МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **СПОСОБИ ПОБУДОВИ ЗАХИСТУ РАДІОКАНАЛУ НА ОСНОВІ ПРОТОКОЛУ IEEE 802.11 ac**

Студентка групи СЗЗ-51 Сукач Олександра Юріївна _____
(підпис)

Науковий керівник: к.т.н., доц Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студентці: Сукач Олександрі Юріївні

1.Тема роботи: Способи побудови захисту радіоканалу на основі протоколу IEEE 802.11 ac, затверджено наказом від «24 » лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси захисту інформації, яка передається через радіоканали та Wi-Fi - мережі.

4. Предметом дослідження: технології захисту, які забезпечують безпеку передачі інформації, та можуть бути реалізовані на основі стандарту IEEE 802.11 a.c.

5. Мета роботи: удосконалення та рекомендації щодо застосування методів захисту інформації, яка передається по радіоканалу на основі стандарту IEEE 802.11 a.c.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз стандарту IEEE 802.11 a.c.;
- аналіз та дослідження існуючих методів захисту радіоканалу за допомогою стандарту IEEE 802.11 a.c.;
- створення рекомендацій щодо застосування стандарту IEEE 802.11 a.c. в Wi-Fi-мережах.

7. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Шуклін Г.В.
(підпис)

Завдання прийняла до виконання _____Сукач О.Ю.
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «24» лютого 2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 26.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студентка: СЗЗ -51 Сукач О.Ю. _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Г.В. _____
(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____
(підпис)

ЗМІСТ

РЕФЕРАТ

Дипломна робота містить 50 сторінок, 3 рисунки, 6 таблиць.

Стандарт IEEE 802.11ac на теперішній час є великою новацією в завданнях передачі та прийому даних. Не зважаючи на те, що постійно здійснюється намір створити нові технології, Wi-Fi все ж таки залишається на перших місцях. Вперше первинна хвиля точок доступу корпоративного класу було надоно в четвертому кварталі 2012 року, і відтоді точки доступу, що підтримують IEEE 802.11ac, отримали величезний попит. Так як мережа Wi-Fi є радіоканал з власною частотою та своїми параметрами, то передача та прийом даних знаходяться в зоні спостережень зловмисників. Отже, застосування нових стандартів для забезпечення безпечного захисту інформації, яка передається та отримується через мережу Wi-Fi є запорукою гарантованого захисту інформації на об`єктах, які цього потребують. В даній роботі представлено застосування стандарту IEEE 802.11ac для захисту радіоканалу.

Об’єктом дослідження: процеси захисту інформації яка передається через радіоканали та Wi-Fi-мережах.

Предметом дослідження є технології захисту, які забезпечують безпеку передачі інформації, та можуть бути реалізовані на основі стандарту IEEE 802.11 a.c.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації, яка передається по радіоканалу на основі стандарту IEEE 802.11 a.c.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз стандарту IEEE 802.11 a.c.;
- аналіз та дослідження існуючих методів захисту радіоканалу за допомогою стандарту IEEE 802.11 a.c.;
- створення рекомендацій щодо застосування стандарту IEEE 802.11 a.c. в Wi-Fi-мережах.

ABSTRACT

Thesis contains 79 pages, 3 figures, 6 tables

The IEEE 802.11ac standard is currently a major innovation in data transmission and reception. Despite the fact that new technologies are constantly being developed, Wi-Fi is still at the forefront. The first initial wave of enterprise-class access points was delivered in the fourth quarter of 2012, and since then, access points that support IEEE 802.11ac have been in great demand. Since the Wi-Fi network is a radio channel with its own frequency and parameters, data transmission and reception are within the scope of observation by intruders. Therefore, the use of new standards to ensure the secure protection of information transmitted and received over a Wi-Fi network is a guarantee of guaranteed information protection at facilities that need it. This paper presents the application of the IEEE 802.11ac standard for radio channel protection.

Object of research: processes for protecting information transmitted via radio channels and Wi-Fi networks.

The subject security technologies that ensure the security of information transmission and can be implemented on the basis of the IEEE 802.11 a.s. standard.

The purpose improvements and recommendations for the use of methods for protecting information transmitted over a radio channel based on the IEEE 802.11 a.s. standard.

To achieve this goal, the following main tasks are performed:

- analysis of the IEEE 802.11 a.s. standard;
- analysis and research of existing methods of radio channel protection using the IEEE 802.11 a.s. standard;
- development of recommendations for the use of the IEEE 802.11 a.s. standard in Wi-Fi networks.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БЛОС	Бездротові локальні обчислювальні системи	Wireless local cleaning systems
ОІД	Об`єкт інформаційної діяльності	Object of information activity
СІЗ	Системи інформаційного захисту	Information protection systems
МКФЗ	Метод квадратичного фазового зсуву	Quadrature phase shift keying
ПКП	Попереджувальна корекція помилки	Forward error correction
ВМП	Відношення модуляція/помилка	Modulation error ratio
RAM	Пам’ять з довільним доступом	Random Access Memory
RFID	Радіочастотна ідентифікація	Radio frequency identification
ROM	Пам’ять лише для читання	Read Only Memory
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	
ЗЗІ	Засоби захисту інформації	
ІС	Інформаційна система	
ІТС	Інформаційно-телекомунікаційна система	
ОЗП	Оперативний запам’ятовувальний пристрій	
УВЧ	Ультра високі частоти	

ВСТУП

З того часу, як було ратифіковано стандарт IEEE 802.11ac у 1999 році отримало широке застосування бездротові локальні обчислювальні системи (БЛОС). Дані системи отримали широкого застосування на об`єктах інформаційної діяльності (ОІД), в приміщеннях, де проводяться конференції, та в багатьох містах промисловості та відпочинку. БЛОС стандарту IEEE 802.11a.c стикається з певною кількістю нових проблем в адмініструванні мереж та систем інформаційного захисту (СІЗ). На відміну від дротових мереж, БЛОС стандарту IEEE 802.11a.c застосовують загальнодоступний радіоканал, за допомогою якого здійснюється зв'язок з абонентами. Застосування такого каналу призводить до множини нових складних проблем, розв`язання яких призвело до здійснення певних доповнень до стандарту IEEE 802.11.

Засоби, функцією яких є забезпечення захисту інформації та інформаційної безпеки і які передбачені специфікацією IEEE 802.11 та відповідні доповнення 802.11b, 802.11a, 802.11g, зазнали ретельного аналізу та багатьох зауважень від експертів. Експертами було виявлено дуже шкідливі вразливості в механізмах *аутентифікації*, в механізмах забезпечення конфіденційності інформації та цілісності інформації, яка обробляється на ОІД.

Актуальність теми На теперішній час більшість компаній застосовують безпосередньо Wi-Fi-мережі. Це пов`язано зі зручністю, мобільністю та відносною низькою ціною послуг зв'язку відокремлених приміщень та спроможністю їх переміщення в зоні експлуатації обладнання. У Wi-Fi-мережах застосовуються складні алгоритми, які є результатами математичного моделювання автентифікації, шифрування інформації, контролю цілісності передачі цієї інформації. Це дає змогу мати певні гарантії надійного збереження конфіденційної інформації протягом застосування даної технології. Однак, якщо не забезпечувати постійного контролю в налаштуванні бездротової мережі. До початку налаштування зловмисник (хакер) вже володіє певними навиками та навичками щодо несанкціонованого доступу, а саме: доступ до ресурсів локальної мережі; прослуховування Інтернет-трафіку та його крадіжка;

спотворення інформації, яка передається та приймається через мережі; впровадження фальшивої точки доступу; розсилка спаму від імені власника мережі.

Тому завдання надійного налаштування Wi-Fi-мережі, яка використовує радіоканали є актуальною на теперішній час.

Об’єктом дослідження: є процеси захисту інформації яка передається через радіоканали та Wi-Fi-мережах.

Предметом дослідження є технології захисту, які забезпечують безпеку передачі інформації, та можуть бути реалізовані на основі стандарту IEEE 802.11 a.c.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації, яка передається по радіоканалу на основі стандарту IEEE 802.11 a.c.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз стандарту IEEE 802.11 a.c.;
- аналіз та дослідження існуючих методів захисту радіоканалу за допомогою стандарту IEEE 802.11 a.c.;
- створення рекомендацій щодо застосування стандарту IEEE 802.11 a.c. в Wi-Fi-мережах.

Відповідно даним Інфонетікс, технологія 802.11.ac досягла частки ринку близько 80 % серед корпоративних точок доступу на початок 2018 року та 100 % на початок 2023 року. На рисунку 1.1 представлено квартальний звіт за четвертий квартал 2022 року.

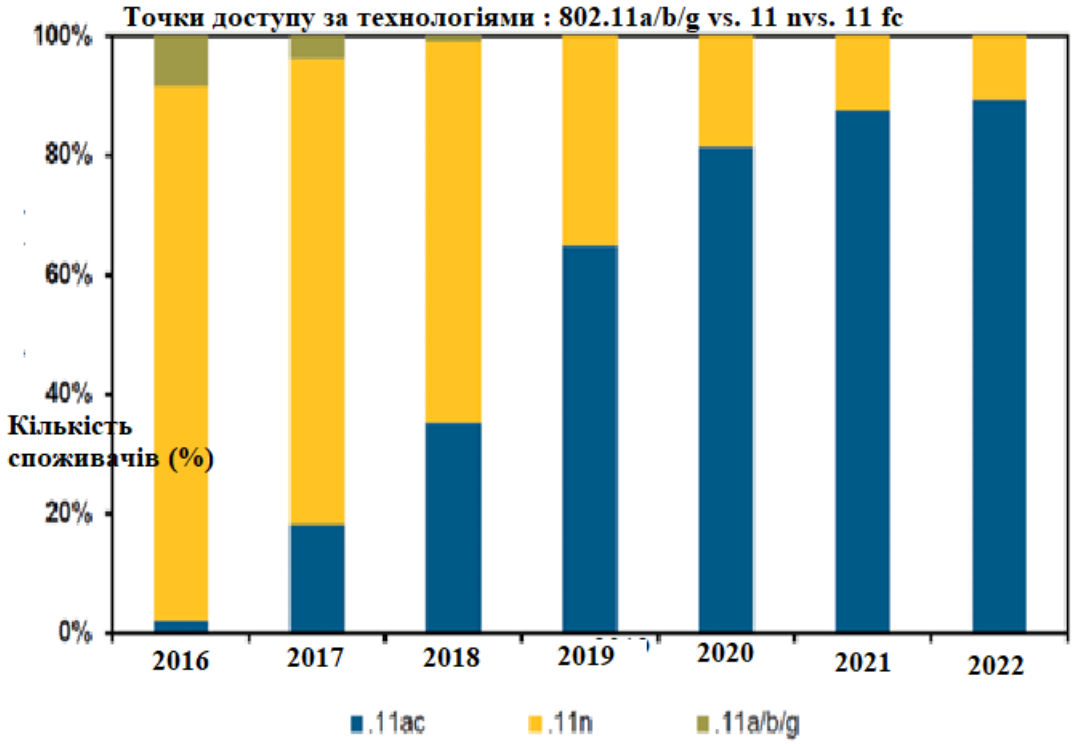


Рисунок 1.1. Звіт за 4 квартал 2022 року щодо світових та регіональних ринковим часткам, розмірам та прогнозам для БЛОС та WiFi- телефонів

Велика кількість власників інфраструктури $11n$ протягом достатнього тривалого часу використовувало існуючу розгортку та знаходилось в стані очікування виходу на ринок другої хвилі продуктів, реалізованих технологією 11ac до здійснення оновлення. Мережі $11n$ - $2x2:2$, $3x3:2$ або $3x3:3$ в багатьох випадках існує спроможність здійснити оптимізацію для отримання більш високої продуктивності, і в свою чергу вони повністю відповідають вимогам більшості сучасних корпоративних розгортань. Недоліком застарілих розгортань мереж $11n$ є те, що багато початкових моделей точок доступу $11n$ не спроможні підтримуватись в оновленнях коду, що призводить до обмеження їх безпеки та

продуктивності.

1.1. Загальна характеристика технології IEEE 802.11 ac

Технологія 11ac реалізована на частоті 5 гіга герц, що пояснює те, що доповнення стандарту IEEE 802.11ac не забезпечує описання її застосування в смузі частот 2,4 гіга герц. Щоб використовувати більш широкі канали, необхідно мати більший частотний діапазон, а ширина смуги 2,4 гіга герц забезпечує 83,5 мега герц. На фізичному рівні довільні реалізації для смуги частот 2,4 гіга герца є особливими.

