,44 \cdot 10^{-2}$
Тканина	1,49	$5,96 \cdot 10^{-5}$
Скловолокно	1,02	$9,21 \cdot 10^{-4}$
Стекло	6,38	$2,6 \cdot 10^{-2}$
Лінолеум	3,08	$1,45 \cdot 10^{-3}$
Хвойна дошка	2,58	$2,0 \cdot 10^{-2}$
ДСП	2,7	$1,1 \cdot 10^{-1}$
Фанера	2,47	$1,27 \cdot 10^{-1}$
Гіпсова плита	1,07	$4,29 \cdot 10^{-1}$
Кахель	3,08	$5,88 \cdot 10^{-2}$
Толь	2,47	$3,86 \cdot 10^{-2}$

У тій самій роботі представлені результати вимірювань коефіцієнтів проходження та відбиття для тих самих будівельних матеріалів. Дослідження проводилося на двох частотах — **2,3 ГГц** і **5,25 ГГц**, що дозволяє оцінити вплив частоти сигналу на поведінку радіохвиль під час взаємодії з різними матеріалами.

Отримані дані є важливими для моделювання поширення радіохвиль у будівлях, оскільки вони дозволяють враховувати специфічні властивості матеріалів під час проектування безпроводових мереж. Відповідні результати вимірювань наведено у таблиці 3.3, що слугує базою для аналізу ефективності радіосигналів у приміщеннях із різними будівельними елементами.

Таблиця 3.3 Коефіцієнти проходження й відбиття

Матеріал	T(дБ)			R(дБ)		
	2,4 ГГц	5,25 ГГц	Δ	2,4 ГГц	5,25 ГГц	Δ
1	2	3	4	5	6	7
Оргскло (7,1 мм)	-0,356	-0,927	0,5707	-12,2	-5,65	-6,575
Оргскло (2,5 мм)	-0,005	-0,204	0,1994	-21,7	-13,25	-8,477
Жалюзі (закриті)	-0,002	0,002	-0,004	-31	-20,39	-10,58
Жалюзі (відкриті)	0,0137	0,0315	-0,018	-44,2	-46,95	2,721
Червона цегла (волога)	-4,512	-14,6	10,087	-12,5	-9,41	-3,119
Червона цегла (суха)	-4,435	-14,62	10,182	-12,5	-8,98	-3,546
Килим	-0,027	-0,006	-0,021	-26,9	-18,7	-8,271

Продовження таблиці 3.3

1	2	3	4	5	6	7
Стельове покриття	-0,087	-0,18	0,0923	-21,1	-18,7	-2,347
Тканина	0,0216	0,0133	0,0083	-41,7	-30,1	-11,57
Стекло	-0,5	-1,691	1,1908	-11,3	-4,9	-6,345
Лінолеум	-0,02	-0,128	0,1081	-23,7	-16	-7,669
ДСП	-1,651	-1,951	0,2997	-8,59	-14,1	5,5359
Фанера	-1,914	-1,834	-0,08	-9,05	-30,5	21,42
Гіпсова плита	-14,86	-13,24	-1,628	-2,38	-9,24	6,858 7
Кахель	-2,216	-1,422	-0,795	-6,24	-14,9	8,609 3
Толь	-0,096	-0,134	0,038 5	-28,9	-17,8	-11,07
Шлакоблок (сухий)	-6,714	-10,33	3,611 9	-7,67	-6,13	-1,532
Шлакоблок (вологий)	-7,353	-12,38	5,031 3	-5,05	-7,55	2,508 0

Варто зазначити, що найбільші відмінності в коефіцієнтах проходження радіохвиль у різних частотних діапазонах спостерігаються для матеріалів, таких як червона цегла та шлакоблоки. Ці матеріали суттєво впливають на характеристики сигналу, особливо в умовах багатоповерхових будівель або густої міської забудови, де вони широко використовуються.

Для розрахунку характеристик сигналів усередині приміщень застосовуються різні модифікації променевих методів. Ці методи дозволяють враховувати численні фактори, що впливають на поширення радіохвиль, зокрема:

- ✓ відбиття хвиль від стін, підлоги, стелі та інших великих поверхонь;
- ✓ взаємодію радіосигналу з місцевими предметами, такими як меблі чи техніка;
- ✓ дифракцію хвиль на краях дверей і вікон;
- ✓ розсіювання, спричинене нерівностями поверхонь та наявністю людей у приміщенні.

Застосування таких підходів дозволяє моделювати поширення сигналів із високою точністю, враховуючи всі основні явища, які супроводжують проходження радіохвиль у замкнених просторах. Це важливо для оптимального проектування безпроводових мереж і забезпечення стабільності їхньої роботи в реальних умовах.

### ***3.2 Порівняння результатів вимірювань і розрахунків***

На рисунку 3.4 представлені результати вимірювань загасання сигналу всередині будівлі на різних відстанях від передавача. Кружечками позначено результати вимірювань, виконаних на тому ж поверсі, де знаходився передавач, а іншими значками — вимірювання, проведені на інших поверхах.

Аналіз отриманих даних показав, що загасання сигналу значною мірою залежить від розташування приймальної антени. На цьому ж графіку пунктирною лінією показано залежність загасання від відстані між

передавальною та приймальною антенами, яка була розрахована за емпіричною формулою.

Середнє значення загасання сигналу на відстані 10 метрів від передавача становить приблизно **75 дБ**, але відхилення від цього значення можуть досягати **13 дБ**. Така значна варіативність обумовлена нерівномірністю умов поширення радіохвиль у приміщеннях, включаючи багатопроменевість, відбиття від стін і меблів, а також дифракцію на краях об'єктів.

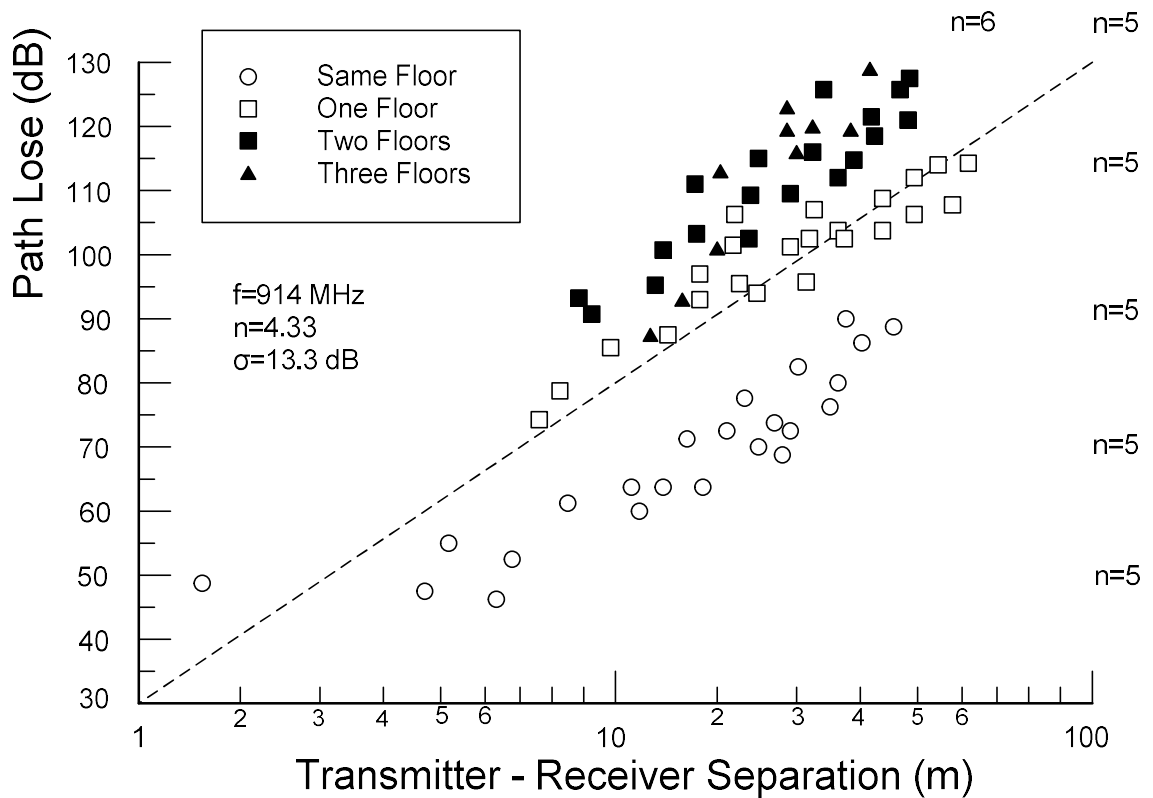


Рисунок 3.4 Результати вимірів загасання сигналу усередині будинку на різних відстанях від передавача.

Ці результати підкреслюють важливість урахування просторового розташування антен і характеристик середовища під час проєктування безпроводових мереж у багатоповерхових будівлях. Вони також демонструють обмеження емпіричних моделей, які дають лише усереднені

оцінки, але не враховують локальних особливостей приміщень і будівельних матеріалів.

### **3.3 Оцінка пропускної спроможності**

Роботу досліджуваної безпроводової локальної мережі (БЛМ) можна умовно розбити на неоднорідні віртуальні слоти часу. У кожному з цих слотів станції послідовно зменшують значення свого лічильника відкладеного часу на одиницю. Як тільки лічильник якоїсь станції досягає нуля, вона отримує можливість почати передачу даних. Віртуальний слот часу може бути одного з трьох типів:

1. «Порожній» слот: жодна з наявних станцій у цьому слоті не веде передачу.
2. «Успішний» слот: передача виконується лише однією станцією.
3. «Колізійний» слот: дві або більше станцій починають передачу одночасно, що призводить до конфлікту.

Припустимо, що ймовірність початку передачі кожною станцією у будь-якому конкретному слоті є однаковою і незалежною як від попередніх подій, так і від поведінки інших станцій. Це значення ймовірності залишається сталим для всіх станцій.

Тоді ймовірність того, що випадково вибраний віртуальний слот буде:

- ✓ «порожнім» (жодна станція не передає дані),
- ✓ «успішним» (передача ведеться однією станцією),
- ✓ «колізійним» (одночасна передача кількома станціями),

визначається відповідними математичними виразами, представленими у [12].

$$p_e = (1 - \tau)^N = (1-)^{10} =$$

$$p_s = N\tau(1 - \tau)^{N-1} = 10 * (1-)^9 =$$

$$p_c = 1 - p_e - p_s = 1 - =$$

Ці формули враховують загальну кількість станцій, їх імовірність початку передачі та механізм розподілу слотів.

Такий підхід дозволяє моделювати поведінку мережі в умовах конкуренції за спільний канал передачі, оцінювати ефективність протоколів доступу до середовища та виявляти ключові фактори, які впливають на ймовірність виникнення колізій.

Таким чином, шукана пропускна спроможність  $S$  знаходиться по виразу [12]:

$$S = \frac{p_s U}{p_e \sigma + p_s T_s + p_c T_c} = \frac{\square}{+} \quad (3.18)$$

де  $T_s$  і  $T_c$  - середня тривалість «успішного» і «колізійного» слотів, а  $U$  – середнє число байт інформації, успішно переданих протягом «успішного» слота.

Тривалість «колізійного» слота визначається як сума кількох компонентів. По-перше, це час передачі фрейма максимальної довжини серед тих, що беруть участь у колізії. По-друге, додається інтервал EIFS (Extended Interframe Space), який використовується для відновлення синхронізації після колізії. Нарешті, до цієї тривалості додається «порожній» слот затримки, який завжди завершує невдалу спробу передачі відповідно до прийнятого механізму управління доступом до середовища.

Припускаючи, що ймовірність колізії більше двох фреймів є настільки малою, що нею можна знехтувати, можна отримати формулу для обчислення

середньої тривалості «колізійного» слота. Ця формула враховує стандартні параметри мережі, такі як максимальна довжина фрейма, час очікування в інтервалі EIFS та механізм завершення невдалої передачі. Її розрахунок наводиться у джерелі [12].

Така оцінка є важливою для аналізу продуктивності безпроводової мережі, оскільки дозволяє моделювати втрати продуктивності, спричинені колізіями, та визначати оптимальні параметри для зниження затримок і збільшення ефективності передачі даних.

$$T_c = \sum_{l=l_{\min}}^{\bar{p}} t_d(l) \hat{d}_l \left\{ \hat{d}_l + 2 \left( \sum_{k=l_{\min}}^{l-1} \hat{d}_k + \sum_{k=P+1}^{l_{\max}} \hat{d}_k \right) \right\} + t_{RTS} \left( \sum_{l=P+1}^{l_{\max}} \hat{d}_l \right)^2 + EIFS + \sigma + \delta \quad (3.19)$$

де  $t_d(l) = H + l/V$  час передачі фрейма DATA, що включає пакет завдовжки  $l$  і заголовки, передаваний за час  $H$ ;

$t_{RTS}$  - час передачі фрейма RTS, причому  $t_{RTS} < H$ ;

$\delta$  - час розповсюдження сигналу, передбачуваний однаковим для всіх пар станцій.

Нарешті,  $\hat{d}_l$  - вірогідність того, що здійснювана звичайна спроба передачі пов'язана з пакетом завдовжки  $l$ . Відмітимо, що розподіл  $\{d_l, l = l_{\min}, \dots, l_{\max}\}$  відрізняється від, оскільки число спроб, здійснюваних для передачі одного і того ж пакету, в середньому тим більше, чим довше пакет зважаючи на більшу вірогідність спотворення відповідного фрейма DATA перешкодами.

На початку «успішного» слота одна і лише одна станція ініціює передачу пакета довжиною  $l$ . Ця спроба вважається успішною, якщо всі фрейми, якими обмінюються передавальна та приймальна станції під час процесу передачі, проходять без спотворень. Іншими словами, успішна передача можлива за умови, що жоден із фреймів не зазнає впливу радіозавад або інших негативних факторів, які можуть призвести до спотворення даних.

Ймовірність успішної передачі залежить від низки параметрів, зокрема:

- ❖ якості радіосигналу на момент передачі;
- ❖ рівня радіозавад у середовищі;
- ❖ коректності роботи механізмів виявлення та корекції помилок;
- ❖ довжини пакета  $I$ , адже з більшою довжиною пакета збільшується ймовірність помилки.