Варто відмітити, що технологія 11ac залежить не тільки від радіоканалів. Точка доступу уявляє собою комп'ютер, мозком якого є процесор, оперативна пам`ять, флеш-пам'ять тощо. Зі створенням нових технологій передачі інформації по радіоканалам, створюються і нове програмне забезпечення з розширеними функціями, що в свою чергу призводить до більшого навантаження точок доступу. Існує цілий клас точок доступу 11ac, які містять подвійний модуль радіозв`язку, роботу яких забезпечують двох та більше ядерних процесорів, та великим об'ємом оперативної пам'яті, з наявними портами *Gigabit Ethernet* і які спроможні здійснювати розвантаження шифрування з одночасною наявністю функцій високого класу.

Таке признання технології 11ac над більш старим стандартом IEEE 802.11n пов`язано з тим, що технологію 11ac було реалізовано двома етапами фундаментом яких були властивості та можливості *радіочінсета*. На рисунку 1.2 показано відмінності між технологіями, реалізованими в кожній із двох етапів.

PHY/Feature	802.11n	Хвиля-1 802.11ac	Хвиля-2 802.11ac
Ширина каналу	20, 40 МГц	20, 40 МГц	20, 40, 80, 160 МГц
Просторові потоки (SS)	1, 2, 3	2, 3	2, 3, 4
Модуляція QAM	64 QAM	256 QAM	256 QAM
Тип MIMO	SU-MIMO	SU-MIMO	MU-MIMO
Підтримка MCS	MCS 0-23 для 1, 2, 3 SS	MCS 0-9 для 1, 2, 3 SS	MCS 0-9 для 1, 2, 3, 4 SS
Максимальна швідкість передачі даних	450 Мбіт/с	1,3 Гбіт/с	3,467 Гбіт/с
TxBF	Ні	Змінна	Так
Варіації радіо модуля	2x2:2, 3x3:2, 3x3:3	2x2:2, 3x3:3	4x4:4*

Рисунок 1.2. Відмінність між двома етапами технології 11 ac

Обладнання 802.11*n* забезпечують підтримку діапазон радіоканалів від 20 мега герц до 40 мега герц. Обладнання «*Хвиля* 1» 11*ac* забезпечують підтримку радіоканалів 20 мега герц, 40 мега герц та 80 мега герц. Що стосується обладнання «*Хвиля* 2», то воно забезпечує підтримку радіоканалів 20 мега герц, 40 мега герц, 80 мега герц та 160 мега герц. На теперішній час радіоканали, які забезпечують 160 мега герц не можливо застосовувати в корпоративних розмежуваннях. Це пов`язано з тим, що в таких корпоративних розмежуваннях не існує просторового радіоканалу, який би забезпечував неперервну передачу інформації в смугах частот 5 гіга герц *UNII*. Однак комісія *FCC* зробола пропозиція, результатом якої є застосування до чотирьох радіоканалів, які не корелюють один з одним на частоті 160 мега герц в Сполучених Штатах Америки. Що стосується інших країн, то це компетентність органів, які здійснюють відповідне регулювання. За допомогою імітаційної моделі радіоканалів, на рисунку 1.3 представлено допустимий спектр частот, який не вимагає відповідного дозволу.

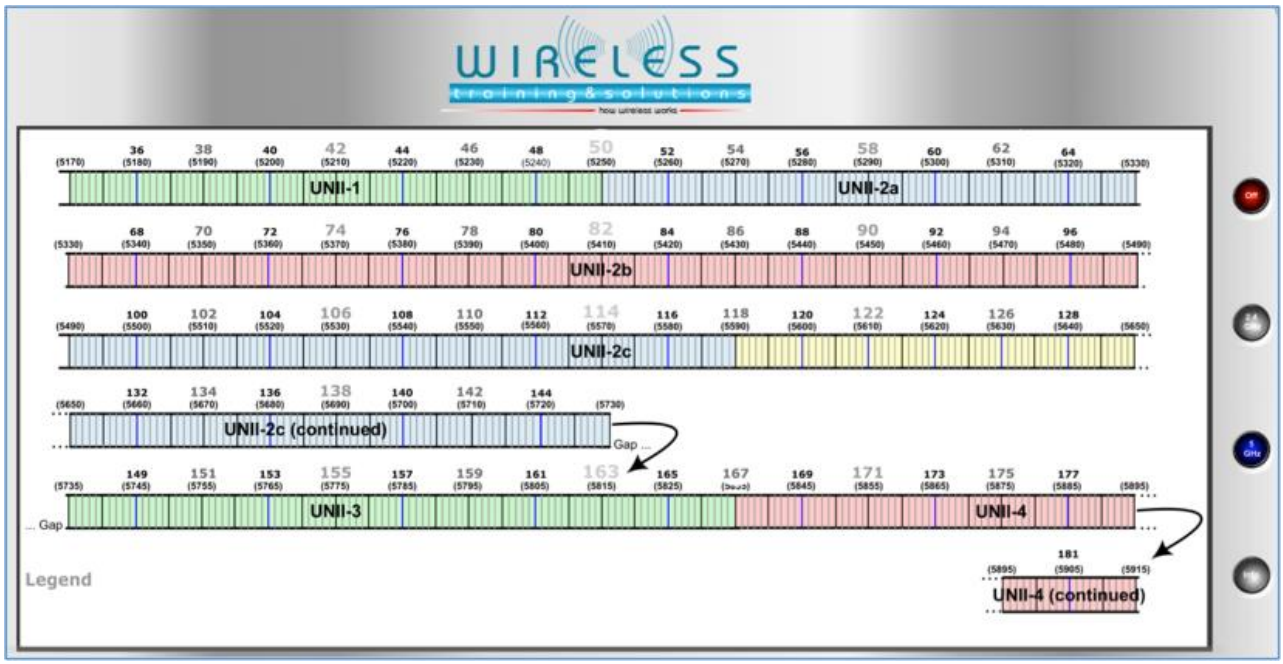


Рисунок 1.3 Смуга допустимого діапазону частот радіоканалів зв`язку.

Для того, щоб розширити пропускну спроможність мережі Wi-Fi, необхідно здійснити подвоєння ширини каналу при наявності достатнього числа таких каналів. Подвоєння ширини каналу прямо пропорційне подвоєнню його пропускної спроможності. Однак, треба розуміти, що збільшення пропускної спроможності призводить до зменшення потужності самої системи. Це зменшення для вихідної потужності скорочується два рази для всього каналу. При певних умовах таке подвоєння не викликає труднощів, однак в багатьох випадках це призводить до додаткових технічних труднощів. Подвоєння ширини каналу призводить до зростання базового рівня шуму до 3 децибел, що в свою чергу призводить до зростання ймовірності перешкод. Тому канали 80 мега герц та 160 мега герц завжди є динамічними. Точки доступу можуть застосовувати механізми інформаційного захисту, такі як RTS/CTS для забезпечення чистоти каналів 80 мега герц та 160 мега герц. При наявності доступу лише до певної області широкого каналу, то це призводить до того, що точки доступу зменшать ширину каналу для отримання максимальної пропускної спроможності.

Спроможність застосовувати канали ширини 80 мега герц та 160 мега герц, не означає, що це варто здійснювати. Більш раціонально застосовувати канали 20 мега герцу в середовищах, які мають високу щільність. Такими середовищами є аудиторії, танцювальні зали, виставкові центри, аеропорти та спортивні арени. Це пов`язано з тим, що такі середовища є найбільш ефективними в застосуванні таких каналів. Для середовищ, які мають низьку щільність, але при цьому їх пропускна спроможність достатньо велика, більш ефективно застосовувати канали 40 мега герц в частотній смузі 5 гіга герц, при умові повторного використання каналів. При розгортанні на об'єкті інформаційної діяльності однієї або двох точок доступу і при цьому потужність завад не значна, то варто застосовувати канали і на 80 мега герц. На теперішній час не існує середовища в якому було б ефективно використовувати для каналів 160 мега герц. Єдиним винятком є спрямовані канали виключно "*точка – точка*". При необхідності неперервної наявності достатньо високої пропускної спроможності, варто налаштувати одну точку доступу для застосування каналу 80 мега герц, за відсутності найближчих точок доступу, які не використовують будь-яку частину такого каналу.

Усі засоби $11n$ підтримують $SU-MIMO$. Це означає, що в каналі можливо здійснювати тільки одне передавання: або вихід інформації або вхід її. Засоби $11ac$ "$Eman-1$" підтримують $SU-MIMO$, а точки доступу "$Eman-2$" завжди сумісні з технологією $MU-MIMO$.

Технологія низхідного передавання $MU-MIMO$ від точки доступу до споживача, спроможна здійснювати не одну передачу одночасно, за допомогою технології $TxBF$. Це дає можливість посилювати радіосигнали не в одній області, а також здійснювати заглушення в областях, які не задіяні. Більшість точок доступу $MU-MIMO$ підтримуватимуть три або чотири передачі одночасно. Технологія $MU-MIMO$ дає можливість підвищити ефективність протоколу MAC при умові сумісності з $3SS$ або $4SS$. В цьому випадку точка доступу підтримує кілька споживачів, які сумісні з $1SS$.

Під просторовим потоком будемо розглядати технологічний процес поділу потоку даних на певну кількість частин, які можна вважати просторовими під потоками та одночасного їх передавання через певну кількість радіо ланцюгів на одному каналі. Загальна схема просторового потоку представлено на рисунку 1.4.

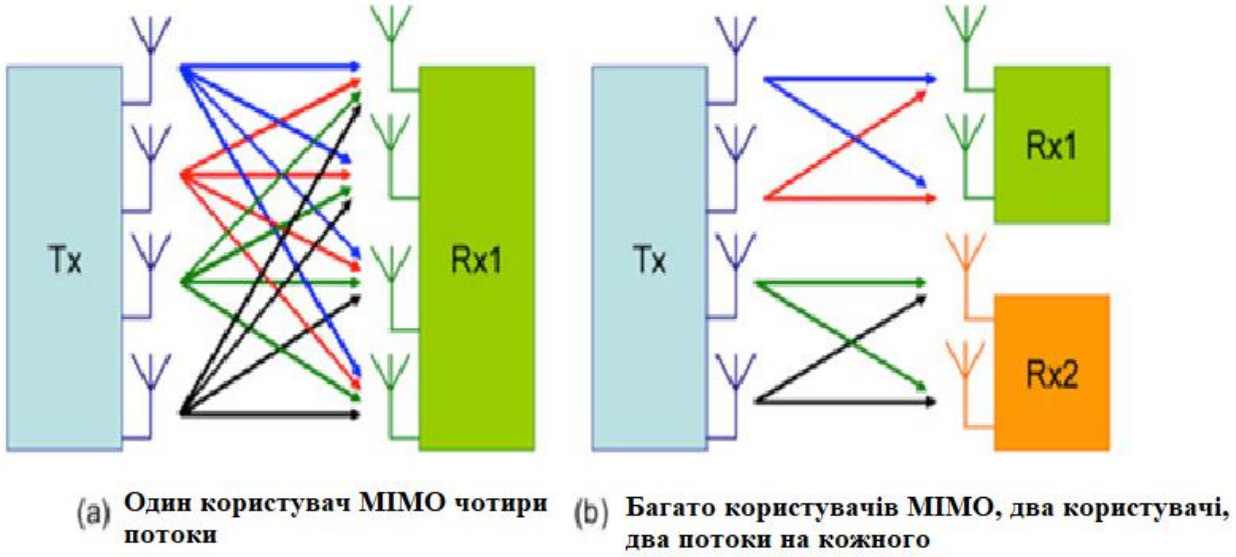


Рисунок 1.4. Схема просторового потоку.

За рахунок використання великої кількості маршрутів та цифрових сигнальних процесорів *DSP* приймачі, які сумісні з *MU – MIMO* спроможні здійснювати декодування просторових потоків та здійснювати відновлення потоків даних.

1.2. Модуляції в технології IEEE 802.11 ac

В даній технології застосовують QAM модуляцію, що англійською мовою означає *Quadrature Amplitud Modulation* і в перекладі на українську мову означає модуляція методом квадратичних амплітуд. Даний метод уявляє собою передачу цифрового інформативного потоку у вигляді аналогового сигналу. Дана технологія досягається за рахунок поділу несучої хвилі на дві несучі хвилі, які

мають однакові частоти, але зсунуті одна відносно другої на кут 90^0. Кожну з цих хвиль модулюють за одним із двох або більше дискретних значень амплітуди. Комбінація всіх значень амплітуд на цих двох несучих хвилях уявляє собою бінарне бітове зображення. На рисунку 1.5. представлено схему даної бітової модуляції. Компонента I моделює несучу хвилю без зсуву, а компонента Q моделює несучу хвилю, яка має зсув на 90^0 по відношенню до першої хвилі.