Таким чином, успіх передачі визначається ймовірністю відсутності спотворень для всіх фреймів протягом усього процесу обміну. Цей показник є ключовим для оцінки ефективності роботи безпроводової мережі та розробки протоколів, що знижують імовірність впливу негативних факторів на передачу даних [12].

$$\pi_h(l) = [1 - \xi_d(l)](1 - \xi_a) \text{ при } l \leq \bar{P} \quad (3.20)$$

і

$$\pi_h(l) = [1 - \xi_d(l)](1 - \xi_a)^2 \text{ при } l > \bar{P} \quad (3.21)$$

де,  $\xi_r$  і  $\xi_a$  - вірогідність спотворення перешкодами фрейма DATA з пакетом завдовжки, фрейма RTS ( $\xi_r$ ) і фреймів CTS і ACK ( $\xi_a$ ) що мають однаковий формат. Ця вірогідність спотворення визначається на основі показника BER (Bit Error Rate) – вірогідність спотворення одного біта (цей показник називатиметься також інтенсивністю перешкод), тобто фрейм, що складається з  $l_f$  байт, спотворюється з вірогідністю

$$\xi_{lf} = 1 - \exp\{-8l_f BER\}$$

Спроба передачі пакета завершується при спотворенні перешкодами будь-якого з обмінюваних фреймів. Таким чином, середня тривалість спроби,

що здійснюється протягом «успішного» слота, залежить від довжини  $I$  переданого пакету і рівна

$$t_s(l) = A_1(l)[(1 - \xi_d(l))(t_{ACK} + SIFS + \delta) + t_d(l) + SIFS + \delta] + A_0(l) + t_{IF}(l)$$

де при

$$A_1(l) = (1 - \xi_r)(1 - \xi_a)$$

$$A_0(l) = (1 - \xi_r)(t_{CTS} + SIFS + \delta)$$

А при

$$A_1(l) = 1$$

$$A_0(l) = -SIFS$$

Крім того,  $t_{RTS}$ ,  $t_{CTS}$  і  $t_{ACK}$  часи передачі відповідно фреймів RTS, CTS і ACK, а  $t_{IF}(l) = \pi_h(l)DIFS + [1 - \pi_h(l)]EIFS$ .

При успішному завершенні процесу передачі станція вибирає з черги наступний пакет і з вірогідністю  $W_0^{-1}$  ініціює процес його передачі (ситуація миттєвого повтору), таким чином продовжуючи поточний віртуальний слот. Віртуальний слот завершується «порожнім» слотом затримки або при невдалому завершенні процесу передачі, або при виборі відкладеного часу  $b > 0$  (з вірогідністю  $1 - W_0^{-1}$ ) після успішного завершення передачі. Таким чином, протягом «успішного» слота може відбутися як одна, так і декілька спроб передачі пакетів, причому при першій спробі довжина передаваного пакету  $I$  визначається імовірнісним розподілом, а при подальших спробах розподілом  $\{d_i\}$ .

Нехай  $\pi_h^0$  і  $T_s^0$  - значення вірогідності  $\pi_h(l)$  і тривалості  $t_s(l)$ , усереднені відповідно до розподілу  $\{\bar{d}_l\}$ , тобто

$$\pi_h^0 = \sum_{l=l_{\min}}^{l_{\max}} \pi_h(l) \hat{d}_l \quad T_s^0 = \sum_{l=l_{\min}}^{l_{\max}} t_s(l) \hat{d}_l$$

А при  $\pi_h^1$  і  $T_s^1$  - аналогічні значення, але з використанням при усереднюванні розподілу  $\{d_l\}$  замість  $\{\hat{d}_l\}$ . Тоді середня тривалість «успішного» слота знаходиться по формулі:

$$T_s = \sigma + T_s^0 + \frac{c}{W_0} T_s^1 \sum_{i=0}^{\infty} \left( \frac{\pi_h^1}{W_0} \right)^i = \sigma + T_s^0 + \frac{\pi_h^0 W_0^{-1} T_s^1}{1 - \pi_h^1 W_0^{-1}} \quad (3.22)$$

Отже, визначені всі необхідні компоненти формули 3.18, що дозволяє знайти шукану пропускну спроможність  $S$  за умови, що відомі вірогідність початку передачі і вірогідність розподілу  $\{\bar{d}_l\}$ .

### **3.4 Моделювання безпроводової локальної мережі в умовах високого навантаження**

Ефір, як і радіоканал у безпроводових мережах, є унікальним середовищем передачі, доступним усім станціям одночасно. За своєю поведінкою він нагадує концентратор у дротовій мережі Ethernet: коли кілька станцій одночасно намагаються передати дані, їхні сигнали починають взаємно заважати один одному. У такій ситуації в безпроводових мережах, як і в Ethernet, виникає явище, що називається колізією.

Щоб зменшити ймовірність колізій, стандарти WLAN передбачають механізм перевірки середовища перед передачею. Станція перевіряє, чи є

середовище вільним, перш ніж розпочати передачу. Однак це не гарантує, що дві або більше станцій одночасно не визначать середовище як вільне і не почнуть передачу. Така ситуація призводить до конфлікту, який у дротових мережах Ethernet називається колізією.

У дротових мережах відправники можуть розпізнати колізію під час передачі, припинити її та повторити спробу після випадкового інтервалу часу. У радіомережах цього недостатньо, оскільки станції не можуть одночасно передавати й отримувати сигнал. Для вирішення цієї проблеми в стандарті 802.11 було введено механізм підтвердження прийому пакета (ACK). Одержувач надсилає підтвердження відправнику, що вимагає додаткового часу очікування.

Якщо врахувати всі передбачені протоколом періоди очікування, включно з міжкадровими інтервалами Short Inter Frame Space (SIFS) і Distributed Coordination Function Inter Frame Space (DIFS) для мереж стандарту 802.11a, накладні витрати на кожен пакет становлять близько 50 мкс. Ці витрати включають час для передачі підтвердження, обробки колізій та повторних спроб передачі (рисунк 3.5).

Цей підхід дозволяє забезпечити надійну передачу даних у безпроводовій мережі, хоча накладні витрати збільшують загальний час передачі пакета.

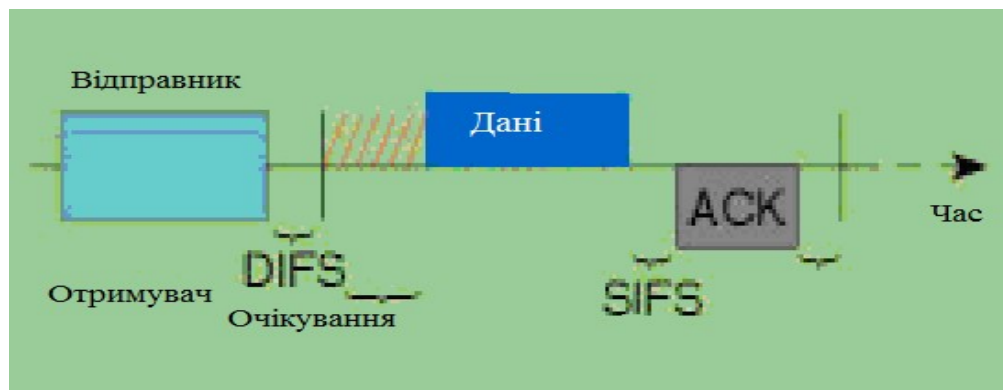


Рисунок 3.5 Витрати часу для передачі підтвердження, обробки колізій та повторних спроб передачі.

Коли станція WLAN планує розпочати передачу, але виявляє, що середовище зайняте, вона змушена чекати. Доступ до середовища регулюється за допомогою міжкадрових інтервалів різної тривалості, таких як DIFS (Distributed Inter-Frame Space) і SIFS (Short Inter-Frame Space). Ці інтервали забезпечують керування передачею даних і уникнення колізій у середовищі.

При аналізі витрат часу також необхідно враховувати, що кожен пакет даних містить не лише корисну інформацію, але й службові заголовки, що належать до різних рівнів протоколу (рисунок 3.6). Наприклад, у випадку пакета довжиною 1500 байт, який передається за стандартом 802.11 зі швидкістю 54 Мбіт/с, додатково передається 64 байти службових даних, що відповідає витратам часу у 20 мкс.

Крім того, підтверджувальний пакет АСК (Acknowledgement) обробляється фізичним рівнем аналогічно основному пакету даних. Однак у пакеті АСК відсутні деякі частини, такі як порядковий номер і контрольна сума, а його заголовок є скороченим. Завдяки цьому час обробки пакета АСК становить лише 24 мкс. Ці скорочені накладні витрати дозволяють ефективніше використовувати середовище передачі, зберігаючи загальну продуктивність мережі.

Такі особливості структури даних і процедури доступу до середовища є ключовими елементами, що впливають на ефективність роботи безпроводових мереж.

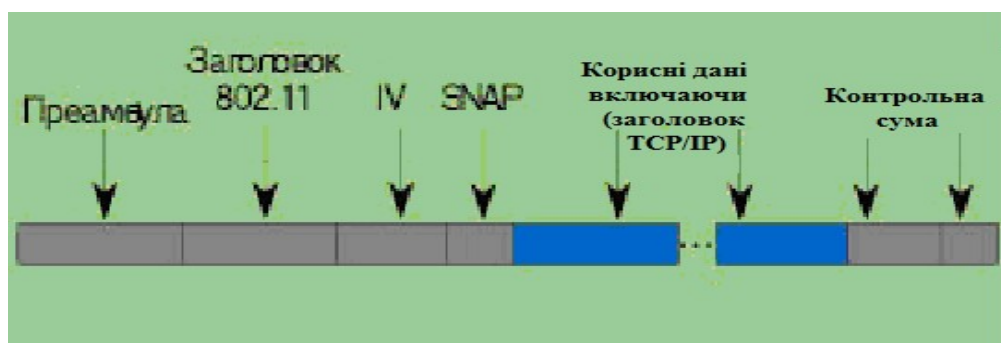


Рисунок 3.6 Заголовки для протокольних рівнів.

У пакеті даних WLAN корисна інформація обрамлена преамбулою, заголовком і контрольною сумою. Ці службові елементи є основною причиною значного розриву між номінальною та фактичною швидкістю передачі даних. Наприклад, передача пакета довжиною 1500 байт із номінальною швидкістю 54 Мбіт/с займає приблизно 325 мкс, що знижує фактичну швидкість передачі до 37 Мбіт/с.

Додаткові накладні витрати, пов'язані з протоколами верхнього рівня, такими як TCP/IP (наприклад, службові дані у 40 байт на кожен пакет, а також підтверджувальні TCP пакети), і повторні передачі через збої ще більше знижують швидкість. У підсумку реальна швидкість передачі зменшується до 25 Мбіт/с. Аналогічне співвідношення спостерігається і в стандарті 802.11b: при номінальній швидкості 11 Мбіт/с фактична швидкість становить лише 5–6 Мбіт/с.

Стандарт 802.11g, що є спадкоємцем 802.11b і базується на подібних принципах, має вимогу зворотної сумісності з 802.11b, що може ще більше знижувати швидкість передачі даних. Проблеми виникають, коли у процес передачі між двома пристроями стандарту 802.11g втручається пристрій 802.11b. Оскільки методи модуляції в цих стандартах різні, пристрої 802.11b не можуть розпізнати зайнятість середовища і починають власну передачу, що призводить до колізій.

Для уникнення таких конфліктів станції 802.11g перед передачею основних даних надсилають пакет Clear To Send (CTS), сумісний зі стандартом 802.11b. Цей пакет резервує середовище на певний час, повідомляючи всі пристрої про зайнятість каналу. Проте передача такого пакета створює додаткові витрати, оскільки його розмір порівнянний із розміром основного пакета даних. У результаті практична швидкість передачі може впасти до 15 Мбіт/с.

Основні втрати швидкості виникають, коли в одному каналі одночасно працюють пристрої, що підтримують обидва стандарти — 802.11b і 802.11g. Навіть якщо в мережі використовується виключно обладнання 802.11g, присутність сусіднього пристрою 802.11b може значно знизити продуктивність. Хоча багато пристроїв 802.11g підтримують режим «тільки g», у якому відключається передача пакетів CTS, такий підхід не рекомендується. Втрата даних через колізії може призвести до ще більшого зниження пропускної здатності порівняно зі стандартною процедурою передачі.

Спочатку стандарт 802.11 був розроблений для роботи на швидкостях 1 та 2 Мбіт/с. Усі службові дані також передавалися на цих швидкостях. Передавальні станції інформували інші пристрої, що ефір буде зайнятий з моменту часу X до моменту часу Y, щоб уникнути конфліктів. Інші станції в цей період припиняли передачу, не створюючи завад.

Стандарт 802.11b враховував сумісність із 802.11. Це означало, що пристрої 802.11b повинні були передавати службові дані на швидкостях 1 або 2 Мбіт/с, зрозумілих для пристроїв 802.11. Інакше старі пристрої могли б проігнорувати зайнятість середовища та почати власну передачу, створюючи конфлікти. Процедура відправки одного кадру в стандарті 802.11b представлена на рисунку 3.7:

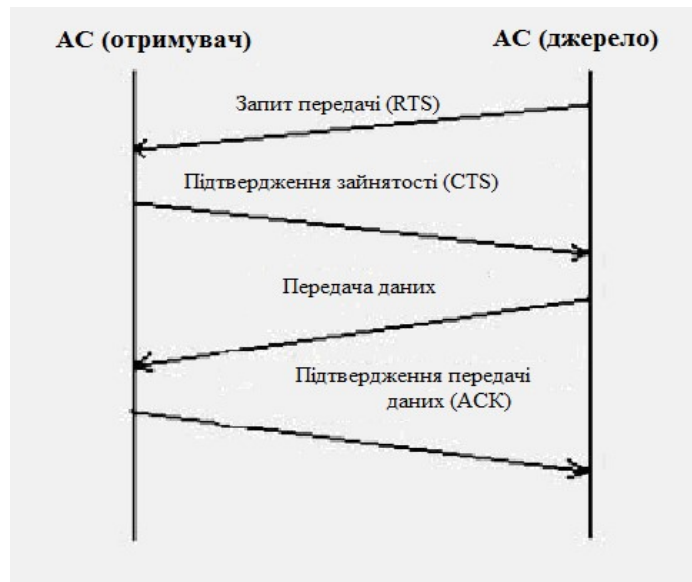


Рисунок 3.7 Процедури відправки одного кадру в стандарті 802.11b.

Пояснення до рисунка 3.7:

На рисунку наочно відображена передача ряду попередніх службових пакетів, а також пакетів підтвердження отримання інформаційного пакету.

Базовий алгоритм передачі даних у безпроводовій мережі складається з двох основних етапів: передача кадру даних від джерела до одержувача та передача підтвердження прийому (ACK, **Acknowledge**) від одержувача до джерела. Такий підхід дозволяє забезпечити базову надійність передачі, гарантуючи, що переданий кадр успішно досягнув одержувача.