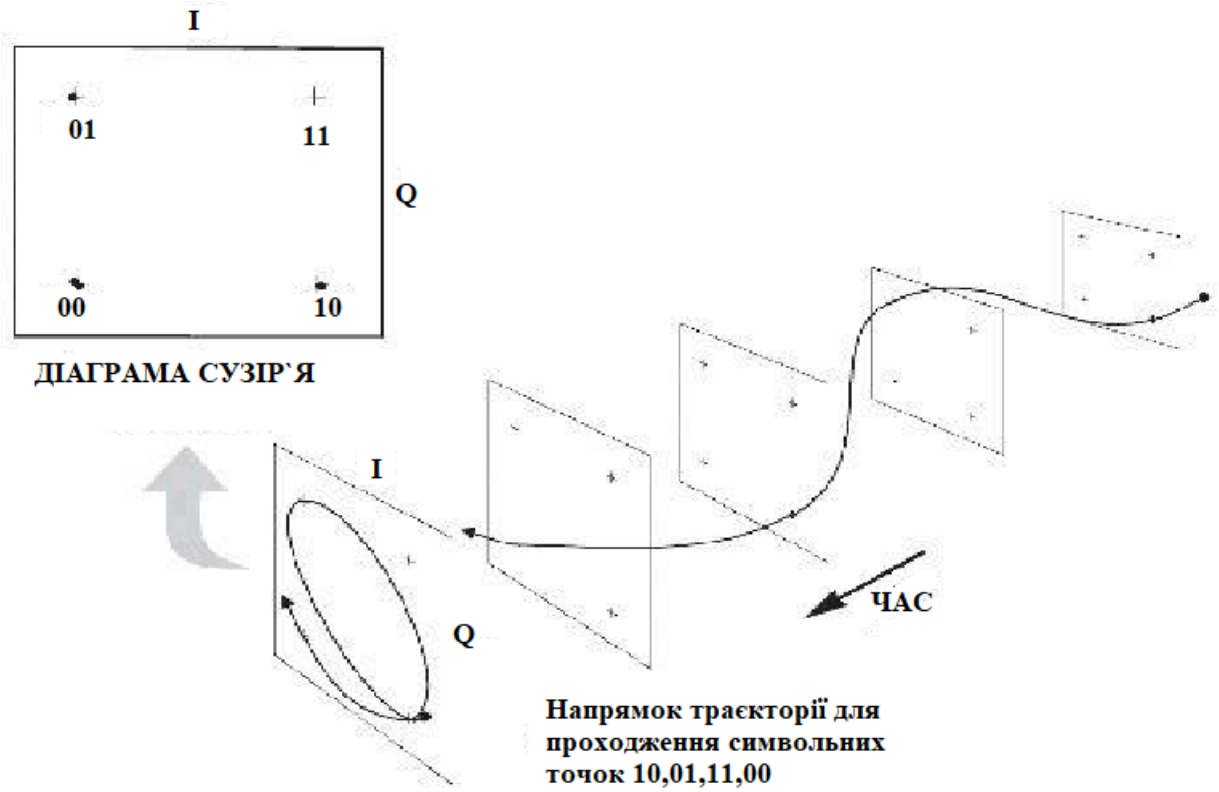


Рисунок 1.5 Діаграма сузір`я відображення I/Q вектора.

Одна з найпростіших форм QAM модуляції є метод квадратичного фазового зсуву (МКФЗ), яка отримала позначення $4\,QAM$. Даний метод використовує дві несучі електромагнітні хвилі, які розповсюджуються з однаковими частотами, однак які мають зсув на 90^0, та два різних значення амплітуд. Одне значення амплітуди дорівнює 0, друге значення дорівнює 1, як це зображено на рисунку 1.5. Рисунок 1.5 уявляє собою квадратну матрицю, кожний елемент якої уявляє собою два значення I і Q компонент QAM сигналу, які представлені у вигляді значущих точок в декартовій системі координат $I0Q$.

Координата I є абсцисою точки, а Q - ординату, як це зображено на рисунку 1.6.

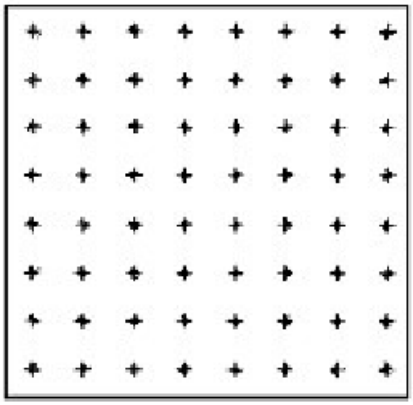


Рисунок 1.6. Структура матриці $I0Q$ $64\,QAM$ модуляції.

З рисунку 1.6 видна діаграма сузір`я і елементи даної квадратної матриці утворюються з горизонтальних та вертикальних відрізків , які з'єднують можливі значення компонент I та Q. Ціле чисельне значення кожної визначеної точки записується в комірку матриці, в яку вона потрапляє. Помилка визначається як вилучення точки, яка була вимірювана з комірки.

Матриці 4х4 відповідає $16\,QAM$, в якій кожна з 16 комірок уявляє одну з 16 можливих бінарних комбінацій. Вертикальне і горизонтальне положення кожної точки відповідає I та Q значенням амплітуди сигналу, який було відправлено протягом одного часового циклу. Матриці 8х8 відповідає $64\,QAM$ модуляція, яку представлено на рисунку 1.6.

Аналіз діаграми сузір`я полягає в в тому, що зовнішній вид значущих точок у комірках квадратної матриці дає ключову інформацію про те, що відбувається під час передачі інформативного сигналу. На рисунку 1.7 представлено діаграму, якій відповідає відношення $сигнал/шум$, при якому потужність завади значно вище по відношенню до інформативного сигналу.

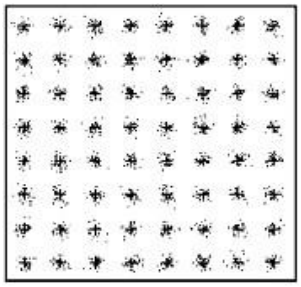


Рисунок 1.7. Потужність завади більше потужності інформативного сигналу

Зображення поки можна розібрати, але, якщо потужність інформативного сигналу буде зменшуватись при зростанні потужності завади, то це призведе до повної втрати картинки. Розпливчасте зображення точки займає практично всю комірку.

На рисунку 1.8 представлено зображення діаграми при наявності шумів інгресії, тобто всі небажані радіочастотні сигнали.

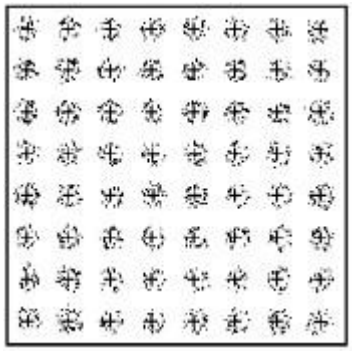


Рисунок 1.8. Зображення діаграми при наявності шумів інгресії

При наявності когерентного шуму у кожній комірці утворюються концентричні зображення.

На рисунку 1.9 представлено діаграму при фазовому зсуві.

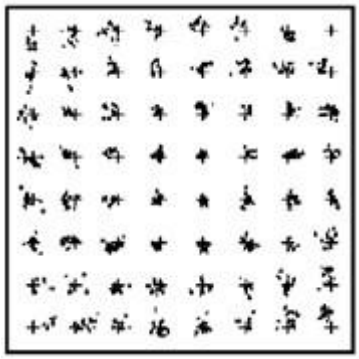


Рисунок 1.9. Фазовий зсув

Фазовий зсув з`являється за рахунок радіочастотних завад, які залишились, що як правило відноситься до головного обладнання. Точки в комірках спотворені таким чином, що виникає візуальний ефект сферичної симетрії відносно центру діаграми сузір`я.

На рисунку1.10 представлено вид діаграми, якій відповідає амплітуда характеристика, яка має нелінійну залежність.

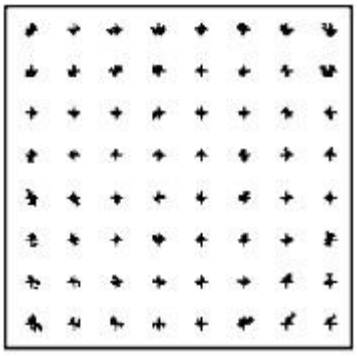


Рисунок 1.10 Не лінійність амплітудної характеристики

Не лінійність амплітудної характеристика виникає у зв`язку з наявності не лінійності проміжних та високочастотних підсилювачів, фільтрів, конвертерів та еквалайзерів. Точки зсунуті відносно центру осередку по осях I та Q, таким чином, що відстань між ними пропорційна відстані осередку від центру діаграми.

На рисунку 1.11 представлено діаграму, якій відповідає нестабільність IQ векторів.

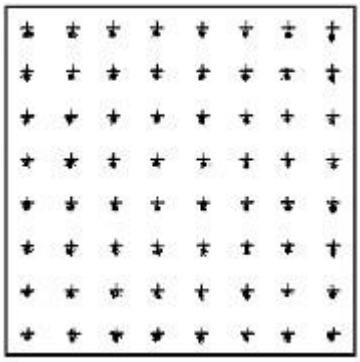


Рисунок 1.11 Нестабільність IQ векторів.

Нестабільність IQ векторів виникає при наявності складності в підсилювачах несучої частоти, фільтрів та цифрових модуляторів головних станцій.

Також виникає ще одна проблема, яка пов`язана з ухиляннням несучої хвилі, як наслідок дисбалансу в змішувачі модулятора або наявності паразитного постійного струму в системі передачі. В цьому випадку всі елементи в комірці діаграми зсунуті в одному напрямку.

Перевага високих значень номера *QAM* - це підвищена швидкість передачі інформативних сигналів, оскільки таким чином більший об`єм інформації в бітах можна передати протягом одного циклу. Однак, в такій спроможності більша кількість значень амплітуди інформативного сигналу розташовуються близько один до одного, підвищуючи тим самим ймовірність не роспізнавання двох значень, що в свою чергу призводить до підвищення чутливості системи до завад. Отже, високі значення номера *QAM* потребують більших вимог до параметрів, які забезпечують необхідне відношення *сигнал/шум*. На рисунку 1.12 представлено відношення параметра *сигнал/шум* до іншого параметру *біт/помилка*.

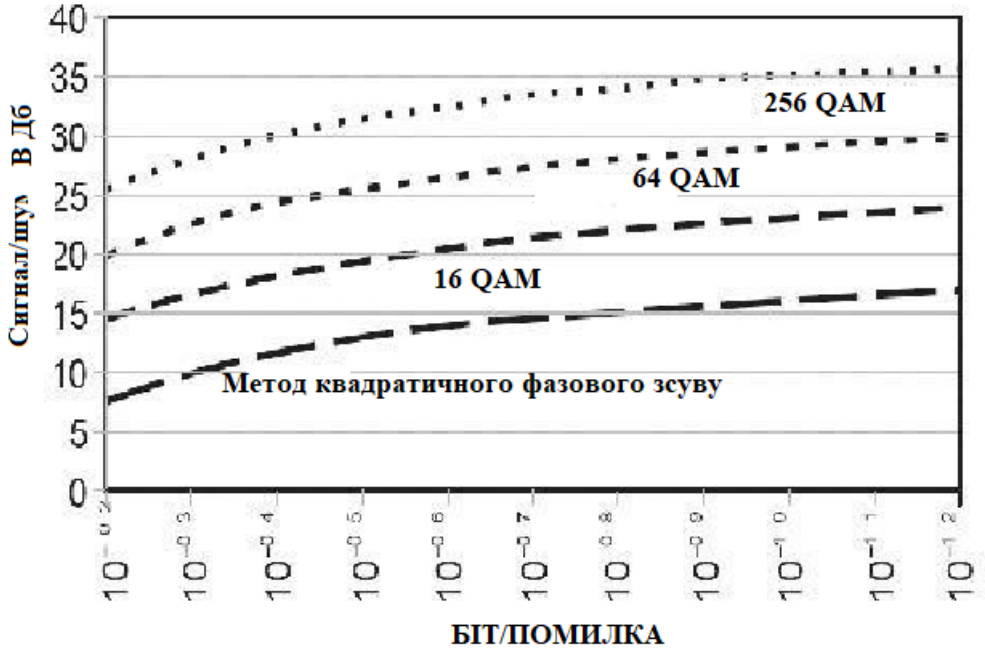


Рисунок 1.12. Відношення параметра *сигнал/шум* до іншого параметру *біт/помилка*

Значення *біт/помилка* визначається як результат підрахунку невірно отриманих бітів об`єму інформації. Інакше кажучи, значення *біт/помилка*

дорівнює значенню відношення числа помилково прийнятих бітів до числа всіх переданих бітів. Одиниця вимірювання даного відношення може бути децибели, але в багатьох випадках одиниця вимірювання береться у форматі 10^{-n}. Тобто, значення 10^{-9} означає, що один помилковий біт був прийнятий при отриманні потоку інформації обсягом в 1 мільярд бітів.