Для підвищення надійності передачі використовується вдосконалений алгоритм, що включає обмін чотирма кадрами. У цьому випадку процес передачі виглядає наступним чином:

1. AC-джерело (станція-джерело) передає кадр запиту на передачу (RTS, Request to Send) до одержувача. Цей кадр служить сигналом для всіх станцій у зоні радіовидимості про початок обміну інформацією.

2. Усі станції, які отримали кадр RTS, тимчасово утримуються від передачі даних, щоб уникнути можливих конфліктів у середовищі передачі.
3. АС-одержувач (станція-одержувач) у відповідь передає кадр готовності до прийому (CTS, Clear to Send) до станції-джерела. Цей кадр підтверджує готовність одержувача прийняти дані.
4. Після отримання кадру CTS станція-джерело передає основний кадр даних до одержувача.
5. Після успішного отримання кадру даних станція-одержувач надсилає підтвердження прийому у вигляді кадру АСК.

Такий обмін дозволяє мінімізувати колізії та покращити загальну стабільність і надійність передачі даних у мережі. Завдяки RTS/CTS-обміну конфлікти між станціями знижуються, оскільки всі пристрої, що отримали кадр RTS, знають про зайнятість середовища передачі.

Цей алгоритм є основою для забезпечення ефективної роботи безпроводових мереж, особливо в умовах підвищеного навантаження або великої кількості станцій, що працюють у межах одного радіоканалу.

Для того, щоб відобразити реальну пропускну спроможність мережі стандарту 802.11b детально розглянемо часову діаграму доступу до середовища з використанням режиму передачі DCF (Distributed coordination function).

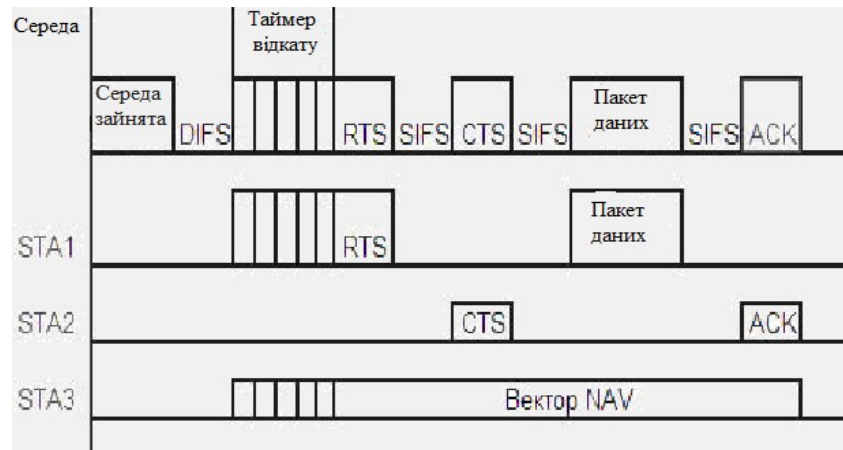


Рисунок 3.8 Часова діаграма доступу до середовища з використанням режиму передачі DCF.

Пояснення до рисунка 3.8:

Після того, як середовище звільнилося, станція STA1 чекає інтервал DIFS (DCF inter-frame space) і включає таймер відкату. Таймер відлічує випадкове число, вибране в межах вікна змагання CW (contention windows) і починає передачу. Якщо станція STA2 і STA3 згенерують випадкове число рівне числу STA1 – станції спробують одночасно почати передачу і створять колізію, в результаті якої дані всіх станцій передані не будуть.

Після того, як значення таймера стало рівним нулю, станція STA1 посилає фрейм RTS. Станція STA2, отримавши пакет від STA1, чекає інтервал SIFS (short inter-frame space) і посилає фрейм готовності CTS. Приймавши CTS, станція STA1 також чекає інтервал SIFS і починає передачу інформації. У результаті STA2 підтверджує прийом пакету даних пакетом ACK.

На рисунку, на першій лінії, видно, що відбувається в середовищі передачі – відображені всі дані, які потрапили в радіо-ефір.

На другій лінії видно, те, що передала перша станція STA1. На третій і четвертій лінії станції STA2 і STA3 відповідно. В даному випадку, станція STA1 намагається передати дані станції STA2. Для цього, вона чекає коли ефір

звільниться і почекавши інтервал DIFS (за стандартом всі станції зобов'язані почекати цей інтервал) починає боротися за право передачі (адже не тільки STA1 бажає передати дані, а передача можлива тільки по черзі). Отримавши право передачі STA1 починає процедуру, відображену на попередньому рисунку з АС отримуємо АС джерелом: спершу посилаємо пакет RTS і повідомляємо, що готова передати дані. STA2 одержувач, отримує пакет RTS і відправляє пакет CTS – повідомляє про те, що готова прийняти дані. STA1 передає дані і у відповідь отримує пакет підтвердження від STA2, який говорить, про те, що дані були успішно передані.

Між всіма кадрами присутній інтервал SIFS – маленька пауза, для того, щоб один пакет не накладався на інший.

Тепер, коли склалося уявлення про передачу даних в мережі Wi-Fi, приступаємо до чистого математичного розрахунку.

Порахуємо, який об'єм даних передається під час такої процедури і скільки часу вона займає:

-пакет готовності передачі RTS. Його довжина складає 20 байт. При бітовій швидкості 1 Мбіт/с тривалість пакету готовності передачі, з урахуванням рівня РНУ, рівна  $TRTS=(20*8+192)/1000000=352$  мкс;

-пакет готовності прийому CTS. Його довжина складає 14 байт. При бітовій швидкості 1 Мбіт/с тривалість пакету готовності прийому, з урахуванням рівня РНУ, рівна  $TACK=(14*8+192)/1000000=304$  мкс;

-пакет підтвердження АСК. Його довжина складає 14 байт. При бітовій швидкості 1 Мбіт/с тривалість пакету підтвердження, з урахуванням рівня РНУ, рівна  $TACK=(14*8+192)/1000000=304$  мкс;-Пакет даних станції, що приймає відео. Його тривалість складає 1536 байт. При бітовій швидкості 11 Мбіт/с тривалість пакету даних станції з урахуванням рівня РНУ  $TVID=192/1000000+1536*8/11000000=1309$  мкс;

-Пакет даних станції, що приймає дані. Його довжина складає 1024 байт. При бітовій швидкості 11 Мбіт/с тривалість пакету даних станції з урахуванням рівня PHY TDATA=192/1000000+1024\*8/11000000=937 мкс.

Між всіма пакетами існує проміжок SIFS, тривалість якого в стандарті 802.11b TSIFS=10мкс.

При розрахунку пропускної спроможності, вважатимемо, що дані фізичного рівня передавалися із швидкістю 2 Мбіт/с, окрім режиму роботи 1 Мбіт/с. Результати розрахунку приведені в таблиці:

Таблиця 3.4 Пропускна спроможність каналів

	DF S	Тайме р відкат у	RT S	SIF S	CT S	SIF S	Паке т дани х	SIF S	AC K	Всього	Швидкіст ь Мбіт/с
Час 1Мбіт/с. Відео, мкс	50	100	352	10	304	10	1248 0	10	304	13620	0,93
Об'єм даних 1Мбіт/с. Відео, байт	0	0	20	0	14	0	1536	0	14	1584	
Час 1Мбіт/с. Дані, мкс	50	100	352	10	304	10	8384	10	304	9524	0,9
Об'єм даних 1Мбіт/с. Дані, байт	0	0	20	0	14	0	1024	0	14	1072	
Час 2Мбіт/с. Відео, мкс	50	100	176	10	152	10	6336	10	152	6996	1,81
Об'єм даних 2Мбіт/с. Відео, байт	0	0	20	0	14	0	1536	0	14	1584	
Час 2Мбіт/с. Дані, мкс	50	100	176	10	152	10	4288	10	152	4948	1,73
Об'єм даних 2Мбіт/с. Дані, байт	0	0	20	0	14	0	1024	0	14	1072	
Час 5,5Мбіт/с. Відео,мкс	50	100	176	10	152	10	2426	10	152	3086	4,11

Продовження таблиці 3.4

Об'єм даних 5,5Мбіт/с. Відео, байт	0	0	20	0	14	0	1536	0	14	1584	4,11
Час 5,5Мбіт/с. Дані, мкс	50	100	176	10	152	10	1681	10	152	2341	3,66
Об'єм даних 5,5Мбіт/с. Дані, байт	0	0	20	0	14	0	1024	0	14	1072	
Час 11Мбіт/с. Відео, мкс	50	100	176	10	152	10	1309	10	152	1969	6,44
Об'єм даних 11Мбіт/с. Відео, байт	0	0	20	0	14	0	1536	0	14	1584	
Час 11Мбіт/с. Дані, мкс	50	100	176	10	152	10	937	10	152	1597	5,37
Об'єм даних 11Мбіт/с. Дані, байт	0	0	20	0	14	0	1024	0	14	1072	

Розділимо час на байти отримаємо пропускну спроможність мережі Wi-Fi. Як бачимо з математичного розрахунку, пропускну спроможність мережі Wi-Fi не добирається до швидкості 7 Мбіт/с при цьому, нас ніхто не обдурив – дані насправді передаються із швидкістю 11 Мбіт/с, ні більше і не менше, незалежно від того, працює поряд мікрохвильова піч чи ні.

Не дивлячись на те, що звичайне мережеве устаткування під IEEE 802.11g обіцяє пропускну спроможність 54 Мбіт/с, а устаткування класу Super G- 108 Мбіт/с, реальна швидкість передачі для одного користувача далекі від рекламних гасел. Реальна пропускну спроможність 54-мегабитної мережі складає порядка 2,8-3 Мб/с. Тобто, приблизно 23-25 Мбіт/с на один пристрій. Режим Super G дає більш ніж двократне збільшення пропускну спроможності мережі. Тепер в режимі Super G можна чекати повноцінні 54 Мбіт/с – не якійсь міфічній швидкості обслуговування декількох користувачів, а реальній швидкості між двома комп'ютерами.

Розглянемо безпроводову мережу (БЛС), що складається з  $N$  (при тестуванні  $N=10$ ) статичних однорідних станцій, що працюють в режимі високого навантаження, коли до всіх станцій БЛС завжди є непорожні черги. Статична однорідність станцій полягає в однаковому імовірнісному розподілі  $\{d_l, l = l_{\min}, l_{\max}\}$  довжин пакетів, вибраних кожною станцією з черги. Відстані між станціями БЛС малі, тому припустимо:

- 1) Відсутність прихованих станцій;
- 2) Одночасність проявів перешкод на всіх станціях.

Зазначені припущення формують модель поведінки станцій у мережі, де кожна станція веде відлік відкладеного часу лише тоді, коли канал є вільним. Значення лічильника затримки зменшується на одиницю лише за умови, що протягом усього попереднього слота канал залишався незайнятим. Коли лічильник досягає нульового значення, станція отримує дозвіл розпочати передачу.

Якщо канал стає зайнятим, відлік слотів затримки припиняється. Лічильник затримки відновлює роботу тільки тоді, коли канал знову стає вільним протягом визначеного часу: або після успішної передачі, або після невдалої, залежно від ситуації.

Розглянемо слот, який починається безпосередньо після завершення інтервалу DIFS, що слідує за успішною передачею станції А. На початку цього слота значення лічильника відкладеного часу для станції А дорівнює  $b$ , тоді як лічильники інших станцій залишаються незмінними порівняно з їхніми значеннями до початку передачі станції А. У цьому випадку слот стає неконкурентним, оскільки лише станція А може здійснити передачу, якщо її лічильник відкладеного часу  $b$  досягне нуля. Така ситуація називається миттєвим повтором передачі.

Передачі, які виконуються в результаті миттєвого повтору, називають миттєво повторюваними спробами, на відміну від звичайних спроб передачі. У цих умовах станція А може здійснити серію передач, миттєво повторюючи їх. Жодна з цих спроб не зазнає колізій, оскільки відсутня конкуренція з боку інших станцій.

Аналогічний сценарій спостерігається після завершення інтервалу EIFS, що слідує за колізією між кількома станціями. У цьому випадку лише ті станції, які брали участь у попередній колізії, можуть передавати дані, миттєво повторюючи свої спроби. Такий механізм передачі створює явище, відоме як Ефект Захоплення.

Цей ефект дозволяє станції, що ініціювала передачу, забезпечити серію безперервних передач без ризику колізій, але водночас може знижувати загальну продуктивність мережі через затримки для інших станцій.

Обмежимося обліком миттєвих повторів тільки після успішної передачі, нехтуючи такими повторами після невдалих спроб. Для цього злегка змінимо правило вибору відкладеного часу  $b$ : після успішної передачі  $b$  рівноімовірно вибирається з множини  $(0, \dots, W_0 - 1)$ , а після будь-якої невдалої спроби – з множини  $(1, \dots, \omega - 1)$ , де  $\omega$  – (конкурентне вікно) залежить від  $n_r$  – (число зроблених спроб передачі поточного пакету) і визначається (3.23).

$$w = W_i = W_0 2^{n_r} \text{ при}$$

$$w = W_m \text{ при } n \geq m \quad (3.23)$$

де, -  $w$  максимальне конкурентне вікно.

Таким чином, після невдалої спроби (включаючи інтервал EIFS) завжди слідує «порожній» слот, після закінчення якого починається конкурентний слот, коли будь-яка станція може почати передачу.

### 3.4.1 Розрахунок дальності роботи безпроводового каналу зв'язку

Формула розрахунку дальності має вигляд [14]:

$$FSL = 33 + 20(\lg F + \lg D) \quad (3.24)$$

FSL визначається сумарним посиленням системи. Вона вважається таким чином [17]:

$$Y_{\text{дБ}} = P_{t,\text{дБмВт}} + G_{t,\text{дБи}} + G_{T,\text{дБи}} - P_{\text{min},\text{дБмВт}} - L_{t,\text{дБ}} - L_{T,\text{дБ}} \quad (3.25)$$

де  $P_{t,\text{дБмВт}}$  - потужність передавача;  $G_{t,\text{дБи}}$  - коефіцієнт посилення передавальної антени;  $G_{T,\text{дБи}}$  - коефіцієнт посилення приймальної антени;  $P_{\text{min},\text{дБмВт}}$  - чутливість приймача на даній швидкості;  $L_{t,\text{дБ}}$  - втрати сигналу в кабелі і роз'ємах передавального тракту;  $L_{T,\text{дБ}}$  - втрати сигналу в кабелі і роз'ємах приймального тракту [17].

FSL обчислюється за формулою [16] :

$$FSL = Y_{\text{дБ}} - SOM \quad (3.26)$$

де SOM (System Operation Margin) — це запас в енергетиці радіозв'язку, виражений у децибелах (дБ). Цей параметр враховує вплив різних факторів, які можуть негативно позначитися на дальності та якості зв'язку, таких як завади, багатопроменевість, погодні умови чи інші несприятливі умови роботи радіосистеми.

Для інженерних розрахунків прийнято використовувати стандартне значення SOM, яке зазвичай становить 10 дБ. Це означає, що в розрахунках додається 10-децибельний запас потужності, що вважається достатнім для компенсації непередбачуваних втрат і забезпечення стабільного зв'язку в більшості умов.

Цей запас дозволяє забезпечити надійну роботу системи навіть у випадках, коли радіосигнал зазнає значних втрат через відбиття, поглинання чи дифракцію. Використання SOM як частини інженерного проектування гарантує, що система буде функціонувати відповідно до вимог навіть у складних умовах експлуатації.

$$P_{t,\text{дБмВт}}=16; G_{t,\text{дБ}}=4; G_{T,\text{дБ}}=2; P_{\text{min},\text{дБмВт}}=66.$$

$$\text{FSL}=88-10=78\text{дБ}$$

$$D = 10^{\left(\frac{\text{FSL}}{20} - \frac{33}{20} - \lg F\right)}$$

$$D \approx 40\text{м.}$$

### ***Висновок по розділу***

Проведені розрахунки пропускної спроможності мережі показали, що реальні результати часто відрізняються від заявлених виробниками характеристик безпроводового обладнання. Ця різниця обумовлена накладними витратами, впливом радіозавад, колізіями та іншими факторами, які впливають на ефективність роботи мережі в реальних умовах.

Однак використання покращеного протоколу 802.11g, відомого як **Super G**, дозволяє значно підвищити продуктивність мережі. Ця технологія забезпечує достатньо високі показники пропускної здатності, які відповідають потребам надання масового доступу до Інтернету, особливо в умовах середніх та невеликих навантажень.

Таким чином, хоча реальна пропускна здатність мережі може бути нижчою за теоретичні значення, впровадження сучасних оптимізованих протоколів і правильне налаштування обладнання дозволяють забезпечити стабільну та ефективну роботу безпроводової мережі.

## **ВИСНОВКИ**

Проведений аналіз стандартів безпроводових мереж, зокрема IEEE 802.11a/b/g, показав, що їхня архітектура базується на інтеграції фізичного та канального рівнів моделі OSI. Це забезпечує не лише сумісність із провідними мережами, але й підтримку високоефективної пакетної передачі даних, яка є ключовою для сучасних телекомунікаційних систем. Зокрема, стандарт 802.11g демонструє суттєве підвищення продуктивності в порівнянні з попередніми стандартами, такими як 802.11b, завдяки вдосконаленим методам модуляції. Технологія Super G, яка базується на розширенні можливостей 802.11g, дозволяє значно збільшити пропускну здатність мережі, зберігаючи при цьому сумісність і стабільність роботи навіть у складних умовах.

Запропонована архітектура мережі, яка передбачає розташування точок доступу на 2-му, 5-му та 8-му поверхах багатоповерхової будівлі, довела свою ефективність у забезпеченні стабільного покриття та високоякісного зв'язку для всіх користувачів. Використання кабельної інфраструктури категорії 5e у горизонтальних підсистемах не лише відповідає сучасним вимогам до підтримки протоколів, таких як Gigabit Ethernet, але й створює резерв пропускну здатності для майбутніх удосконалень і масштабування мережі. Такий підхід гарантує гнучкість і адаптивність мережі до зростаючих потреб користувачів.

Моделювання роботи мережі за умов високого навантаження дозволило виявити ключові проблеми, що впливають на її продуктивність, зокрема радіозавади, колізії під час передачі даних та значні накладні витрати. Реальна пропускну здатність для стандарту 802.11g становить близько 25 Мбіт/с, що вдвічі менше від заявленого теоретичного максимуму 54 Мбіт/с. Втім, застосування оптимізацій, таких як RTS/CTS-обмін, дозволяє значно зменшити ймовірність колізій, особливо у змішаних мережах, де одночасно працюють пристрої стандартів 802.11b та 802.11g.

Розроблений проєкт мережі враховує економічні, технічні та безпекові аспекти. Використання сучасного обладнання D-Link із підтримкою технології Super G забезпечує стабільність роботи мережі та високі показники пропускну здатності навіть за умов значного навантаження. Особливий акцент зроблено на впровадженні енергоефективних режимів роботи пристроїв, що дозволяє знизити витрати енергії без шкоди для продуктивності та якості зв'язку.

Для успішного впровадження розробленої мережі рекомендовано використовувати точки доступу, які підтримують сучасні протоколи безпеки, такі як WPA2. Це дозволить значно підвищити захист даних і мінімізувати ризики несанкціонованого доступу. Важливими складовими експлуатації мережі є належне технічне обслуговування та резервування мережевого обладнання, що забезпечить безперервну роботу мережі й мінімізує простой. Запропоновані рішення є технічно обґрунтованими, економічно доцільними та відповідають вимогам до надійності, швидкості передачі даних і безпеки в сучасних мережах.

## ПЕРЕЛІК ПОСИЛАНЬ

1. Бутко П.М., Сидоренко В.П. *Безпроводні технології передачі даних: основи та застосування*. Київ: Політехніка, 2018.
2. Драчук В.В., Бойко О.М. *Основи комп'ютерних мереж та телекомунікацій*. Київ: Кондор, 2017.
3. Жуковський А.В. *Мережі та мережеві технології: навчальний посібник*. Харків: ХНУРЕ, 2015.
4. Іванов С.О., Коваленко М.В. *Технології побудови бездротових мереж*. Львів: Львівська політехніка, 2019.
5. Крамаренко О.П. *Архітектура комп'ютерних систем і мереж*. Київ: Видавництво Київського університету, 2016.
6. Мироненко В.І. *Основи проектування локальних мереж передачі даних*. Одеса: Одеська національна академія зв'язку, 2018.
7. Ніконов Д.А., Сухомлин О.М. *Безпека даних у бездротових мережах*. Київ: Видавництво НТУУ "КПІ", 2020.
8. Петриченко С.В. *Інженерія локальних мереж: підручник*. Харків: Видавництво ХПІ, 2017.
9. Савченко І.П. *Моделювання систем і мереж*. Київ: Академія, 2019.
10. Сидоренко О.М. *Телекомунікаційні системи та мережі: практикум*. Київ: Видавництво НАУ, 2021.
11. Шевченко О.В. *Протоколи мережевих технологій: теорія та практика*. Київ: Видавництво Київського університету, 2018.
12. William A. Arbaugh, Jonathan M. Smith. *"An In-Depth Analysis of the IEEE 802.11 Protocols."* IEEE Communications Surveys & Tutorials, 2003.
13. William Stallings. *"Wireless Communications & Networks."* Pearson, 2002.  
Link
14. Andrew S. Tanenbaum, David J. Wetherall. *"Computer Networks."* 5th Edition, Pearson, 2010. Link

14. Behrouz A. Forouzan. *"Data Communications and Networking."* 5th Edition, McGraw-Hill, 2012. Link
15. Charlie Kaufman, Radia Perlman, Mike Speciner. *"Network Security: Private Communication in a Public World."* 2nd Edition, Prentice Hall, 2002. Link
16. Bruce Schneier. *"Applied Cryptography: Protocols, Algorithms, and Source Code in C."* 2nd Edition, Wiley, 1996.
17. Douglas E. Comer. *"Internetworking with TCP/IP Volume One: Principles, Protocols, and Architecture."* 6th Edition, Pearson, 2013. Link
18. James F. Kurose, Keith W. Ross. *"Computer Networking: A Top-Down Approach."* 7th Edition, Pearson, 2016. Link
19. Richard Stevens, Kevin R. Fall. *"TCP/IP Illustrated, Volume 1: The Protocols."* 2nd Edition, Addison-Wesley, 2011. Link
20. Michael T. Goodrich, Roberto Tamassia. *"Introduction to Computer Security."* Pearson, 2010
21. Stallings, William. *Wireless Communications and Networks.* Pearson, 2002. P.656.
22. Gast, Matthew S. *802.11 Wireless Networks: The Definitive Guide.* O'Reilly Media, 2005. P.700.
23. Geier, Jim. *Wireless Networking Handbook.* New Riders, 2001. P.380.
24. Bensky, Alan. *Wireless Networking: Introduction to Bluetooth and Wi-Fi.* CRC Press, 2004. P.420.
25. Held, Gilbert. *Deploying Secure 802.11 Wireless Networks with Microsoft Windows.* Wiley, 2003. P.350.
26. Wright, Joshua. *Kismet Hacking: Optimizing Home Wireless Networks.* Syngress, 2007. P.280.
27. Odom, Wendell. *CCNA Wireless Official Exam Certification Guide.* Cisco Press, 2008. P.720.
28. Pahlavan, Kaveh, and Krishnamurthy, Prashant. *Principles of Wireless Networks: A Unified Approach.* Prentice Hall, 2001. P.600.

29. Hashemi, H., & Thibault, L. "Indoor propagation measurements at 946 MHz and 1920 MHz." *IEEE Transactions on Vehicular Technology*, (1994). 43(3), 550–557.

30. Obayashi, S., & Taga, T. "Propagation characteristics in indoor wireless communication environments." *IEEE Transactions on Antennas and Propagation*, (1990). 38(8), 1199–1206.

## ДОДАТКИ

## **Додаток А**

Розділ, котрий виконано англійською мовою

### ***1. ANALYSIS OF THE PRINCIPLES OF BUILDING WI-FI ACCESS NETWORKS.***

#### ***1.1. The main elements of the network***

The IEEE 802.11 standard, like all IEEE 802 standards, covers the two lower layers of the OSI model: the physical layer and the Data Link Layer. The data link layer, in turn, is divided into two sublayers. The upper sublayer, known as Logical Link Control (LLC), is described in the IEEE 802.2 standard. The lower sublayer, Medium Access Control (MAC), is responsible for controlling access to the data transmission medium.

The physical layer defines how devices interact with the transmission medium, as well as the speed and methods of signal modulation. The MAC layer standardises the rules for accessing a common channel, how devices connect to access points, and the mechanisms for authentication and data protection.

The IEEE 802.11 standard was created as ‘wireless Ethernet’ and uses packet transmission with 48-bit addresses, similar to Ethernet networks. Considerable attention has been paid to ensuring that all IEEE 802 standards are compatible, allowing wired and wireless networks in this family to easily interoperate with each other.

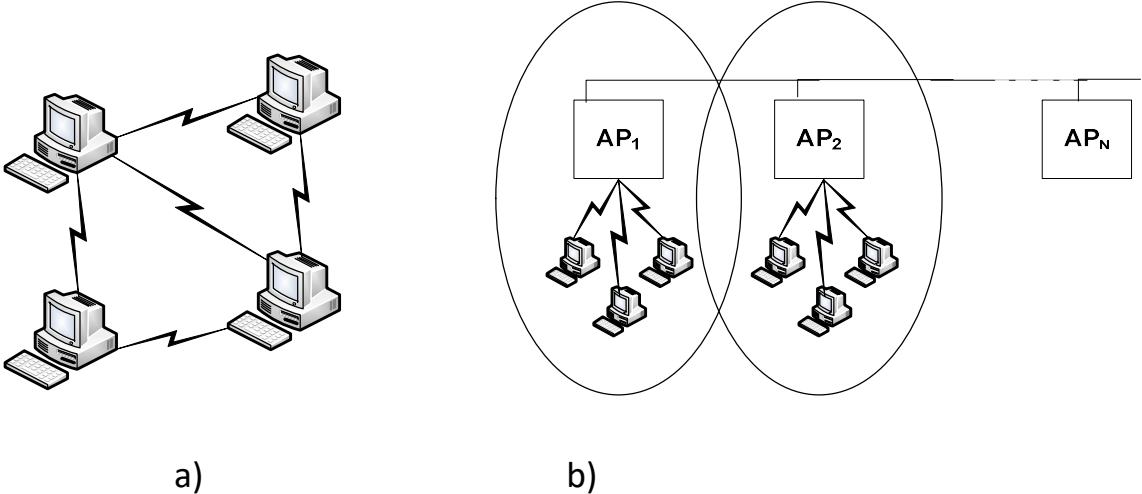
#### ***1.2. IEEE 802.11 architecture***

The IEEE 802.11 standard provides for two main approaches to organising local area networks. The first is based on the principle of ‘peer-to-peer’ (ad-hoc network) and provides a direct connection between two stations without the need for centralised administration. The second approach is implemented in the form of structured networks, which are the main way to build IEEE 802.11 networks in practice. In such networks, an Access Point (AP) is a mandatory element, which is a stationary device tuned to a fixed channel. Communication between client devices is carried out exclusively through APs, which also provide access to external wired networks such as Ethernet.

Structured networks can include multiple access points interconnected by a wired network, creating a set of base stations with overlapping coverage areas. The standard supports roaming, which allows devices to move between the coverage areas of different access points without losing their connection, thereby ensuring user mobility. An important component is a special power management protocol that allows the transmitting device to put the receiver into standby mode during inactivity, which is critical for mobile stations with limited power resources.

Network management is typically performed in a Distributed Coordination Function (DCF) mode, where coordination functions are distributed among all devices in the network. However, for structured networks, it is possible to use the Point Coordination Function (PCF) mode, in which control is transferred to one of the access points. This mode is used to transmit delay-sensitive data, such as streaming video.

Most IEEE 802.11 networks use competitive access to the channel without prioritisation, but with the introduction of the IEEE 802.11e standard, it is expected that distributed control with prioritisation for critical traffic will be possible. It is important to note that the PCF mode operates only during certain predefined time intervals that are repeated periodically.



Picture 1.1 802.11 network architecture: a) - ad-hoc network, b) - structured networks

One of the main requirements for wireless communication standards is to ensure the security of data transmission. A security mechanism is implemented at the medium access control (MAC) layer, which includes device authentication and information encryption procedures. This mechanism was developed to provide a level of protection comparable to conventional wired Ethernet networks and is called WEP (Wired Equivalent Privacy).

WEP is based on the use of four 40-bit secret keys shared by the network. The RC4 algorithm developed by RSA Security is used to encrypt data. This algorithm works by multiplying blocks of source data into a pseudorandom sequence whose length corresponds to the size of the data block to be encrypted. The pseudorandom sequence is generated using a 64-bit number that includes a 24-bit Initialisation Vector (IV) and a 40-bit secret key.