Значення *сигнал/шум* визначається за допомогою технології вимірювання в аналогових пристроях, що працюють у режимах *QAM* або МКФЗ. Оскільки ці режими мають частотний спектр у вигляді білого шуму, то тест на визначення *сигнал/шум* здійснюється шляхом підміни сигналу еквівалентною смугою білого шуму. Ближче до середини смуги цей шумовий фрагмент, як правило чотири мега герців опускається. Коли смуга шуму проходить через пристрій, глибина фрагменту визначається термічним шумом, як це представлено на рисунку 1.13.

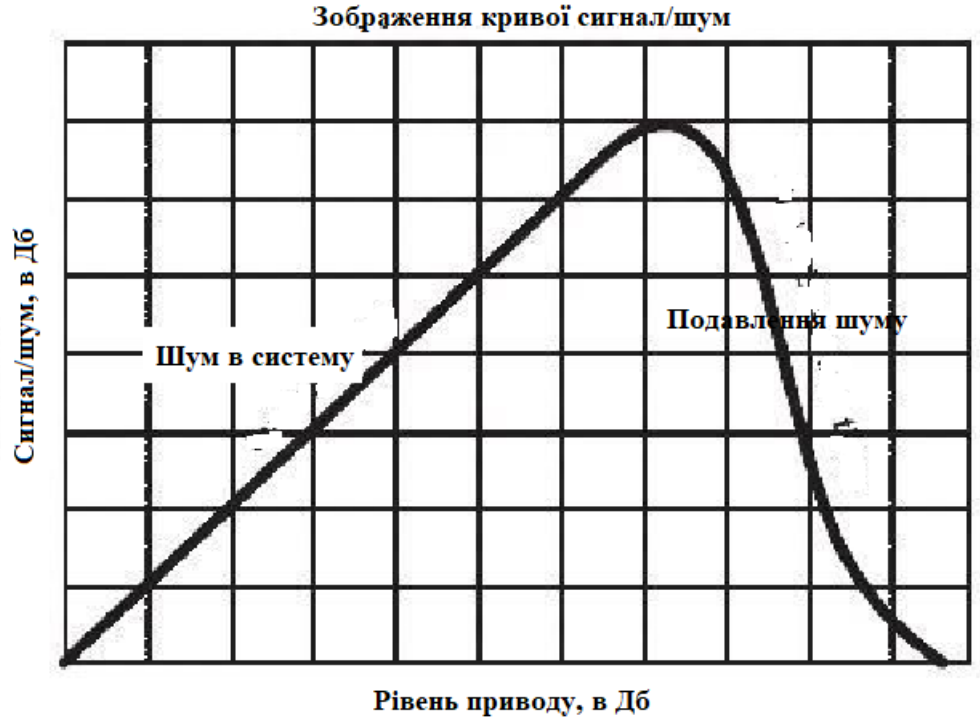


Рисунок 1.13. Вхід завади та її подолання

В даних задачах застосовується так звана попереджувальна корекція помилки (ПКП), яка уявляє собою програмну технологію для визначення та усунення помилок в процесі цифрової передачі інформативних сигналів. Це достатньо складна та достатньо не дешева задача в розумінні потужності процесора, однак

таке завдання є необхідним, а саме здійснювати попередження втрати бітів об`єму інформації, що в свою чергу поліпшує якість діаграми.

На рисунку 1.14 представлено схему визначення *модуляція / помилка* , яка собою уявляє величину відхилення отриманої модуляції за амплітудною та фазною від модуляції, яка була передана.

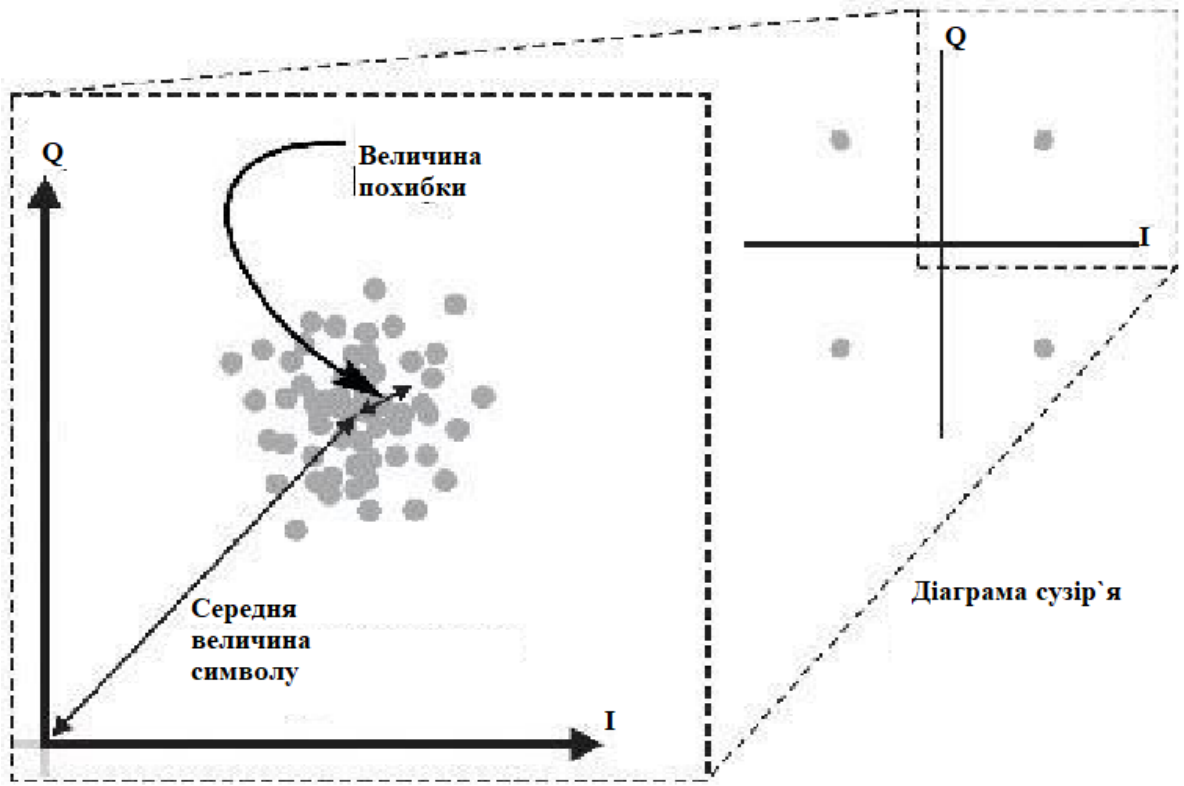


Рисунок 1.14. Схема відношення *модуляція / помилка*

При збільшенні *модуляція / помилка* до такого значення, при якому точки потрапляють на межі комірки або за її межами, то *біт / помилка* зростає з достатньо великою швидкістю. При умові, коли *біт / помилка* досягає значення, яке більше за значення ПКП, то відбувається збій передачі інформативного сигналу. Дослід показав, що на точці зриву, якість діаграми ще залишається відмінною, і при цьому ще не відомо щодо зриву. Це явище має назву " *ефект зриву* ". Даний ефект викликає складність для несподіваного моменту часу, коли за діаграмою не можливо визначити час зриву.

Так як модуляція уявляє собою процес кодування даних на несучій хвилі, то стандарт 11*n* обмежений 64 *QAM* -модуляцією. На відміну від стандарту 11*n*

стандарт 11*ac* підтримує модуляцію 256 *QAM* . Модуляція 256 *QAM* уявляє собою більш складнішою з існуючих типів модуляції, так як вона потребує значно більш потужного сигналу по відношенню до шуму. Виходячи з вищевикладеного, можна зробити висновок, що в багатьох випадках з'єднання користувач - точка доступу застосовують 64 *QAM* на відстані дванадцять – п`ятнадцять метрів. На рисунку 1.15 праворуч представлено комбінацію 64 *QAM* , при умові, що кожна точка уявляє собою 6 *біт* . У комбінації 256 *QAM* точки на квадрант, а в кожній точці кодується 8 *біт* .

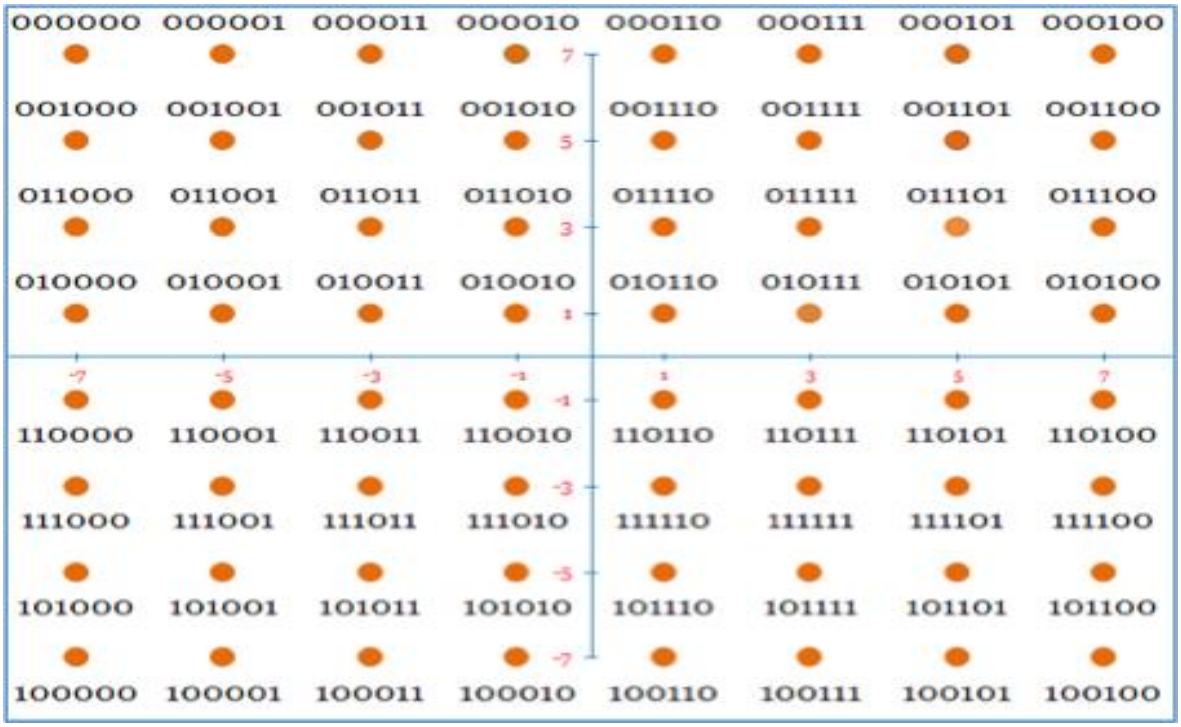


Рисунок 1.15. Комбінація 64 *QAM* - праворуч, 256 *QAM* - ліворуч.

Значно більші значення *MCS* стандарту 11*ac* отримуються при застосуванні модуляції 256 *QAM* . Однак процес подвоєння ширини каналу призводить до збільшення базового рівня шуму до трьох децибел, що призводить до того, що базовий рівень шуму каналів 80 мега герц автоматично збільшиться до шести децибел, в порівнянні з каналами 20 мега герц. На рисунку 1.15 представлено таблицю, в якій видно, що для досягнення найвищого показника *MCS* стандарту 11*ac* для каналу 80 мега герц необхідно, щоб відношення *SNR* , було як найменше в 37 децибел. Це критично високе значення *SNR* , а без достатнього повторного використання каналу перешкоди від вільного

використання каналів будуть вельми значними. На рисунку 1.16 представлено зіставлення рівнів MCS з необхідним значенням SNR.

MCS Value Achieved by Clients at Various Signal to Noise Ratio Levels (SNR)

Protocol	Channel	1	2	3	4	5	6	7	8	9	10
802.11b	20MHz	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1
802.11a/g	20MHz	None	MCS 0	MCS 0	MCS 1	MCS 2	MCS 2	MCS 2	MCS 2	MCS 3	MCS 3
802.11n	20MHz	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2
802.11n	40MHz	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1
802.11ac	20MHz	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2
802.11ac	40MHz	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1
802.11ac	80MHz	None	None	None	None	None	None	None	MCS 0	MCS 0	MCS 0
802.11ac	160MHz	None	None	None	None	None	None	None	None	None	None

	SNR in dB	11	12	13	14	15	16	17	18	19	20
802.11b	20MHz	MCS 2	MCS 2	MCS 2	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 4	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 5	MCS 6	MCS 6	MCS 7
802.11n	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6
802.11n	40MHz	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4
802.11ac	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6
802.11ac	40MHz	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4
802.11ac	80MHz	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3
802.11ac	160MHz	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MCS 3

	SNR in dB	21	22	23	24	25	26	27	28	29	30
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8
802.11ac	40MHz	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7
802.11ac	80MHz	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6
802.11ac	160MHz	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6	MCS 6

	SNR in dB	31	32	33	34	35	36	37	38	39	40
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	40MHz	MCS 7	MCS 8	MCS 8	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	80MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	160MHz	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8	MCS 9

	SNR in dB	41	42	43	44	45	46	47	48	49	50
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	40MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	80MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	160MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9

Modulation Key

None = Grey

BPSK = Red

QPSK = Orange

16-QAM = Yellow

64-QAM = Blue

256-QAM = Green

802.11 Type Key

802.11b

802.11ag

802.11n

802.11ac

Рисунок 1.16. Зіставлення рівнів MCS з необхідним значенням SNR.

1.3. Переваги технології IEEE 802.11 ac

В типових корпоративних розмежувань $Wi-Fi$ обладнання користувачів застосовують в середньому не більше п`ять мега біт в секунду. Звісно, для споживачів можливі бути такі ситуації, коли пікова пропускна спроможність суттєво вища за сто мега біт в секунду, але всього не велика частина пристроїв споживачів $Wi-Fi$ підтримують високу пропускну спроможність протягом тривалих періодів часу. Це означає, що більшість сучасних розгортань $11n$ в багатьох випадках комутують з офісним середовищем, яке має низьку щільність, а також подібні розгортання. Рентабельність інвестицій в застосуванні технології $11ac$ залежить від модернізації пристроїв споживачів $11ac$ та оптимізації проекту, який створено для розгортання та конфігурації мережі $Wi-Fi$. Показники якісно оптимізованої мережі $11n$ $3x3:3$ можуть мати більш високу якість по відношенню до погано спроектованого розгортання $11ac$ $3x3:3$ з аналогічною встановленою базою пристроїв споживачів.

Згідно свого призначення технологія $11ac$ себе проявляє з гарантованою модернізацією інфраструктури в середовищах високої щільності та з достатньо високою пропускною спроможністю, таких як спортивні арени, амфітеатри, великі аудиторії, розважальні зали, стадіони, та інші. На рисунку 1.17 представлено приклад такого середовища.

Рисунок 1.17. Приклад середовища для успішного застосування $11ac$

11ac мають радіомодуль більш вищої якості, що дає кращу швидкість реакції, кращі процесори і підтримують нові можливості. Також, пристрої 11ac «Хвилі - 2» обіцяють підтримати ефективність MAC, використовуючи MU-MIMO в невеликих середовищах і середовищах мобільних пристроїв.

Одним із головних аспектів розгортання 11ac, являється спільне існування з будь-якими різними точками доступу 11n.Існують наступні рекомендації:

- точки доступу 11ac слід розміщувати в областях з високою щільністю або високою пропускною здібністю, а точки доступу 11n – в областях з низькою щільністю або пропускною здібністю.

Також, можемо спостерігати ряд точок доступу, які використовують широкі канали. Саме, це дозволяє ефективно використовувати спектр, а також задовольняти високу пропускну здібність в окремих областях. Потрібно пам'ятати, що дані пристрої, навіть від одного виробника можуть підтримувати різні набори функції із за обмеження процесора. Це означає, що дані можливості можна реалізувати тільки в визначених областях, що і приводить до обмежень. Наприклад, потрібно ізолювати друг від друга пристрої 11n і 11ac, розмістить їх в різних будівлях або на різних площадках.

Висновки до розділу 1

Дана технологія базується на амплітудно-квадратичній модуляції яка перетворює аналоговий сигнал в цифровий. Це дає можливість створювати криптографічні протоколи для захисту інформації яка приймається, передається та обробляється.

РОЗДІЛ 2 ЗНИЖЕННЯ ШУМІВ ІНГРЕСІЇ

Шуми інгресії , тобто внутрішні наводки, можуть створювати багато проблем, наприклад перезавантаження лазерів зворотного каналу. Коли відбувається сумування шумів інгресії, то спостерігається деяка фазова кореляція даних шумів, тому сумування уражених сигналів інгресії, що надходять з двома потоками, призводить до зниження загального співвідношення S/N більше ніж на три децибел. Якщо б кореляція між шумами не було, то інтеграція, як і звичайний шум, при сумуванні добавляла в знаменник три децибел. Якщо відбудеться сто відсотків збігу, інгресії склалася як напруга, і збільшення шуму склало б шість децибел .

На практиці, можемо спостерігати, що реальна величина шумової добавки змінюється в межах від 13 до $17 \lg 2$. C/N при цьому знижується на 3,9-5,1 децибел.

Таблиця 2.1.

Величина шумової добавки

Два сигнали з однаковою амплітудою	**Значення суми**
20lg2	6 Дб
18lg2	5,4 Дб
17lg2	5,1 Дб
16lg2	4,8 Дб
15lg2	4,5 Дб
14lg2	3,9 Дб
13lg2	3,6 Дб

На практиці, спостерігаємо, що більше 80% шумов інгресії проникають у мережу через розведення у будинку абонента. Зазначимо, що більша частина інгресії з'являється в результаті застосування підсилювачів, дільників, роз'ємів та коаксіальних кабелів, призначених для самостійної установки абонентом.

Дані компоненти характеризуються низьким рівнем екранування, наприклад у коаксіальних кабелях становить від 25 до 40 децибел. При підключенні телевізорів, роз'єми IEC мають слабке екранування і являються джерелом шумів інгресії.

Коли, відбувається створення заходів боротьби із інгресією, то слід використати наведені рекомендації. Для того, щоб створити якісно розведення в будинку абонента, потрібен доступ до абонента, зазвичай він надається, тоді коли абонент підписується на інтерактивні послуги. Але більшість квартир та приватних домів залишаються недоступними. Тому, на відведених до даних абонентів рекомендується застосовувати фільтри, що відсікають смугу зворотного каналу.

З технічної точки зору, дане рішення добре підходить до застосування, але встановлення тисяч таких фільтрів потребують великих вкладень, а при підключені їх до інтерактивних послуг фільтри доводиться просто викидати. Отже, рекомендується використовувати спосіб боротьби, який не потребує періодичних змін.

Розглянемо, більш детально абоненське розведення. У більшості передплатників наявні два телевізори, які самостійно підключені ними через спліттер та коаксіальний кабель (рис. 2.1).

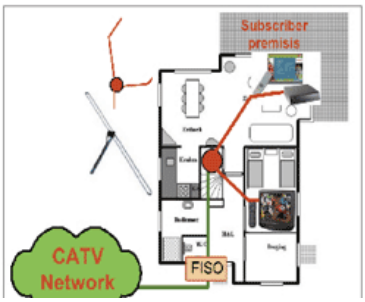


Рисунок 2.1. Розведення користувачів

Через низький рівень екранування дроти та спіттери, дана конструкція, уявляє собою дипольну антену для прийому шумів інгресії, які спрямована в зворотній канал *СКТВ*.

2.1. Джерела інгресії

Розглянемо всі небажані радіочастотні сигнали. Серед них, виділимо:

— перешкоди, створювані *ПЧ* сигналами телевізора, радіо чи відеомагнітофона (10,7 / 38,9*Мгц*);

— перешкоди діапазону цивільного зв'язку (27*МГц*);

— радіо *КВ* діапазону;

— побутові пристрої (пилососи, кухонна апаратура, фени тощо).

Даний список, являється не повним. Загальною особливістю, являється, те що одне джерело інгресії вражає одночасно і спліттер, і різні гілки коаксіального

кабелю, тобто шуми, що приходять з різних гілок, будуть корелювати за частотою та фазою. Довести їх часткову кореляцію легко. Коли, відбувається проникнення в мережу, *КВ* радіо, як перешкода, то він вражає всі абонентські відводи. Також, це можна спостерігати і в тих випадках, коли частина абонентів знаходиться недалеко від антени, що передає.

2.2. Кореляція по фазі

Розглядаючи, хвилю близьку до стоячої, то в точці влучення хвилі в кабельну мережу її фронт близький до прямої лінії (рис. 2.2).

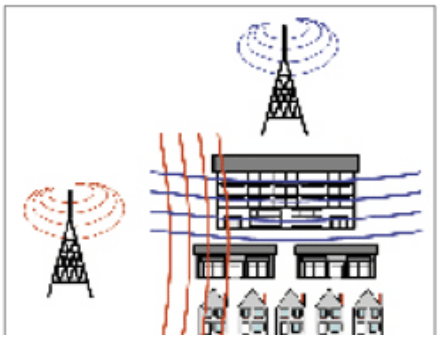


Рисунок 2.2. Хвиля наближена до стоячої

Розглянемо, відстань між двома поверхами близько трьох метрів, а між двома сусідніми приватними будинками близько десять метрів. Тому, сигнал у всі три точки приходять з невеликою різницею в одній фазі. Фазове рознесення, що додатково вноситься за рахунок різниці в довжині абонентських відводів, мінімальний. Далі, в таблиці навели фазові зрушення, зумовлені різницею у частоті сигналів та довжині кабельних відводів. Дані наведені для кабелю, що поширює сигнал зі швидкістю $0{,}67 \cdot c$, де c - швидкість світла.

Таблиця 2.2.

Фазові зрушення

Частота	**Довжина хвилі**	**Різниця в довжині кабельних відводів**							
(МГц)	(М)	3	4	5	6	7	8	9	10
5	60	12°	16°	20°	24°	28°	32°	36°	40°
10	30	24°	32°	40°	48°	56°	64°	72°	80°
15	20	36°	48°	60°	72°	84°	96°	109°	121°
20	15	48°	64°	80°	96°	113°	129°	145°	161°

З результатів дослідження бачимо, що при різниці між довжиною відводів в один метр частотне рознесення сигналів на $10 МГц$ створює фазовий зсув наближено до 8^0, а частотний розмах на $20 МГц$ створює зсув наближено на 16^0.

2.3. Структура розгалужувача

На рисунку 2.3 зображено стандартний розгалужувач, що застосовується в *СКТВ* , має один загальний порт і два або більше портів для введення/виведення окремих гілок. Саме, вони являються виходами для сигналів прямого каналу і одночасно виходами для зворотного каналу. Отже, *сплітер* працює, зокрема, як суматор шумів інгресії.

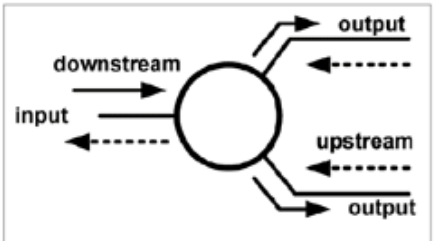


Рисунок 2.3. Стандартний розгалужувач

На рисунку 2.4 зображено роботу *сплітеру* як суматора перешкод. Так як перешкоди на обидва входи надходять з одного джерела, їх частота, рівень і фаза

приблизно однакові, і їх сума перевищить кожен з вихідних сигналів приблизно на шість децибел.

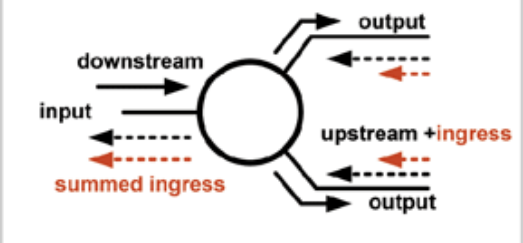


Рисунок 2.4. Роботу *сплітер* як суматора перешкод

Щоб вирахувати рівень *РЧ* сигналу за напругою, можемо використати:

$$V = V_{top} \cdot \sin(2\pi ft). \tag{2.1}$$

В результаті, ми маємо розгалужувач із двома однаковими сигналами на входах зворотного каналу. Отримаємо:

$$f_1 = f_2,\ V_{top1} = V_{top2},\ \omega f_1 = \omega f_2, \text{ при } \varphi_1 \neq \varphi_2. \tag{2.2}$$

Тоді, сума даних сигналів має наступне представлення

$$V = V_{top1} \cdot \sin \omega t + V_{top2} \cdot \sin(\omega t + \varphi). \tag{2.3}$$

При $\varphi = 0^0$ відбувається операція суми двох сигналів, а при $\varphi = 180^0$ обидва сигнали додаються в проти фазі, тобто сума буде дорівнювати нулю.