The peculiarity of this approach is that the Initialisation Vector (IV) changes with each packet, even if the secret key remains constant. This reduces the risk of data compromise. For additional protection, each encrypted packet is accompanied by a 32-bit Integrity Check Value (ICV), which ensures that changes in the transmitted data are detected. As a result, 8 bytes of service information are added to each packet: 4 bytes for ICV, 3 bytes for IV, and 1 byte to identify the key used.

It is worth noting that although the standard allows the use of longer keys (e.g. 64 or 128 bits), US legal restrictions on the export of devices with a key length of more than 40 bits force manufacturers to adhere to this limit. Thus, WEP-enabled devices are typically limited to 240 key variants.

### ***1.3. Standards of the 802.11 protocol***

The IEEE 802.11.a standard was introduced almost simultaneously with the IEEE 802.11b standard in September 1999. Its specification is focused on operation in the 5 GHz frequency range and is based on a fundamentally different data coding mechanism - frequency division multiplexing using orthogonal carriers (OFDM). In this standard,

each frame is transmitted using 52 orthogonal carriers, each with a bandwidth of approximately 300 kHz (20 MHz/64). The channel width in the standard is 20 MHz. The carriers are modulated using BPSK, QPSK, and 16- and 64-level quadrature amplitude modulation (QAM). Depending on the type of modulation and coding rate (1/2, 3/4, for 64-QAM - 2/3 and 3/4), data rates are available: 6, 9, 12, 18, 24, 36, 48 and 54 Mbit/s.

Of the 52 orthogonal carriers, 48 are used to transmit information symbols, and the remaining 4 perform service functions. Although the structure of the physical layer headers of the IEEE 802.11.a standard is slightly different from the IEEE 802.11.b standard, these differences are not significant (Picture 1.2). The frame consists of a preamble (12 synchronisation characters), a physical layer header (PLCP header) and an information field generated at the MAC layer. The header contains information about the coding rate, modulation type and frame length. The preamble and header are transmitted at the lowest possible rate (BPSK, coding rate  $r = 1/2$ ), while the information field is transmitted at the maximum rate specified in the header, depending on the transmission conditions.

OFDM symbols are transmitted every 4  $\mu\text{s}$ , of which 3.2  $\mu\text{s}$  is the symbol duration and 0.8  $\mu\text{s}$  is the guard interval. This interval provides resistance to multipath propagation, as a reflected signal that is received with a delay falls into the guard interval and does not affect the next symbol.

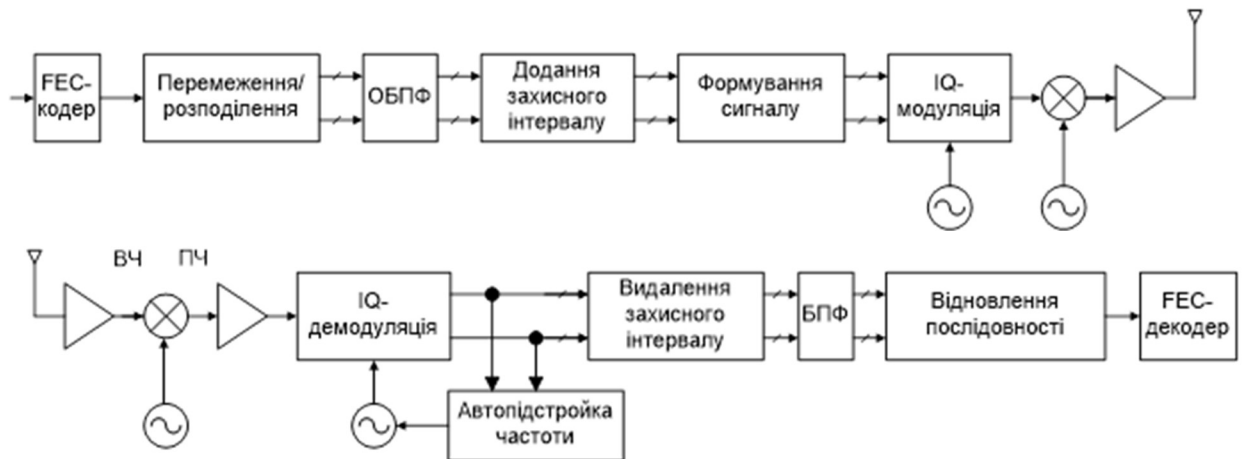


Picture 1.2 Structure of the physical layer header of the IEEE 802.11.a standard

The process of generating and decoding OFDM symbols is implemented using a fast Fourier transform (forward or inverse, FFT/OBFT). The typical scheme of the receiving and transmitting paths (Picture 1.3) is standard for this method and includes

components such as a convolutional encoder, an interleaving mechanism (redistribution) to protect against packet errors, and an FFT processor.

The Fourier processor combines the signal into a single sequence, adds a protective interval to the symbol, and then generates an OFDM symbol, which is transferred to the required frequency range using a quadrature modulator/converter. When receiving a signal, all operations are performed in the reverse order.



Picture 1.3 Functional diagram of the IEEE 802.11a transmit/receive paths

The IEEE 802.11g standard essentially adapts the OFDM modulation mechanism successfully used in the 802.11a standard to operate in the 2.4 GHz band while maintaining compatibility with 802.11b devices. This adaptation was made possible by the similarity of the channel widths in the 2.4 and 5 GHz bands, which are 22 MHz at power levels of -30 dB and -20 dB, respectively. In the 5 GHz band, the 802.11a standard allows a spectral bandwidth of up to 40 MHz at -28 dB.

One of the main requirements for the 802.11g specification was to ensure backward compatibility with 802.11b devices. This caused a dispute between Intersil and TI. In the 802.11b standard, the main modulation technology is CCK (Complementary Code Keying), and PBSS is additionally supported. The developers of the 802.11g standard decided to keep the CCK modulation for speeds up to 11 Mbit/s and use OFDM for higher speeds.

Despite this, 802.11 networks operate on the basis of the CSMA/CA principle (carrier sense multiple access and collision avoidance). This means that devices must make sure that there is no active traffic before they can transmit.

If 802.11b and 802.11g devices are in range, the latter use OFDM, which may not be understood by 802.11b devices. In such cases, 802.11b devices may try to start transmitting, creating conflicts.

To avoid such situations, the 802.11g standard provides a mixed CCK-OFDM mode. In this mode, frames are transmitted in two parts: the preamble and header are encoded using the CCK method, and the information field is encoded using the OFDM method. This allows 802.11b devices to recognise the frame headers and refrain from transmitting when 802.11g traffic is being transmitted. However, this approach reduces network throughput because the preamble and header are transmitted at a rate of only 1 Mbps.

To eliminate the limitations associated with the use of CCK technology, the 802.11g standard provides an optional PBSS mode, as in 802.11b. In this mode, the header and preamble are transmitted in the same way as with CCK, and the information field is modulated by PBSS at 22 or 33 Mbit/s. This ensures that 802.11g devices remain compatible with all 802.11b versions, minimising the risk of conflicts. Supported rates for different types of modulation are listed in Table 1.1, and the dependence of the transmission rate on the modulation method is shown in Picture 1.4.

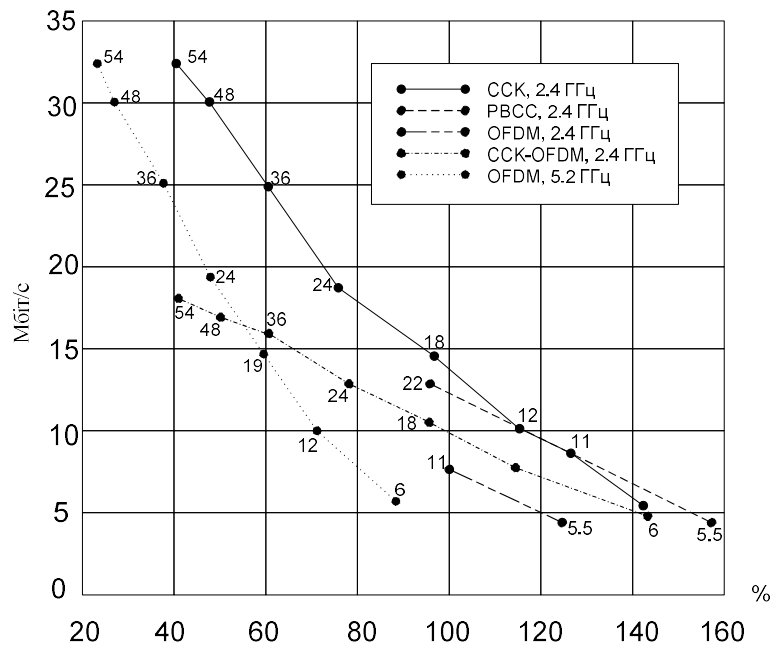
Table 1.1. Possible modulation rates and types in the IEEE 802.11.g specification

Speed, Mbps	Modulation type	
	Necessarily	For example
1	2	3
1	Barker's sequence	
2	Barker's sequence	

5,5	CCK	PBCC
-----	-----	------

Continuation of Table 1.1

1	2	3
6	OFDM	CCK-OFDM
9		OFDM, CCK-OFDM
11	CCK	PBCC
12	OFDM	CCK-OFDM
18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM



Picture 1.4 Dependence of transmission rate on distance for different transmission technologies. The distance is given in percentage, 100% is the transmission distance with SCM modulation at 11Mbps.

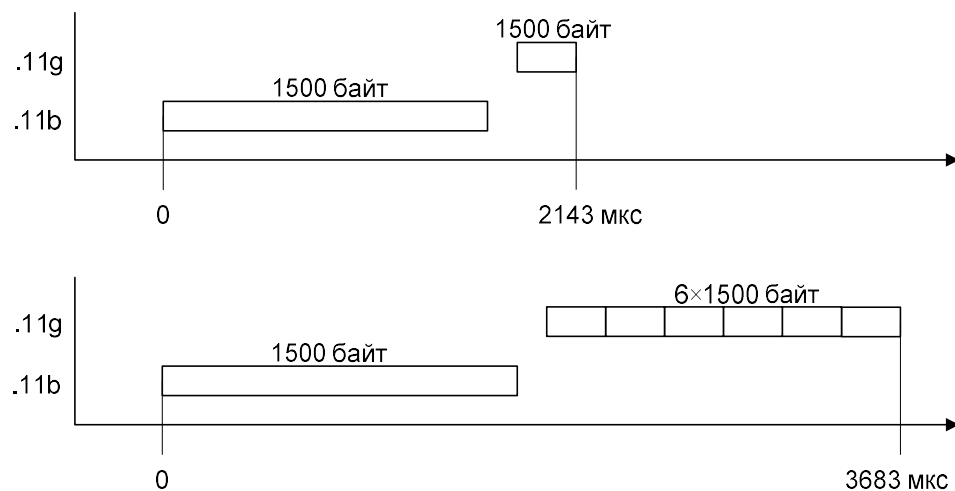
Obviously, IEEE 802.11g devices will have to operate in joint networks with equipment that supports only the 802.11b standard for a long time to come. It is worth noting that most manufacturers will be reluctant to implement CCK-OFDM and PBSS modes, as they are not mandatory, and the cost of devices often determines the final price. One of the key objectives of the new standard was to ensure conflict-free operation of mixed 802.11b/g networks.

The basic principle of 802.11 networks is the concept of 'listen before you transmit'. However, 802.11b devices are unable to recognise traffic created by 802.11g equipment operating in OFDM mode. This creates a situation similar to the 'hidden station' problem: when two devices that are not in range of each other try to transmit data to a third station, creating a conflict. To avoid such situations, the 802.11 standard introduced a protection mechanism based on RTS/CTS frames ('request to transmit' and 'acknowledgement of transmission'). This mechanism also works in mixed 802.11b/g networks, allowing devices to avoid simultaneous transmission. In this case, RTS/CTS frames are transmitted using CCK modulation, which is understood by all devices.

However, the protection mechanism significantly reduces network throughput. For example, in 802.11g networks with a physical speed of 54 Mbit/s, the actual throughput due to overheads is about 32 Mbit/s, and for devices with conventional equipment, it is about 24 Mbit/s. In mixed networks using RTS/CTS, this figure drops to 12 Mbps, which is almost twice the throughput of 802.11b networks (~6 Mbps), but still below expectations. As an alternative, only CTS frames can be used, which are transmitted before each OFDM frame, which can increase the throughput to 14.5 Mbps. However, this approach has limitations if not all devices in the network are in line of sight.

To solve this problem, manufacturers have begun to introduce their own technologies to increase speeds within existing standards. For example, Atheros has developed Turbo Mode, which doubles the transmission speed to 108 Mbit/s using two channels simultaneously. For this purpose, the company created the AR5001X+ chipset, equipped with an upgraded AR5212 processor.

Intersil Corporation took a different approach with its PRISM Nitro technology. This technology includes two main elements: a security mechanism and a method of group transmission of OFDM frames. The protection mechanism, similar to RTS/CTS, involves the transmission of a CTS frame before each OFDM frame. At the same time, group transmission can significantly increase throughput in both mixed and homogeneous networks. For example, in mixed networks, each device is offered an equal time slot for transmission. A CCK frame transmitted at 11 Mbit/s takes approximately the same amount of time as six OFDM frames transmitted at 54 Mbit/s, including all overhead. As such, 802.11b and 802.11g devices can efficiently distribute transmission time to minimise bandwidth loss. For example, for two devices with an information field size of 1500 bytes, the transmission can take 2143  $\mu$ s (Picture 1.5).

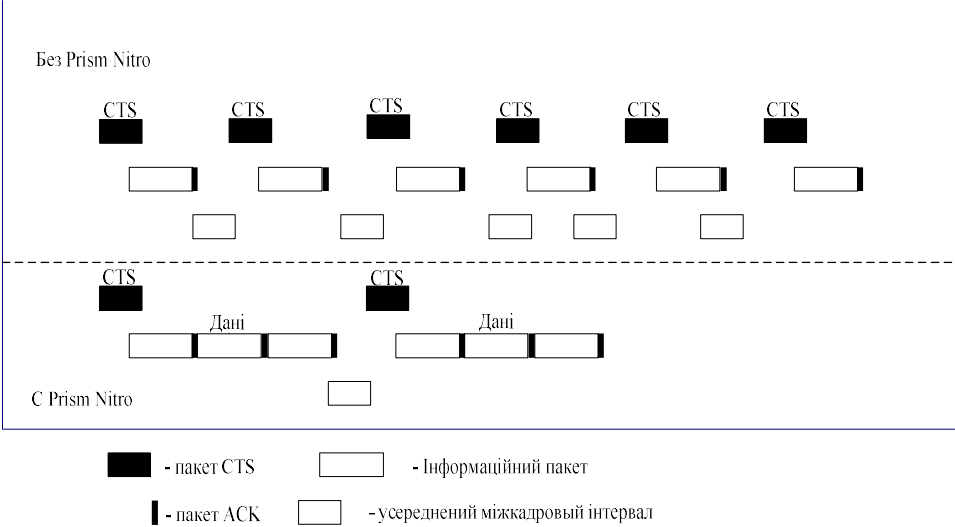


Picture 1.5 Group transmission of OFDM packets using PRISM Nitro technology in a mixed network.