2.4. Векторне представлення

Виконавши обчислення, можемо зобразити графічно, у формі векторного представлення сигналу *РЧ* (рис. 2.5)

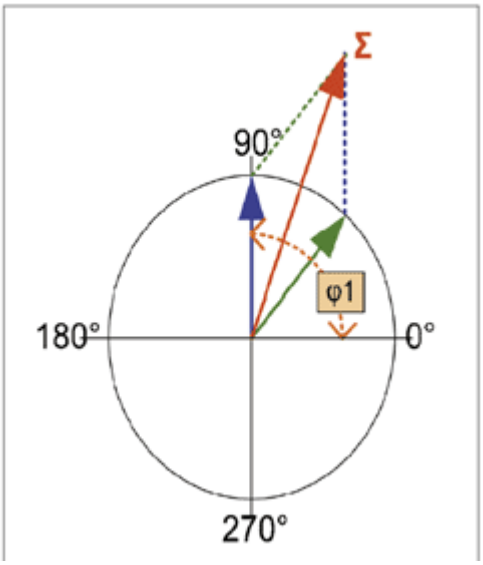


Рисунок 2.5. Векторного представлення сигналу $РЧ$

Вектор одного сигналу інгресії, що зображено синім кольором, має фазовий кут 90^0, а другий сигнал, який зображено зеленим кольором, має фазовий кут 45^0. Результатуючий вектор суми цих сигналів зображена червоним кольором.

$$V_1 = 1B,\ V_2 = 1B,\ \varphi_1 - \varphi_2 = 45^0,\ \sum = 1{,}414\,B. \qquad (2.4)$$

На рисунку 2.6 зображені сигнали, але синій вектор зрушений по фазі на 180^0, тобто фазовий кут між сигналами інгресії становить 270^0 замість 90^0. Сума сигналів , що зображено червоним кольором, при цьому значно менша:

$$V_1 = 1B,\ V_2 = 1B,\ \varphi_1 - \varphi_2 = 225^0,\ \sum = 0{,}7B. \qquad (2.5)$$

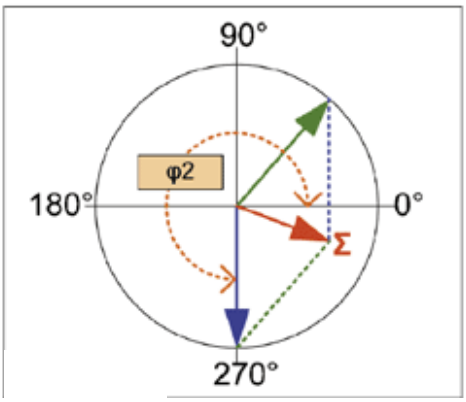
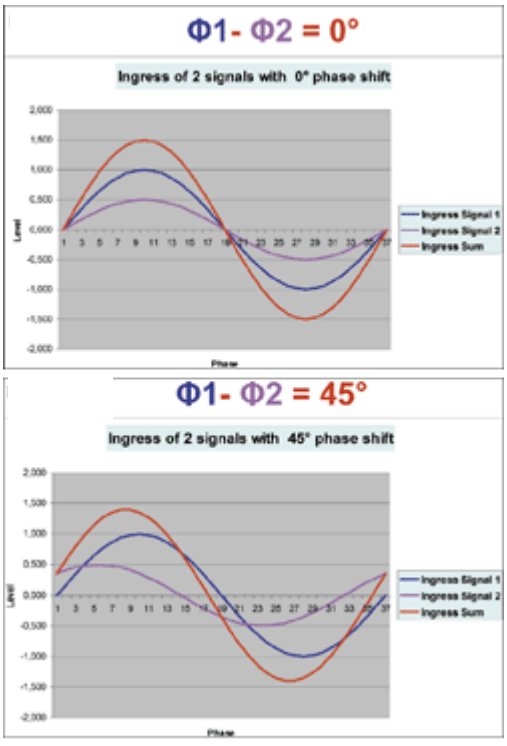


Рисунок 2.6. Сигнали інгресії

В результаті, отримаємо фазову інверсію сигналу, яка призведе до зменшення рівня сумарного шуму вдвічі. Застосовуючи, дані знання на практиці, маємо, що шуми інгресії на двох сусідніх входах розгалужувача будуть також корелювати за фазою та частотою, але рівні сигналів будуть різними.

Далі, на рисунку 2.7 наведемо приклади підсумування сигналів з різними амплітудами $V_1 = 2B$ та $V_2 = 0.5B$ та різними фазовими розносами. Якщо фаза одного із сигналів не зсунута на 180^0, то значення сумарного сигналу завжди більший.



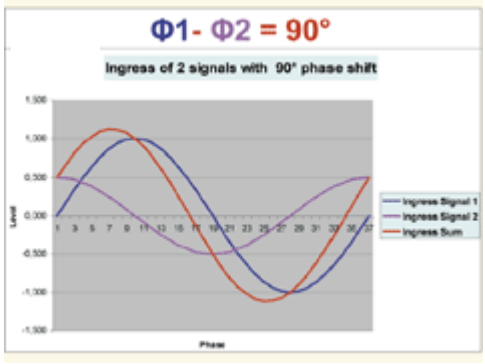


Рисунок 2.7. Приклади підсумування сигналів з різними амплітудами

Виняток становить випадок, зображений на рис.2.8 де сигнали інгресії на виході мають рознесення в 180^0 .

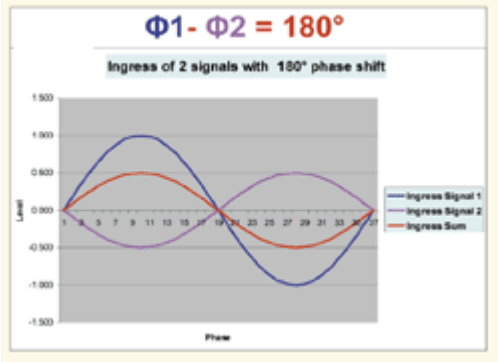


Рисунок 2.8. Виняток

Висновок до розділу 2

В результаті аналізу шумів інгресії, які впливають на системи можна отримати схему практичної реалізації фазової інверсії, яку представлено на рисунку 2.9.

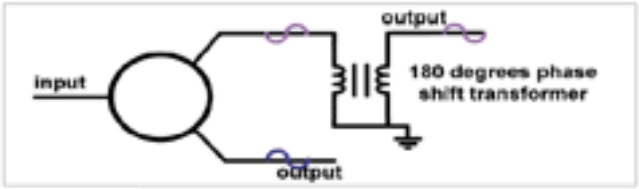
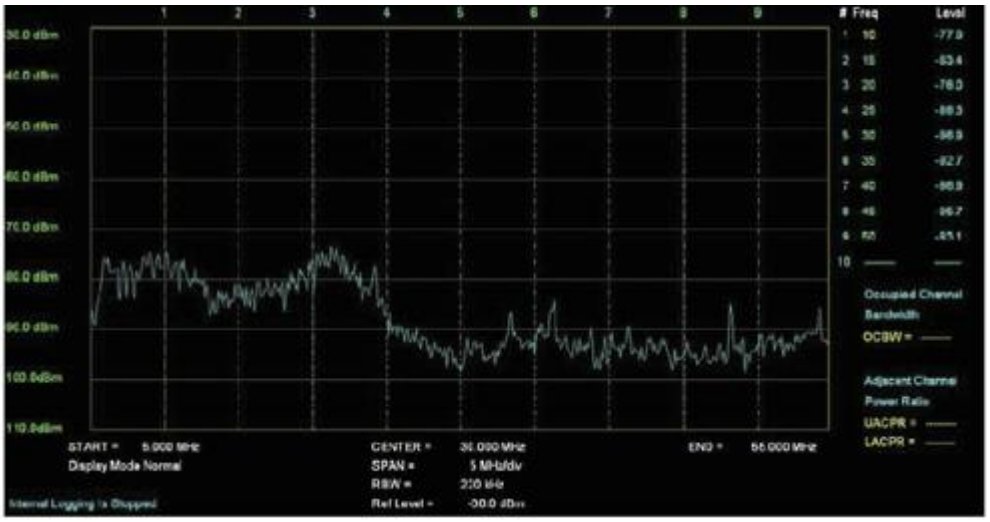


Рисунок 2.9. Практична реалізація фазової інверсії

В одному з портів двовихідного *сплітеру* встановлюється широкосмуговий трансформатор. Якщо шуми інгресії, що надходять на обидва порти, мають

спільне джерело, теоретично фазова інверсія одного їх сигналів повинна їх взаємно знищити. Але якщо через такий розгалужувач підсумовуються сигнали від двох кабельних модемів або *STB*, то на них інверсія ніяк не відіб'ється, оскільки вони не корелюються ні фазою, ні частотою. Не позначатиметься вона і на сигналах прямого каналу, що розгалужуються.

Дана технологія може бути інтегрована в пасивні пристрої будь-якого роду, а вже наявні інсталяції можна додавати зовнішні фазові інвертори сигналу. На наступних рисунках зображено екран спектрального аналізатору, що вимірює випадкові шуми інгресії.



На рисунку 2.10 до спектрального аналізатору підключено вхід звичайного розгалужувача. До одного з його портів підключено провід, який, працюючи як антена, набирає шуми інгресії.

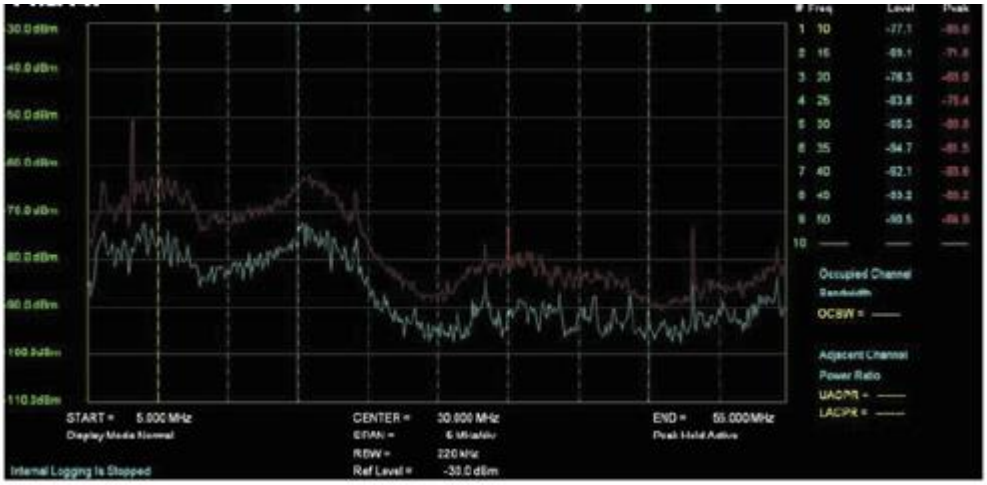


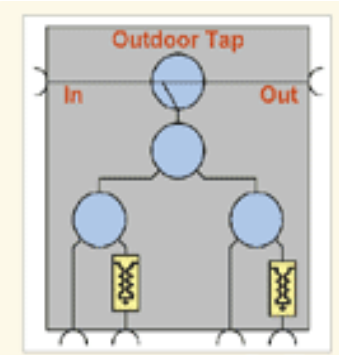
Рисунок 2.10. Екран спектрального аналізатору, що вимірює випадкові шуми інгресії.

Також, на рисунку 2.11 та 2.12 зображено підключення до приладу того самого розгалужувача, але відрізки кабелю, що набирають інгресію, підключені до двох портів.

Якщо, порівнювати червону криву, яка зображена на рисунку 2.10 із блакитною кривою на рисунку 2.12, то можемо зробити висновок, що рівень сумарної інгресії в останньому випадку більш, ніж на тридцять децибел нижче, ніж при використанні звичайного *сплітеру*. Дані, вимірювання виконувалися в ситуації, яка близька до ідеальної. За допомогою статистичних даних є можливість спостерігати, що реальні виміри технології *Ingress Safe@* покращує рівень C/N приблизно на шість децибел. Схожу ситуацію, можемо спостерігається в коаксіальному кластері, що поєднує близько тисячі абонентських відводів. Ефект від фазової інверсії вищий, чим більший частотний і фазовий збіг двох шумових сигналів, то розгалужувачі з *Ingress Safe@* слід встановлювати прямо у абонентів або в максимальній близькості до їхніх будинків.

Втрати *Ingress Safe@* становлять близько $0{,}4дБ$, а втрати на зовнішніх фазових інверторах – близько $0{,}5дБ$. Втрати $0{,}5дБ$ на 50% компенсуються перевагою C/N в шість децибел у ста відсотків абонентських підключень.

На рисунку 2.13 зображена схема двох вивідних та чотири вивідних відгалужувачів з інтегрованою системою *Ingress Safe@*.



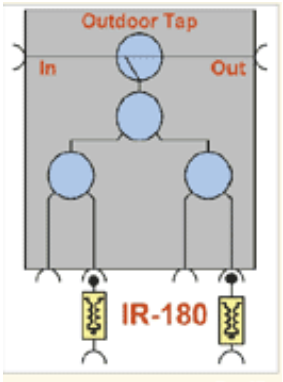


Рисунок 2.13. Схема двох вивідних та чотири вивідних відгалужувачів з інтегрованою системою *Ingress Safe@*

На рисунках 2.14 та 2.15 зображені, *сплітер*, інтегрований з *Ingress Safe@*, і зовнішній інвертор фази.