When used on a homogeneous 802.11g network, packet grouping also provides significant efficiency gains. This is achieved because within a packet group there is no need to transmit CTS frames or wait for interframe intervals between individual transmissions. All overheads are reduced to transmitting only a short ACK frame, which significantly reduces network downtime (Picture 1.6.).

This approach can significantly increase network throughput, especially under high load conditions, providing greater efficiency in the use of the data channel. Thus, group

packet transmission is becoming an important element in optimising the performance of 802.11g networks, both for mixed and homogeneous environments.



Picture 1.6 Group transmission of OFDM packets using PRISM Nitro technology in a homogeneous network.

The PRISM Nitro technology was implemented at the system software level and was designed to integrate with the PRISM Duette and PRISM GT chipsets. Its developers claim that this technology fully complies with the requirements of the IEEE 802.11g standard, providing high efficiency and performance in wireless networks. PRISM Nitro has already been used in a number of modern devices, including the CONNECT2AIR router and network cards from Fujitsu Siemens Computers.

It is noteworthy that Fujitsu Siemens Computers was the first to introduce the latest ISL3893 processor developed by Intersil for access points and wireless routers. This processor is based on the ARM9 microprocessor core, which allows it to function as both a network processor for wireless networks and a processor for Ethernet networks. This versatility enables efficient integration of wired and wireless network components.

The ISL3893 processor is specifically optimised for use with the PRISM GT and PRISM Duette chipsets, making it an ideal solution for high-performance wireless networks. Its architecture provides high data processing speeds, stable connections and support for modern requirements for telecommunications equipment.

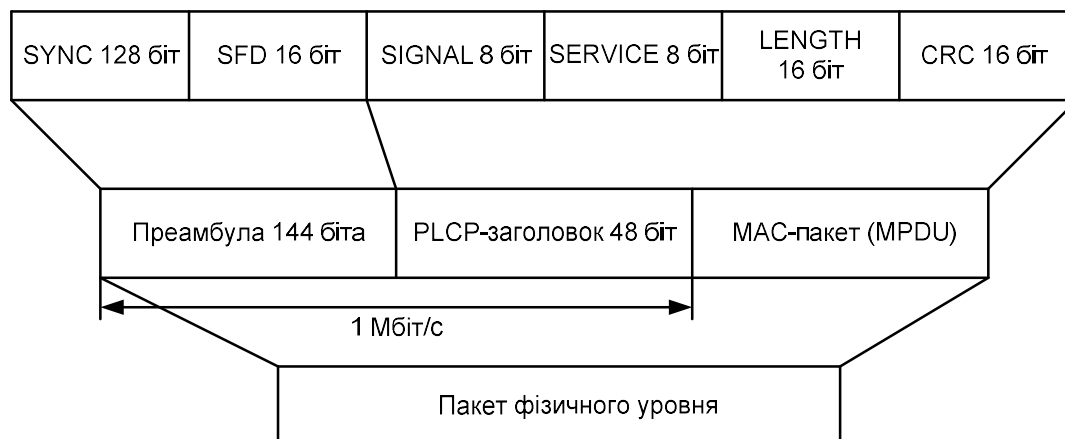
#### ***1.4. Physical layer of the IEEE 802.11.b standard***

At the physical layer, the MAC frames (MPDUs) are preceded by a physical layer header consisting of a preamble and a PLCP header (see Picture 1.7). The preamble includes the start synchronisation sequence (SYNC), which is used to configure the receiver, and the 16-bit start frame data (SFD), which is set to F3A016. The PLCP header contains several key fields: SIGNAL (contains information about the transmission rate and modulation type), SERVICE (contains additional data, such as the use of high-speed extensions or PBSS modulation) and LENGTH (defines the time in microseconds required to transmit the rest of the frame after the header). All three of these PLCP header fields are protected by a 16-bit CRC checksum, which guarantees the integrity of the transmitted data.

The IEEE 802.11b standard provides two types of physical layer headers: long and short (Picture 1.8). The main differences between them are in the length of the synchronous sequence (128 bits for long and 56 bits for short), the methods of generating these sequences, and the order in which the start of the frame is transmitted. In a short header, the start character is transmitted in the reverse order.

Another important difference is the data rate of the headers. For a long header, all fields are transmitted at 1 Mbps. In the case of a short header, the preamble is also transmitted at 1 Mbps, but the rest of the header fields are transmitted at 2 Mbps. The main part of the frame can be transmitted at any of the speeds allowed by the standard, which are defined in the SIGNAL and SERVICE fields.

The introduction of short headers in the IEEE 802.11b standard was aimed at increasing network throughput. This allows to reduce the overheads for frame processing and, accordingly, to increase the efficiency of using the available radio channel, especially in conditions of high load.



Picture 1.7 Structure of 802.11 MAC layer network frames

From the description of the IEEE 802.11 network communication procedures, it is clear that the ‘overhead’ in this standard is higher than in a wired Ethernet network. Therefore, it is crucial to ensure a high data rate in the channel. It is possible to increase the bandwidth of a channel with a given frequency bandwidth by developing and applying more advanced modulation methods. This is the path taken by the IEEE 802.11.b development group. Recall that initially, the IEEE 802.11 standard provided for operation in DSSS mode using the so-called Barker sequence (Barker) with a length of 11 bits:  $B_i = (10110111000)$ . Each information bit is replaced by its product modulo 2 (the ‘exclusive OR’ operation) with this sequence, i.e. each information unit is replaced by  $B_i$ , each zero is replaced by the inversion of  $B_i$ . As a result, the bit is replaced by a sequence of 11 chips. The signal is then encoded using differential two- or four-position phase-shift keying (DBPSK or DQPSK, one or two chips per symbol, respectively). With a carrier modulation frequency of 11 MHz, the total speed is 1 and 2 Mbit/s, depending on the type of modulation.



Picture 1.8 Short header of 802.11.b network frames

The IEEE 802.11b standard additionally provides the ability to transmit data at 11 and 5.5 Mbit/s. To achieve these speeds, a modulation method known as CCK (Complementary Code Keying) is used. This approach is based on the scientific

developments of Intersil (formerly Harris Semiconductor) and Agere Systems, which were part of Lucent Technologies. In this method, DQPSK modulation is used for data transmission in the radio path, and the SCM modulation itself is performed by dividing the incoming data stream into groups of 8 bits (d0-d7).

These eight bits form an information symbol consisting of eight complex chips  $Z = [z_0, \dots, z_7]$ , each of which defines the I- and Q-quadrature components of the signal for DQPSK. Modulation is carried out using an 11 MHz carrier frequency. Each chip in the symbol is a carrier frequency signal with a phase shift calculated for the entire symbol according to the formula:

$$Z[c_0, \dots, c_7] = [j_1 + j_2 + j_3 + j_4; j_1 + j_3 + j_4; j_1 + j_2 + j_4; -(j_1 + j_4); j_1 + j_2 + j_3; j_1 + j_3; -(j_1 + j_2); j_1]$$

The value of the  $j_1$  element is present in each character chip, affecting the phase of the entire character. Phase modulation is differential, as the  $j_1$  value of the current symbol is calculated based on the  $j_1$  value of the previous symbol. The phase shift  $j_1$  is defined by the formula  $\Delta j_1 = (d_0 d_1)\pi/2$  for even symbols, where (d0d1) is a two-bit binary number in the range from 0 to 3. For odd symbols, an additional shift of  $\pi$  is added to  $j_1$ .

In the IEEE 802.11b standard, CSC modulation is applied only to MAC frames. The first CSC character that appears after the physical layer header has the number '0', i.e. it is considered even. The phase of the last symbol of the QPSK modulated frame header is used as a reference for determining the initial value  $j_1$  of the first symbol of the information field, to which the phase shift  $\Delta j_1$  is added. The other three symbol parameters are determined by the formulas:

$$j_2 = (d_2 d_3)\pi/2; j_3 = (d_4 d_5)\pi/2; j_4 = (d_6 d_7)\pi/2, \quad (1.1)$$

where (d<sub>x</sub>d<sub>x+1</sub>) are two-bit binary numbers.

For transmission at 5.5 Mbit/s, DBPSK modulation is used. In this case, the CCS symbol is encoded with four data bits (d0-d3), which results in a halving of the speed

compared to 11 Mbps. In this case,  $j_1$  is calculated using the same formula, while the other parameters are defined as follows:  $j_2 = d_2\pi/2$ ;  $j_3 = 0$ ;  $j_4 = d_3\pi$ .

The main advantage of CSC modulation is its efficiency. As the formula shows, the symbol chips are determined based on Walsh-Adamar sequences, which provide good correlation properties. For 11 Mbit/s, the input data vector  $D = [d_0, \dots, d_7]$  can be represented as a sequence of quadratic numbers  $m_1 - m_4$ , where  $m_1 = (d_0d_1)$ ,  $m_2 = (d_2d_3)$ , ...,  $m_4 = (d_6d_7)$ . Then the vector  $Z$  is calculated as:

$$Z = (M \times (WH + B))\pi/2, \quad (1.2)$$

where  $WH$  is the upper half of the Walsh-Adamar matrix, and  $B$  is the vector that provides phase shift correction.

$$\{WH\} = \begin{matrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{matrix}$$

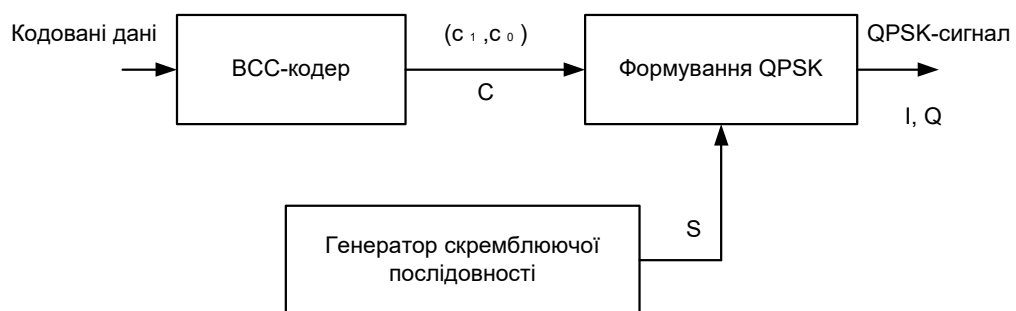
The vector  $B = [0, 0, 0, 2, 0, 0, 2, 0]$ , which physically corresponds to a  $180^\circ$  phase shift of the  $c_3$  and  $c_6$  chips (change of sign to “minus” in formula (1.1)), plays an important role in improving the correlation properties of code sequences. Walsh-Adamar sequences, on the basis of which this approach works, are well studied and have excellent autocorrelation characteristics. Their important feature is the low level of self-correlation even under the condition of phase shift, which makes them effective for combating re-reflected signals in radio paths.

The theoretical operational gain of the SSC modulation is 3 dB (which corresponds to a doubling of the signal power). This is due to the fact that without the use of QPSK coding, an 11 MHz signal can transmit data at a rate of 22 Mbps. Due to its simplicity, the CSC modulation is considered as a block code, which ensures its ease of hardware

implementation. It is this set of properties that has made SSC modulation a mandatory coding method in the IEEE 802.11b standard.

In practice, however, not only the theoretical gain is important. The uniformity of symbol distribution in the phase space also plays a key role: the greater the distance between symbols, the lower the probability of errors during their detection. In this aspect, the SSC modulation has certain disadvantages. Its actual operational gain is usually less than 2 dB, which is inferior to the theoretical value. Due to these limitations, alternative approaches were initially considered.

One such approach was Packet Binary Convolutional Coding (PBCC). This technology was proposed by specialists from Alantro Communications, which became part of Texas Instruments in 2000. PBCC was included in the IEEE 802.11b standard as an additional (optional) modulation method. Its implementation made it possible to achieve throughput in IEEE 802.11b networks at the level of 5.5, 11 and 22 Mbps (Picture 1.9), expanding the possibilities of using this standard.



Picture 1.9 General scheme of PBSS-modulation

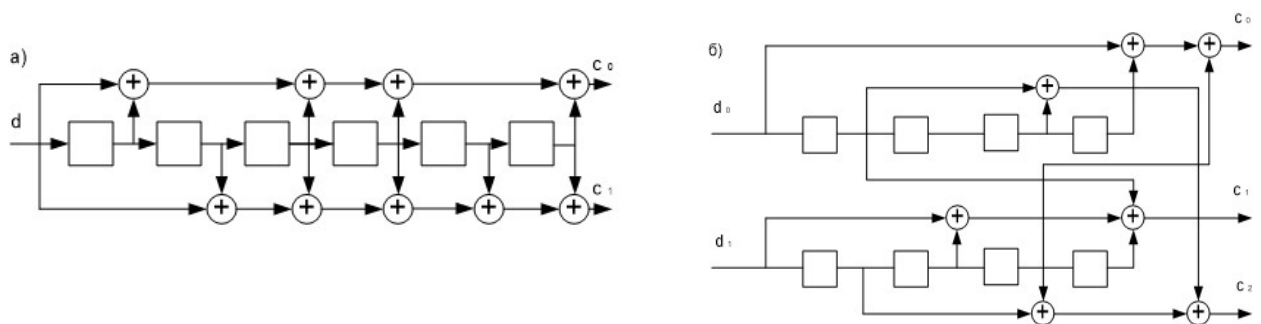
As the name implies, the Packet Binary Convolutional Coding (PBCC) method is based on the principle of convolutional coding. For transmission speeds of 5.5 and 11 Mbps, the information bit stream is processed using a six-bit shift register equipped with adders (Picture 1.10.a). At the initial stage of operation, all register triggers are initialized with zeros. As a result, each input bit of information  $d$  is replaced by two bits of the code sequence  $c_0$  and  $c_1$ .

At a transmission rate of 11 Mbit/s, the  $c_0$  and  $c_1$  bits form a single symbol corresponding to four-position QPSK modulation. At 5.5 Mbit/s, two-position BPSK

modulation is used, which transmits the  $c_0$  and  $c_1$  bits sequentially. If you need to achieve a speed of 22 Mbps, the coding scheme becomes more complex (Picture 1.10.b): in this case, the three coding bits  $c_0$ ,  $c_1$ , and  $c_2$  define one symbol in eight-position PSK modulation.

After the PSK symbols are generated, the scrambling process is performed. This changes the sequence of bits to ensure the uniformity of the statistical distribution of the signal. Depending on the value of the signal  $s$  (see Picture 1.9), the symbol remains unchanged ( $s = 0$ ) or its phase is increased by  $\pi/2$  ( $s = 1$ ). The value of  $s$  is determined by the 256-bit cyclically repeating sequence  $S$ , which is formed on the basis of the initial vector  $U = 338B16$ .

This initial vector has an equal number of zeros and ones, which contributes to the optimal distribution of phase shifts. The sequence  $S$  is generated in the form of 16 vectors  $U_i$  (where  $i = 0 \dots 15$ ), and each vector  $U_i$  is a cyclic shift of the previous  $U_{i-1}$  by several bits. This approach makes the signal more resistant to radio interference and ensures stable data transmission even in difficult conditions [1].



Picture 1.10 Scheme of reverse BCC coding: a - for speeds of 5.5 and 11 Mbps; b - for speed of 22 Mbps

The six-bit shift register used in RVSS for 11 and 5.5 Mbit/s speeds has 64 possible output states. Thus, with RVSS modulation, the information bits in the phase space are much further apart than with SSC modulation. That is why RVSS allows to transmit at a higher rate than in the case of SCC with the same signal-to-noise ratio and error rate.

### ***Conclusion on the section***

Wi-Fi technology is extremely flexible and offers a wide range of modes for organizing and deploying networks. Despite the fact that one of the main drawbacks of this technology is still low security and insufficient data protection, the IEEE 802.11 standard is becoming increasingly popular in crowded places such as cafes, airports, and restaurants. However, its use for organizing mass Internet access in residential buildings is still rare.

Two key factors contribute to this. First, many users still do not have a clear understanding of the benefits of Wi-Fi technology and how to use it effectively in the home. Secondly, the lack of infrastructure to provide high-quality connectivity in residential areas limits the spread of this technology.

To overcome these problems, it is necessary to focus on several areas. In particular, it is important to actively promote the benefits of Wi-Fi to a wide audience, which will help raise awareness of the technology's capabilities. Investing in infrastructure development is also important, as it will create a solid foundation for large-scale Wi-Fi deployment in residential buildings. Only a comprehensive approach will help to significantly expand the use of this technology and ensure its effective use in various fields.

## **Додаток В**

Тези

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**  
**«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ**  
за матеріалами X Всеукраїнської науково-практичної конференції  
**«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:**  
**ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»**  
20 грудня 2024 року



**Полтава 2024**

<b><i>I. Silin, V. Lysechko</i></b> MODELS FOR DESCRIBING THE CONDITIONS OF RADIO WAVE PROPAGATION INSIDE BUILDINGS.....	62
<b><i>С.В. Индик, В.О. Михайленко</i></b> ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ВІРТУАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ ІР ТЕЛЕФОНІЇ.....	63
<b><i>М.М. Губіцький</i></b> МОДЕРНІЗАЦІЯ ЕЛЕКТРОПРИВОДА МЕХАНІЗМУ ПЕРЕВАНТАЖЕННЯ ЦЕГЛИ ШЛЯХОМ ВПРОВАДЖЕННЯ ПРОМИСЛОВОГО РОБОТА.....	64
<b><i>С.Г. Кислиця, А.І. Остапенко</i></b> ДОСЛІДЖЕННЯ АЛГОРИТМІВ УПРАВЛІННЯ СИНХРОННИМ ДВИГУНОМ З ПОСТІЙНИМИ МАГНІТАМИ.....	66
<b><i>О.Г. Дрючко, Б.С. Гребенюк, Д.А. Погрібняченко, Д.О. Фещенко, Р.А. Белей</i></b> ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК ФІЗИЧНИХ СЕРЕДОВИЩ ДЛЯ ПЕРЕДАЧІ ОПТИЧНИХ СИГНАЛІВ.....	68
<b><i>В.М. Галай, Д.П. Плешкань</i></b> РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ АЛГОРИТМУ ІНТЕЛЕКТУАЛЬНОГО СОРТУВАННЯ ПОСИЛОК.....	72
<b><i>А.В. Марчук</i></b> ВИКОРИСТАННЯ СИМУЛЯТОРА AWS СЕРВІСІВ LOCALSTACK ДЛЯ НАВЧАННЯ РОБОТІ З ХМАРНИМИ СЕРВІСАМИ ТА ІНФРАСТРУКТУРОЮ.....	74
<b><i>А.М. Капітон, Р.М. Талибов, О.С. Дзюбан</i></b> ОПТИМІЗАЦІЯ ХАРАКТЕРИСТИК ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ..	76
<b><i>Є.О. Мельник</i></b> ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ФРЕЗЕРУВАННЯ ДЛЯ ВЕРСТАТІВ З ПРОГРАМНИМ КЕРУВАННЯМ....	78
<b><i>С.Г. Кислиця, Є.В. Вітченко</i></b> ДОСЛІДЖЕННЯ СИСТЕМИ АВТОМАТИЧНОГО РЕГУЛЮВАННЯ ГІДРОАГРЕГАТУ МІНІ-ГЕС.....	79
<b><i>О.В. Шефер, А.В. Пащенко</i></b> ШЛЯХИ ЗНИЖЕННЯ ЕНЕРГОВИТРАТ У ПЕРЕХІДНИХ ПРОЦЕСАХ РОБОТИ ЕЛЕКТРОПРИВОДА.....	81

**UDC 621.396.96**

*I. Silin, Student,*

*V. Lysechko, Doctor of Technical Sciences, Professor*

*National University "Yuri Kondratyuk Poltava Polytechnic"*

## **MODELS FOR DESCRIBING THE CONDITIONS OF RADIO WAVE PROPAGATION INSIDE BUILDINGS**

The problem of radio wave propagation inside buildings and premises has recently received much attention. This is primarily due to the creation of local information networks, as well as the need to provide reliable radio communication for employees of enterprises and institutions for operational management and security purposes. The presence of walls, partitions, furniture, electronic equipment, people and other objects inside a building creates a complex environment for radio wave propagation. The conditions for radio wave propagation inside buildings differ significantly from those in free space. The main effects observed in the propagation of radio waves indoors are multipath, caused by multiple reflections of radio waves from walls and other objects, diffraction on numerous sharp edges of objects located inside the room, and scattering of radio waves. These effects create a complex interference structure of the electromagnetic field, which changes greatly when people and other objects move around. Thus, the models used to describe the indoor communication channel differ from traditional mobile communication channel models in two aspects:

- the size of the coverage area is significantly smaller than in urban areas;
- radio wave propagation conditions are more diverse.

The propagation of radio waves inside buildings is mainly determined by the following parameters: building layout, construction materials, and building type.

The main phenomena of propagation inside buildings are the same as in urban areas, namely: reflection, diffraction, absorption, scattering.

The signal strength depends on whether the doors in the rooms are open or closed, and on where the antennas are located (at table level or under the ceiling). There are many walls and partitions inside houses, various objects that significantly affect the formation of the electromagnetic field structure both inside and outside the house.

Usually, walls and partitions inside buildings are divided into two types:

- "hard" walls that are part of the building structure;
- "soft" walls - partitions that can be moved. As a rule, the height of these partitions is less than the height of the walls in the room.

Walls and partitions inside buildings are usually made of different building materials with different electrical properties. This makes it difficult to create a general model suitable for use in different types of buildings.

The attenuation during propagation between different floors is determined by

- the external dimensions and material of the building;
- the design of the floors;
- external environment;
- the number of windows in the building and the nature of the wall surface.

Taking into account the above models for describing the conditions of radio wave propagation inside buildings makes it possible to plan a wireless access network with maximum efficiency.

## **МОДЕЛІ ОПИСУ УМОВ ПОШИРЕННЯ РАДІОХВИЛЬ УСЕРЕДИНІ БУДІВЕЛЬ**

*І. Сілін, студент,*

*В. Лисечко, д.т.н., професор*

*Національний університет «Полтавська політехніка імені Юрія Кондратюка»*

**УДК 621.395.721**

*С.В. Индик, к.т.н., доцент,*

*В.О. Михайленко, магістрант*

*Національний університет «Полтавська політехніка імені Юрія Кондратюка»*

## **ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ВІРТУАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ ІР ТЕЛЕФОНІЇ**

Традиційно телефонні мережі базуються на аналогових або цифрових технологіях комутації каналів, де кожен виклик або з'єднання вимагає виділення певного фізичного каналу для обміну інформацією між абонентами. Це забезпечує високу якість зв'язку, але водночас вимагає значних витрат на підтримку інфраструктури. ІР телефонія, у свою чергу, використовує метод комутації пакетів, при якому голосові дані перетворюються на цифрові пакети і передаються через глобальну мережу Інтернет або інші ІР-мережі, що дозволяє знижувати витрати на зв'язок і зручніше масштабувати мережу.

Перехід від традиційної телефонної мережі до ІР телефонії пов'язаний із заміною фізичних ліній на логічні канали, які передають голосові дані у вигляді пакетів. Це знижує витрати на обслуговування та дозволяє інтегрувати різні мультимедійні сервіси, такі як відеозв'язок та передавання даних, в одну мережу. Перевагою є також можливість забезпечити якість обслуговування, керуючи пропускнуою здатністю і мінімізуючи затримки при передачі даних.

Мережі на основі технології ІР телефонії мають різноманітну архітектуру, що включає SIP сервери, шлюзи, телефонні апарати та інше. Основними перевагами є гнучкість у налаштуваннях і масштабуванні, а також можливість інтеграції з різноманітними корпоративними мережами, у яких відбувається обмін миттєвими повідомленнями або відеоконференції. ІР телефонія дозволяє об'єднувати голосові виклики, передавання даних і відео в одному сервісі, що зменшує потребу в фізичних мережах.

Для забезпечення високої якості обслуговування в мережах ІР телефонії важливою є методика управління пропускнуою здатністю. Ключовими параметрами є мінімізація затримок і забезпечення стабільності з'єднань. Для точного визначення загальної затримки в мережі ІР телефонії була створена

**Додаток С**

**Презентація**

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ  
КОНДРАТЮКА»**

**Розробка безпроводової мережі  
абонентського доступу на основі  
протоколу IEEE 802.11**

Студент: Іван СІЛІН

Керівник: професор Володимир ЛИСЕЧКО

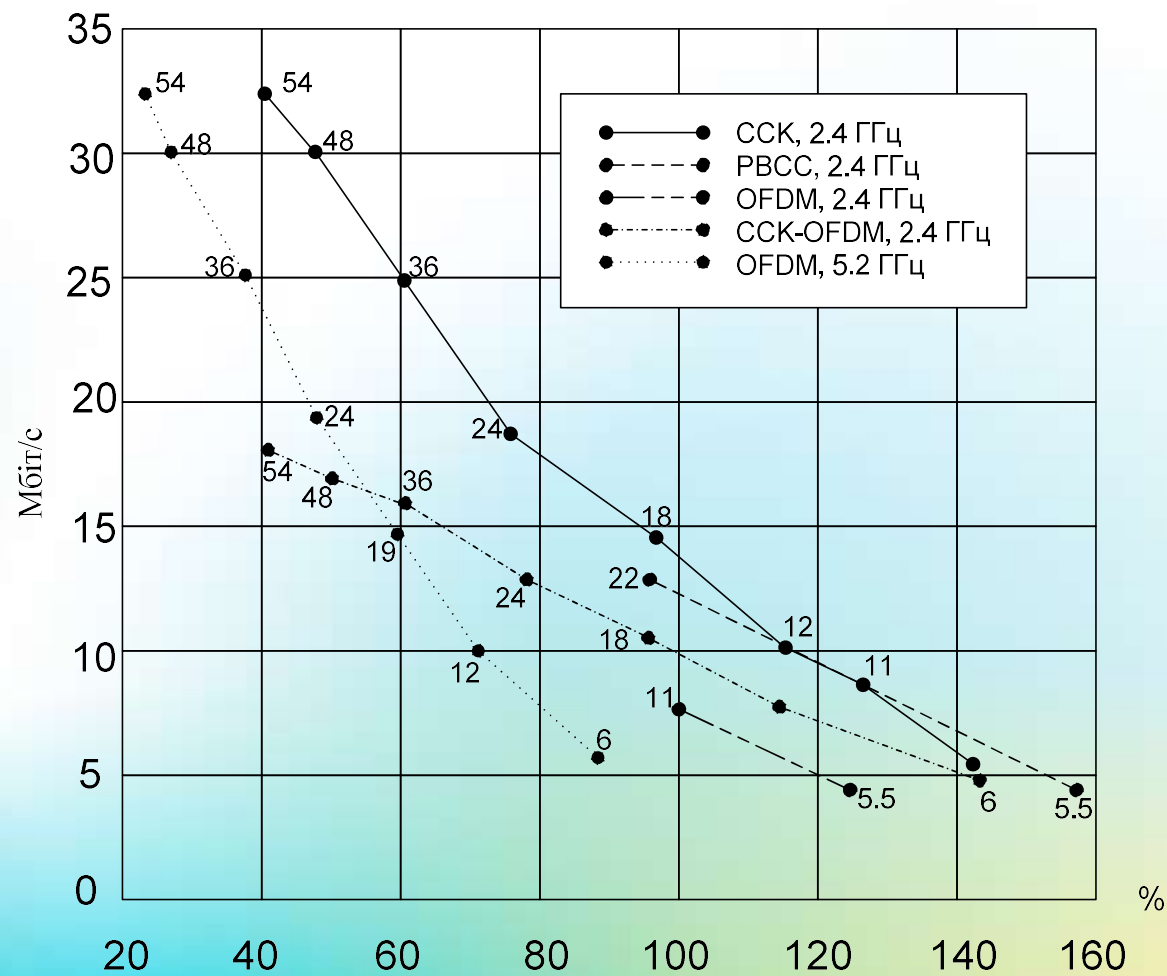
# Мета та задачі роботи

**Мета:** розробка безпроводової мережі абонентського доступу на основі протоколу IEEE 802.11, що забезпечить стабільність, високу швидкість передачі даних та надійний захист інформації.