Рисунок 2.14. *сплітер*, інтегрований з *Ingress Safe@*

Рисунок 2.15. Зовнішній інвертор фази

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ СТАНДАРТУ IEEE 802.11 ac В Wi-Fi МЕРЕЖАХ

Зазвичай, виробники корпоративних пристроїв *Wi Fi* спочатку випускають високоякісні точки доступу при застосуванні нових технологій, щоб зацікавити нових клієнтів. Для того, щоб працювали точки доступу першого покоління застосовують 802.3*at*(*PoE+*). Зазвичай, мало часу проходить, перш ніж виробники інфраструктури *WLAN* випускають менш потужні точки доступу, які працюють на повну потужність у середовищах 802.3*at*(*PoE+*), а потім точки доступу в середній ціновій категорії, які навряд чи впишуться до бюджету.

Дана стратегію застосовували для запуску продукту 11*n* та 11*ac* для першого етапу.

Саме, точки доступу 11*ac* етапу 2 пропонують кращі можливості. По-перше, це підтримка чотирьох просторових потоків 4*SS*. Саме 4*SS* означає, що одночасно доступні чотири радіо ланцюги для передачі та прийому. Це дасть можливість збільшити швидкість, але збільшиться рівень енергозатрати. По-друге, це просор і пам’ять. Завдяки, 4*SS* ми можемо переміщувати велику кількість даних, тому потрібно швидкий процесор і більший об'єм пам'яті, щоб досягти потенційну пропуску здібність точки доступу. Процесори є основним джерелом споживання електроенергії у точці доступу.

802.3*at*(*PoE+*) розвивався повільно, на відміну від 11*ac* . На теперішній час для 802.3*at*(*PoE+*) з'явилися різні стимулюючі фактори. Також, бюджет для даної технології не високий. Потрібно врахувати, що пропускна здатність точок доступу становить п`ятдесят відсотків швидкості передачі даних. Для розрахунку в оптимальному схемотехнічному вирішені та з урахуванням обох

кінців з'єднання, так як це пристрої $11ac$ ми можемо використовувати такі показники:

$$80МГц \cdot 4SS \cdot 256QAM + SGI = 1{,}733\ Гбіт/с - швидкість\ передачі\ даних \cdot 0{,}5 \approx 867Мбіт/с$$

Gigabit Ethernet уявляє собою повно дуплексну технологію, яка спроможна одночасно переміщувати дані зі швидкістю один гіга біт в секунду у висхідному та низхідному потоці. І навпаки, при розрахунку швидкості 867 мега біт в секунду вище не беруться до уваги будь-які радіоперешкоди і передбачається, що існує лише один клієнт, який взаємодіє з однією точкою доступу, тобто без перевантаженості. Тому такі показники здаються нереальними.

Після зростання попиту на соціальні мережі, вхідний/вихідний трафікв більшості мережах відноситься п`ятдесят на п`ятдесят. Однак при двох направленій передачі точка доступу конкуруватиме з власним клієнтом, а процес конкуренції 802.11 викликатиме накладні витрати (колізії, додаткові перемикання тощо). Тому, реалістичне передавання може становити менше чотириста мега біт в секунду в кожному напрямі.

В реальних умовах, даний показник досягти важко із за наступних показників:

- конкуренція кількох клієнтів при доступі до каналу;
- перешкоди сусідніх каналів (ACI);
- джерел радіоперешкод;
- механізми захисту для зворотної сумісності;
- змішані клієнтські середовища PHY чи бездротова інфраструктура;
- обмеження процесора у точці доступу;
- неефективний код у точці доступу чи контролері;
- погані клієнтські драйвери.

Даний список являється неповним, існує багато технічних питань, які можуть призвести до зменшення продуктивності. За наявності близько тридцять клієнтських пристроїв і всім спектром можливостей $11n$ та $11ac$, пов'язаних з точками доступу $4X4:4$ $11ac$ етап 2 тобто двох діапазонні з радіо модулем $11n$

2,4 гіга герц загальна пропускна здатність у реальних розгортаннях таких як сорок мега герц $3SS \cdot 64QAM + SGI$ може змінюватись від ста до двохсот мега біт в секунду, у кращому випадку, для обох радіо модулів. Пропускна здібність повністю залежить від використання клієнтами. Пам'ятайте, що навіть один клієнт $11a$, $11b$ чи $11g$ може обмежити можливості точки доступу.

Деякі виробники пристроїв $WiFi$ почали розробляти точки доступу $11ac$ з двома радіо модулями і частотою п`ять гіга герц в секунду, про те ще не підтверджено, що два такі модуля можуть співіснувати без значної втрати пропускної спроможності через перешкоди сусідніх каналів ACI. Якщо є можливість вирішити дану проблему, то така конфігурація серйозно обмежить вибір налаштування каналів. Якщо два, або більше таких радіомодулів зможуть співіснувати без ACI, тоді ми могли б ефективно використовувати лінію зворотного з'єднання один гіга біт в секунду.

На сучасному ринку, де точка доступу оснащена одним радіомодулем три на три $11ac$ з частотою п`ять гіга герц в секунду та одним радіомодулем три на три $11n$ з частотою ГГц, найвища пропускна здатність, яку можна розглядати - близько чотириста мега біт в секунду для висхідного та низхідного потоку для модуля $11ac$ п`ять гіга герц та додаткові сорок мега біт в секунду для висхідного та сорок мега біт в секунду для низхідного потоку для модуля $11n$ $2,4Гц$. В кращому випадку, це буде становити п`ятдесят відсотків від пропускної здібності лінії один гіга біт в секунду.

У стандарті 802.11 через конкуренцію клієнтів, підключених до точки доступу джерела перешкод модульованих та немодульованих для обох смуг, і через використання каналів сорок мега герц замість вісімдесят мега герц, розрахована двовекторна пропускна здатність чотириста сорок мега біт в секунду швидко може скоротитися на п`ятдесят відсотків чи більше у кожному напрямі.

3.1. Розгортання мереж IEEE 802.11 ac

Якщо ви, вирішили перейти на нову мережу, то у вас буде два варіанти: нова мережа чи оновлена. З урахуванням того, що мережа $WiFi$ має широке

поширення, то біль всього ви будете встановлювати оновлення. Також, можете зіткнутися із тим що минув термін експлуатації наявного устаткування.

Деякі мережеві адмінстратори, не враховують значимість перехода від старої системи з одним входом і одним виходом , тобто *SISO* до системи з кількома входами і виходами *MIMO*. Дані типи систем сильно відрізняються, а розгортання 11*n* чи 11*ac* в якості заміни попередніх систем повинно супроводжуватися новим проектуванням, дослідженням та перевіркою мережі. Оскільки точки доступу 11*ac* стоять практично так, як точки доступу 11*n* для аналогічних специфікацій, перехід від застарілих точок доступу до 11*ac* добре обгрунтований з фінансової точки зору. Перехід від системи 11*n* до 11*ac* потребує проектування, вивчення та перевірки. Якщо проект 11*n* був оптимізований, можливо, що багато з точок доступу можна використовувати знову, якщо щільність клієнтів і потрібна пропускна здатність (через вимоги додатка) залишилися приблизно такими ж. Якщо спостерігається значне збільшення клієнтів чи потрібної пропускної здібності, то рекомендується виконувати проектування знову. Якість радіозв'язку 11*ac* в багатьох випадках значно краща, ніж радіомудулей 11*n*, тому можить знадобиться скоригувати налаштування точки доступу.

Коли точка доступу 11*ac* етапу 2 заміняє точку доступу 11*ac* етапу 1 уявляє собою зміну виробника інфраструктури *WiFi*. Якщо організація не має змого виконати заміну обладнання, то з часом буде виконано «поступове оновлення».

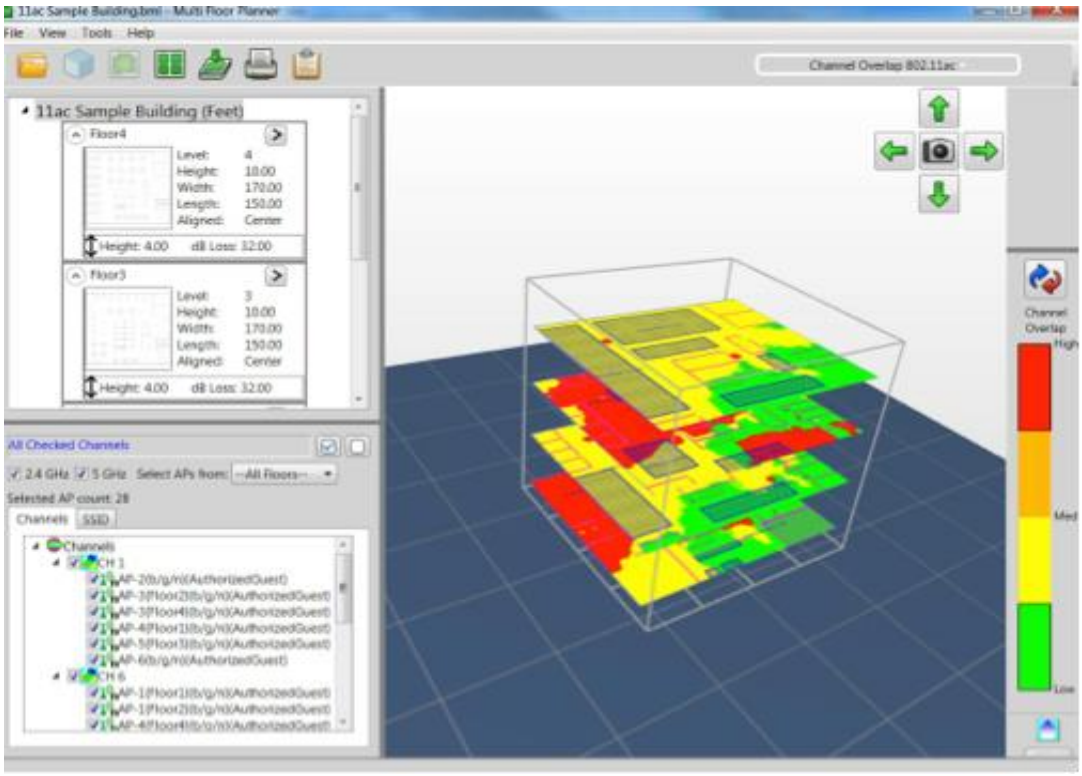
Поступово оновлення призводять до того, що клієнти одночасно використовують різне обладнання стандартів 11*n* чи 11*ac*. Рекомендуємо, розділити різні системи, а потім помістити точки доступу 11*ac* в розташуваннях, де потрібна висока щільність/висока пропускна здатність.

Якщо клієнтами являються не тільки комп'ютери та мобільні пристрої, а і наприклад інфузійні насоси в закладах охорони здоров'я, касові апарати в роздрібній торгівлі та промислові сканери-пістолети на складах, тоді інфраструктура 11*ac* не буде мати багато переваг.

3.2. Інструменти планування та діагностики

Мережа Wi-Fi, потребує точної оцінки вимог та обмежень замовника. Далі, потрібно виконати прогнозуюче модулювання. Чим більша точність, тим вище буде її продуктивність після встановлення. Продукти AirMagnet Planner та Survey Pro компанії Fluke надають інженерам бездротових мереж інструменти для ефективного і точно моделювання та оцінки здатності виконання необхідних вимог до охоплення, пропускної спроможності та мобільності мережі.

За допомогою, Fluke AirMagnet Planner можна моделювати та використовувати, такі функції, як калібрування карти, втрати від стін, 2D- та 3D-візуалізація, моделювання для багатоповерхових будівель, області згасання, виключені області та аналіз повного набору параметрів точок доступу та антен. Всі функції налаштовуються, при цьому підтримують широкий спектр формата карти, у тому числі CAD-файли.