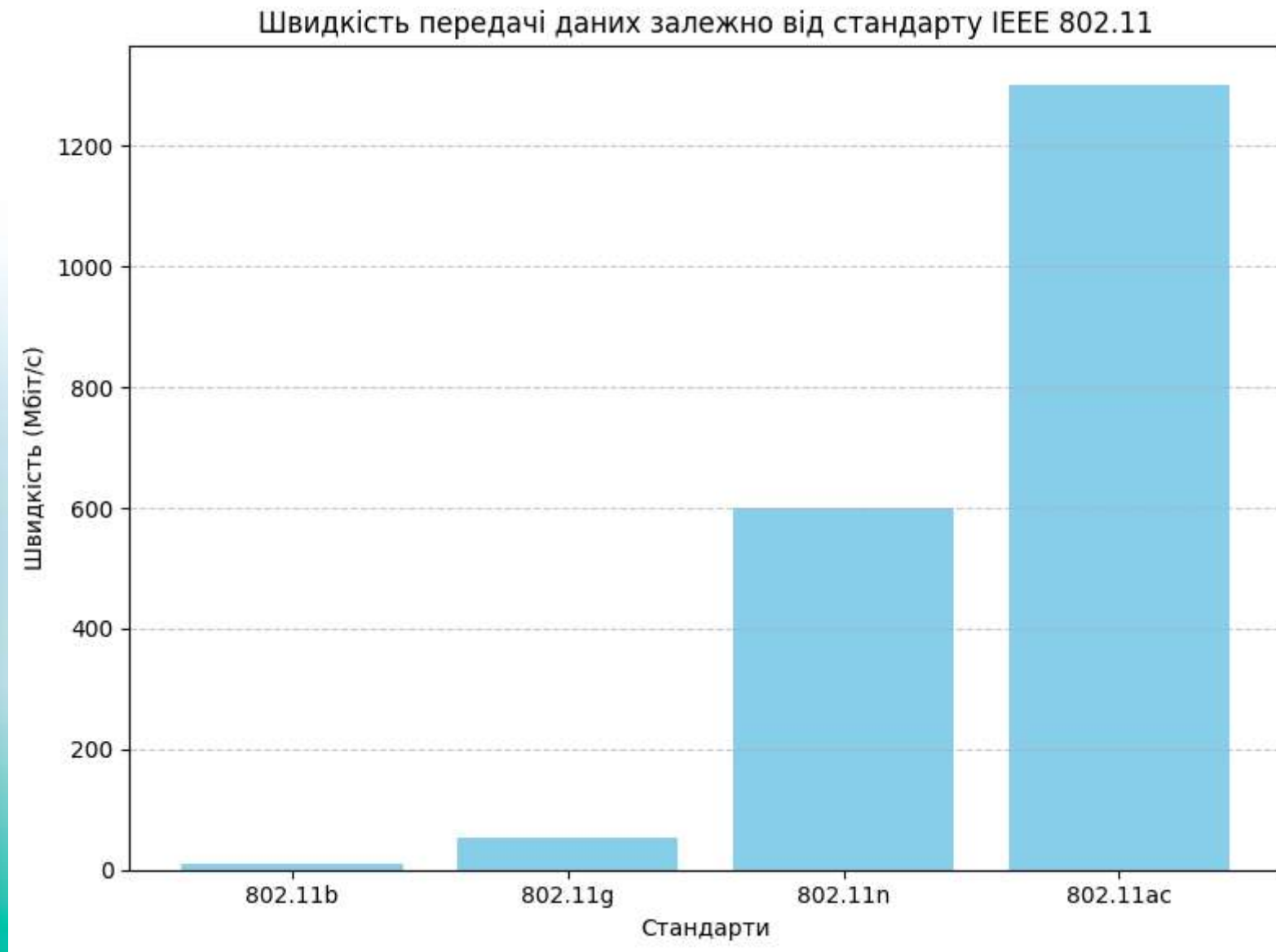
Для досягнення поставленої мети визначено такі **задачі:**

1. Виконати аналіз існуючих стандартів безпроводових мереж і їхніх технічних характеристик.
2. Дослідити принципи проектування та побудови мереж абонентського доступу в умовах багатоповерхових житлових будинків.
3. Виконати моделювання роботи мережі в умовах високого навантаження.
4. Розробити проєкт оптимальної мережі, враховуючи технічні, економічні та безпекові аспекти.
5. Надати рекомендації щодо впровадження розробленої мережі у практичне використання.

Залежність швидкості передачі від відстані для різних технологій передачі.



Залежність швидкості передачі від відстані для різних технологій передачі.



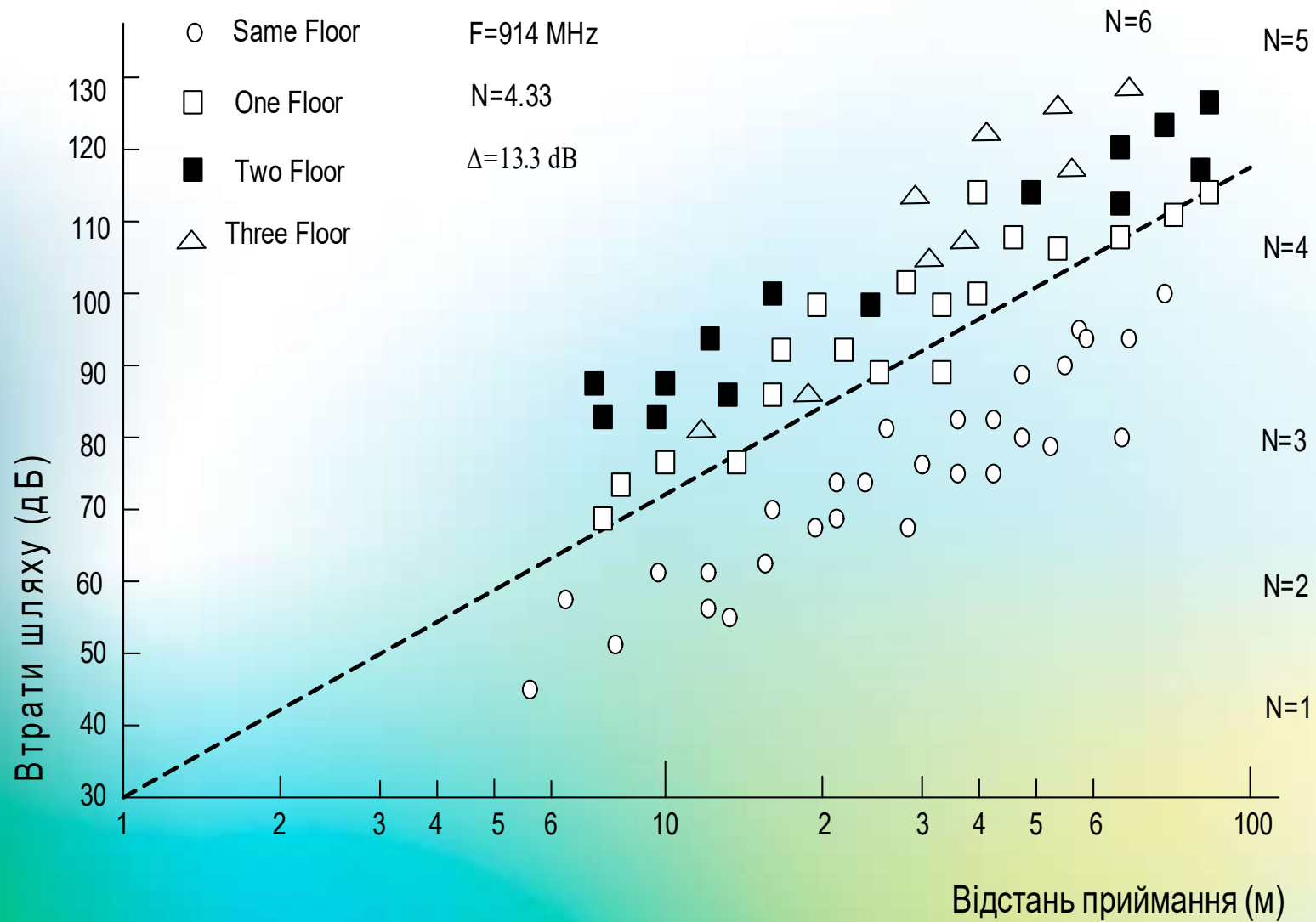
## Відносна діелектрична проникність і тангенс втрат

Матеріал	Відносна діелектрична проникність	Тангенс кута втрат
Оргскло	2,74	$3,2 \cdot 10^{-4}$
Жалюзі (закриті)	3,49	$5,96 \cdot 10^{-5}$
Жалюзі (закриті)	1,96	$5,96 \cdot 10^{-5}$
Червона цегла (суха)	5,86	$1,16 \cdot 10^{-5}$
Червона цегла (волога)	5,92	$1,17 \cdot 10^{-1}$
Килим	1,32	$5,96 \cdot 10^{-4}$
Стельове покриття	1,32	$1,44 \cdot 10^{-2}$
Тканина	1,49	$5,96 \cdot 10^{-5}$
Скловолокно	1,02	$9,21 \cdot 10^{-4}$
Стекло	6,38	$2,6 \cdot 10^{-2}$
Лінолеум	3,08	$1,45 \cdot 10^{-3}$
Хвойна дошка	2,58	$2,0 \cdot 10^{-2}$
ДСП	2,7	$1,1 \cdot 10^{-1}$
Фанера	2,47	$1,27 \cdot 10^{-1}$
Гіпсова плита	1,07	$4,29 \cdot 10^{-1}$
Кахель	3,08	$5,88 \cdot 10^{-2}$
Толь	2,47	$3,86 \cdot 10^{-2}$

# Коефіцієнти проходження й відбиття

Матеріал	T(дБ)			R(дБ)		
	2,3 ГГц	5,25 ГГц	Δ	2,3 ГГц	5,25 ГГц	Δ
Оргскло (7,1 мм)	-0,3560	-0,9267	0,5707	-12,23	-5,65	-6,5753
Оргскло (2,5 мм)	-0,0046	-0,2041	0,1994	-21,69	-13,25	-8,4770
Жалюзі (закриті)	-0,0016	0,002	-0,0035	-30,97	-20,39	-10,578
Жалюзі (відкриті)	0,0137	0,0315	-0,0178	-44,23	-46,95	2,7210
Червона цегла (суха)	-4,4349	-14,621	10,182	-12,53	-8,98	-3,5459
Червона цегла(волога)	-4,5119	-14,599	10,087	-12,52	-9,41	-3,1185
Килим	-0,0271	-0,0056	-0,0214	-26,94	-18,7	-8,2710
Стельове покриття	-0,0872	-0,1795	0,0923	-21,07	-18,7	-2,3470
Тканина	0,021 6	0,013 3	0,0083	-41,70	-30,1	-11,570
Скловолокно	-0,0241	-0,034	0,0099	-39,40	-28,8	-10,581
Стекло	-0,4998	-1,6906	1,1908	-11,29	-4,9	-6,3446
Лінолеум	-0,0198	-0,1278	0,1081	-23,69	-16,0	-7,6690
Хвойна дошка	-2,7889	-6,1253	3,3364	-17,45	-14,8	-2,689
ДСП	-1,6511	-1,9508	0,2997	-8,59	-14,1	5,5359
Фанера	-1,9138	-1,8337	-0,0801	-9,05	-30,5	21,42
Гіпсова плита	-14,863	-13,235	-1,6280	-2,38	-9,24	6,858 7
Кахель	-2,2163	-1,4217	-0,7946	-6,24	-14,9	8,609 3
Толь	-0,0956	-0,1341	0,038 5	-28,88	-17,8	-11,067
Шлакоблок (сухий)	-6,7141	-10,326	3,611 9	-7,67	-6,13	-1,5324
Шлакоблок (вологий)	-7,3527	-12,384	5,031 3	-5,05	-7,55	2,508 0

# Залежність загасання сигналу від відстані



## Результати моделювання пропускної спроможності каналів

	DFS	Таймер відкату	RTS	SIFS	CTS	SIFS	Пакет даних	SIFS	ACK	Всього	Швидкість Мбіт/с
Час 1Мбіт/с. Відео, мкс	50	100	352	10	304	10	12480	10	304	13620	0,93
Об'єм даних 1Мбіт/с. Відео, байт	0	0	20	0	14	0	1536	0	14	1584	
Час, 1Мбіт/с. Дані, мкс	50	100	352	10	304	10	8384	10	304	9524	0,9
Об'єм даних 1Мбіт/с. Дані, байт	0	0	20	0	14	0	1024	0	14	1072	
Час 2Мбіт/с. Відео, мкс	50	100	176	10	152	10	6336	10	152	6996	1,81
Об'єм даних 2Мбіт/с. Відео, байт	0	0	20	0	14	0	1536	0	14	1584	
Час, 2Мбіт/с. Дані, мкс	50	100	176	10	152	10	4288	10	152	4948	1,73
Об'єм даних 2Мбіт/с. Дані, байт	0	0	20	0	14	0	1024	0	14	1072	
Час, 5,5Мбіт/с. Відео, мкс	50	100	176	10	152	10	2426	10	152	3086	4,11
Об'єм даних 5,5Мбіт/с. Відео, байт	0	0	20	0	14	0	1536	0	14	1584	3,66
Час, 5,5Мбіт/с. Дані, мкс	50	100	176	10	152	10	1681	10	152	2341	
Об'єм даних 5,5Мбіт/с. Дані, байт	0	0	20	0	14	0	1024	0	14	1072	6,44
Час, 11Мбіт/с. Відео, мкс	50	100	176	10	152	10	1309	10	152	1969	
Об'єм даних 11Мбіт/с. Відео, байт	0	0	20	0	14	0	1536	0	14	1584	5,37
Час, 11Мбіт/с. Дані, мкс	50	100	176	10	152	10	937	10	152	1597	
Об'єм даних 11Мбіт/с. Дані, байт	0	0	20	0	14	0	1024	0	14	1072	

# Основні кроки проектування безпроводової мережі в багатоповерховій будівлі

**Аналіз існуючих стандартів безпроводових мереж:** Дослідження різних стандартів IEEE 802.11 (a/b/g/n/ac) для визначення оптимального вибору з точки зору швидкості передачі даних, стабільності та безпеки.

**Дослідження принципів проектування мереж абонентського доступу:** Вивчення методів розміщення точок доступу, враховуючи тип будівлі, кількість користувачів та матеріали стін, для забезпечення оптимального покриття та мінімізації інтерференції.

**Моделювання роботи мережі в умовах високого навантаження:** Використання спеціалізованого програмного забезпечення для симуляції роботи мережі при інтенсивному використанні, оцінка пропускної здатності та виявлення потенційних "вузьких місць".

**Розробка оптимальної мережі:** Створення детального плану мережі з урахуванням результатів моделювання, включаючи вибір обладнання, розміщення точок доступу та налаштування параметрів для забезпечення стабільної та швидкої роботи.

**Надання рекомендацій для впровадження:** Розробка рекомендацій щодо вибору обладнання з підтримкою сучасних стандартів безпеки), оптимізації розміщення точок доступу та інвестицій в інфраструктуру для підвищення якості зв'язку.

Дякую за увагу!