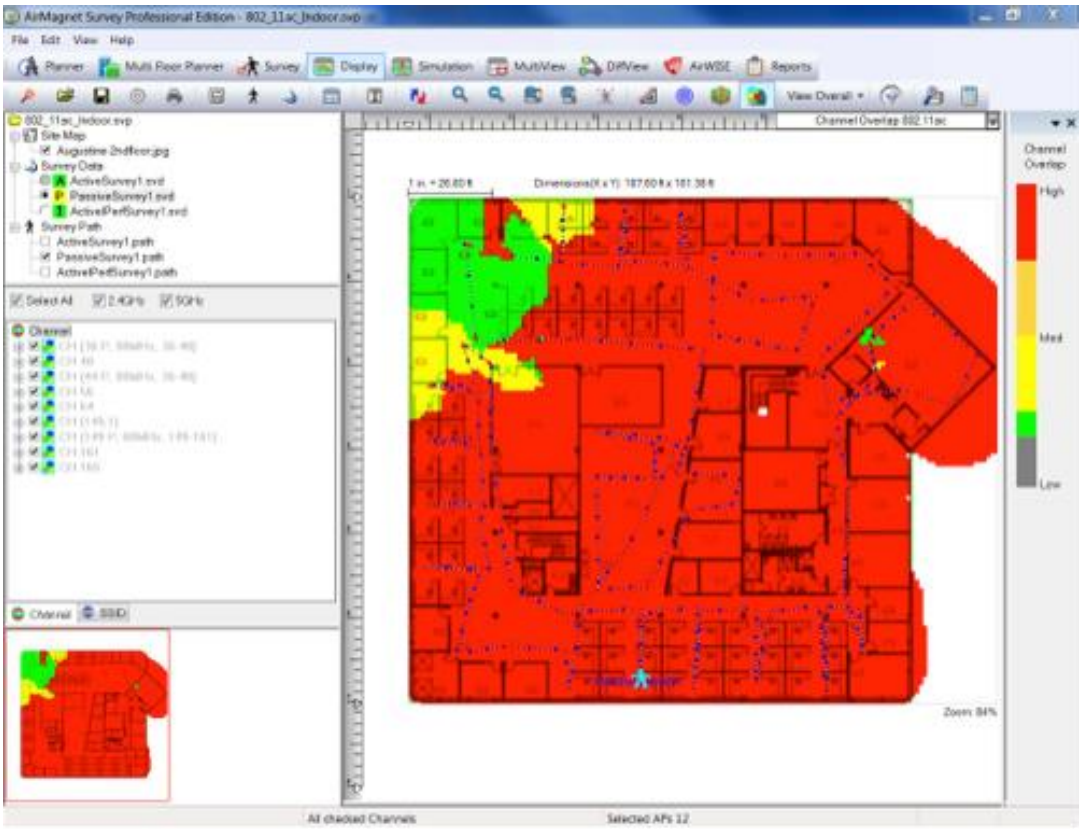


Рисунок 3.1. Інструменти AirMagnet Planner і Survey PRO

Площадка, яка підтримує клієнтів 802.11ac, потрібно використовувати адаптер 802.11ac для точного картування і перевірки перевірки тих областей, де будуть використовуватися нові рівні швидкості передачі даних і ширини каналу. Це схоже на рекомендації по використання смарт-пристроїв для збору даних, якщо в даному середовищі будуть застосовуватися клієнські смарт-пристрої.

Інструменти діагностики, які підтримують лише стандарт 802.11n, можуть усунути деякі проблеми в мережах 11ac (більшість керуючих та контролюючих кадрів відправляються за стандартом 802.11g/n (2,4 ГГц) або 802.11a (5 ГГц)), для отримання повного уявлення про мережу та її продуктивність необхідно обладнання та інструменти для діагностики з підтримкою 802.11ac, наприклад AirMagnet WiFi Analyzer. Вимоги щодо використання чіпсету 11ac у діагностичних інструментах найчастіше пов'язані з тим, що такий чіпсет підтримує тип модуляції (VHT), який використовується для кадрів модульованих даних і каналів шириною 80 або 160 МГц стандарту 11ac.

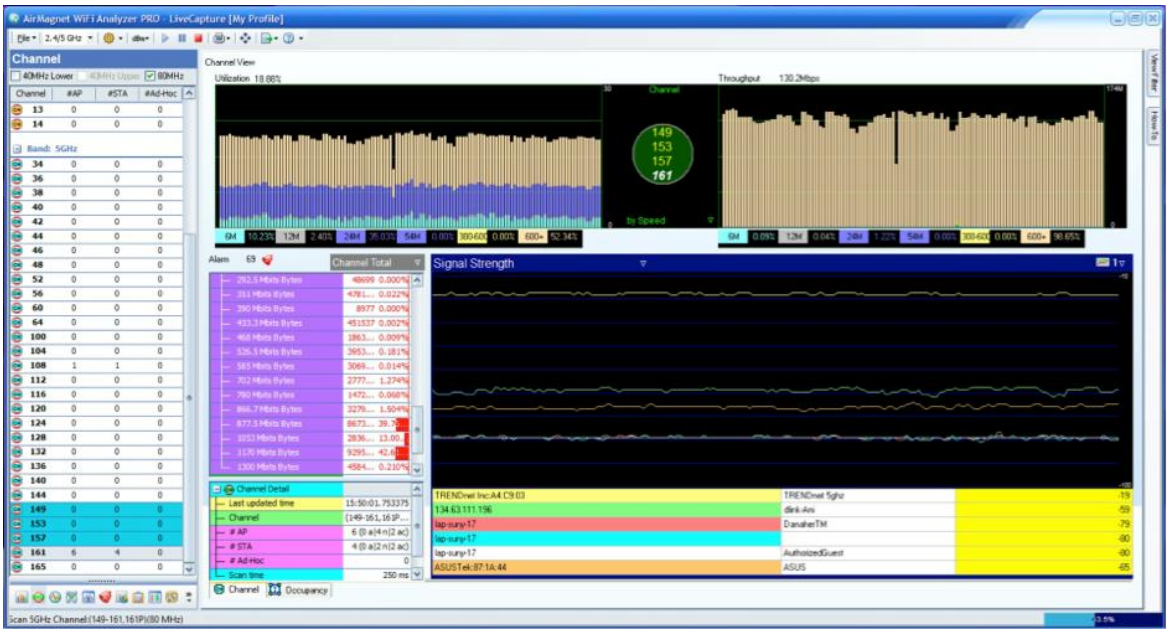


Рисунок 3.2. AirMagnet WiFi Analyzer PRO

Найчастіше надходять діагностичні інструменти з підтримкою 11ac. На даний момент, драйвера для клієнських пристроїв 11ac доступні для багатьох інструментів. Оновлення до інструментів діагностики з підтримкою 11ac, дуже допоможить та підвищить якість радіомодулей 11ac. Отже, чим краща чутливість інструмента, краще він може виконувати свою роботу.

Висновки до розділу 3

Провівши дослідження, можемо зробити висновки, що стандарт 11ac дає ряд технічних удосконалень. Дані покращення зможуть підвищити якість ефективності зв'язку. Проте, деякі із них не можуть бути реалізовані в низці сценаріїв. Переваги:

- Широкі канали до 160 МГц;
- MU-MIMO, низхідний потік;
- Модуляція 256QAM;
- Чотири просторові потоки (4SS);
- Покращена швидкість для діапазону;

- Більш потужне обладнання;
- Підвищена щільність.

В мережах з високою щільністю рекомендується використовувати канали 20 МГц. Технологія MU-MIMO повністю не перевірине, тому не дає позитивний результат. Модуляцію 256QAM можна використовувати на відстані до 50 футів, що в більшості мережах не потрібно. Якщо клієнські пристрої підтримують чотири просторових потоки, за винятком мобільних пристроїв і якщо середовище підтримує декореляцію просторових потоків, то технологія 4SS корисна.

Коли, хочете перейти на 11ac, вам потрібно повністю оновити обладнання або оновити мережу на місці. Потрібно пам'ятати:

• 11ac і 11a/g — це різні технології, кожної з яких потрібен різний тип дизайну мережі;

• 11ac та 11n використовують схожі технології, але з моменту впровадження 11n відбулися значні зміни в обладнанні.

Крім покращення чіпсету 11ac, точки доступу з подвійним радіомодулем і частотою 2,4 ГГц також будуть оснащені більш чутливими чіпсетами 11n з частотою 2,4 ГГц, сприйнятливими до перешкод, і забезпечуватимуть більш високу швидкість.

Якщо, ви плануєте переходити на 11ac, то потрібно максимально відмовитися від використання ISM-смуги 2,4 ГГц. Відмова від 2,4 ГГц покращить можливості користувачів, збільшить пропускну спроможність мережі, зменшить кількість звернень до служби підтримки та значно знизить сукупну вартість володіння інфраструктурою Wi-Fi.

Проектування мережі Wi-Fi, як зазначалося раніше процес, який потребує корегування після встановлення і постійного моніторингу для отримання максимальної рентабельності інвестиції. Для оптимально розміщення і налаштування точок доступу, забезпечення мінімальної інтерференції між каналами, максимальної продуктивності та ефективної роботи WLAN необхідні сучасні інструменти для проектування, дослідження та діагностики, що

підтримують стандарт 802.11ac. Також, компанія Fluke Networks пропонує нові інструменти, які включають AirMagnet Survey and Planner, Spectrum XT, Wi-Fi Analyzer Pro і AirCheck Wi-Fi Tester, а також допомагає своїм клієнтам виконати перехід на 11a.

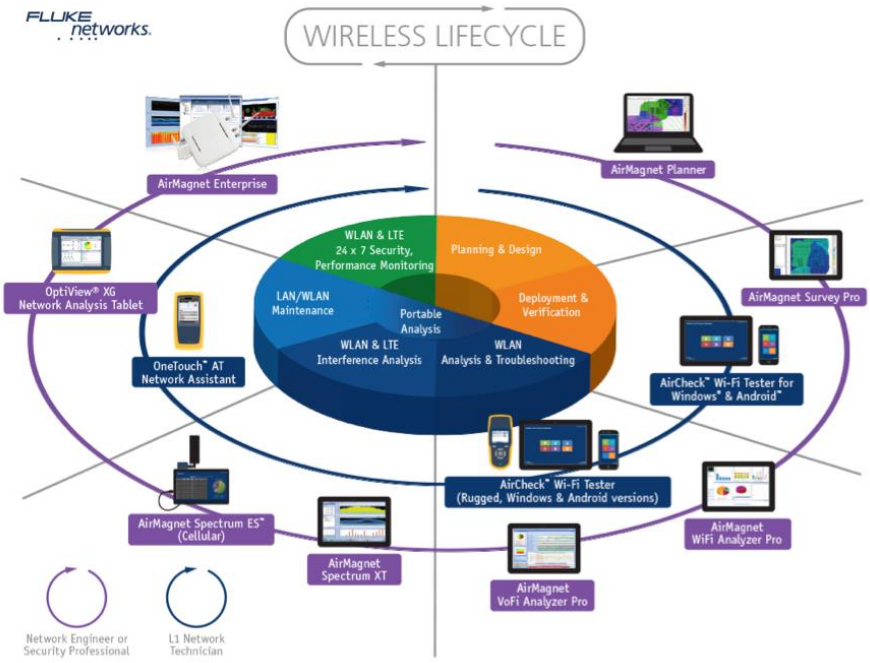


Рисунок 3.3. Інструменти компанії Fluke Networks

Контрольний список міграції, включає аналіз ширини каналів. Рекомендується використовувати канали 20МГц в середовищах високої щільності, наприклад, в аудиторіях, танцювальних залах, виставках, аеропортахи та спортивних аренах, тому що вони збільшують ефективність використання каналу.

ВИСНОВКИ

В мережах низької щільності з високою пропускною здібністю, наприклад у відкритих офісах, краще використовувати канали 40 МГц на частоті 5ГГц, якщо каналів вистачить для повторного використання.

Якщо в будівлі розгорнуто лише 1 чи 2 точки доступу і існує лише мінімальний об'єм перешкод, то можна використовувати канали 80МГц. На даний момент, майже не використовується застосування 160МГц, за винятком каналів «точка-точка».

Якщо у визначеній області постійно потрібно дуже висока пропускна здібність, то можна налаштувати лише одну точку доступу, щоб використовувати канал 80 МГц, якщо точки доступу, що знаходяться поруч, не застосовують будь-яку частину цього каналу.

Але потрібно, враховувати, що швидкість передавання даних не буде високою. Для досягнення MCS9 (найвищий показник MCS для 11ac) для каналу 80 МГц потрібне відношення SNR принаймні 37 дБ. Це невиправдано високе значення SNR, а без повторного використання каналу перешкоди від вільного використання каналів будуть дуже значними.

Потрібно, оцінити провідне зворотнє підключення. Дані лінії не потрібні для 11ac, ні для «Хвиля -1» та «Хвиля-2».

Далі, визначіть методологію проектування. Якщо, збільшується щільність клієнтів чи пропускної здібності, то рекомендується виконати проектування знову. Також, рекомендується розділити різні системи. А потім розмістити точки 11ac. Якщо користувачі хочуть максимізувати повернення інвестицій та отримати переваги 11ac, вони повинні видалити застарілі клієнти та точки доступу.

Врешті, виберіть правильні інструменти. При обстеженні майданчика для перевірки розгортання, що має підтримувати клієнти 802.11ac, слід використовувати адаптери 802.11ac для точного картування та перевірки тих областей, де будуть використовуватися нові рівні швидкості передачі даних і ширини каналу. Для отримання повного уявлення про мережу та її стан необхідно діагностичне обладнання з підтримкою 802.11ac.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. https://help.keenetic.com/hc/uk/articles/213968949-базові положення
2. https://habr.com/ru/articles/149806/
3. https://lanmarket.ua/ua/stats/evolyutsiya-standartov-wifi-802-11/
4. https://ela.kpi.ua/bitstream/123456789/27302/1/Piddubtceva_magistr.pd
5. A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface [Електронний ресурс] // ISO/IEC 14443-2:2020. – 2020. – Режим доступу до ресурсу: https://www.iso.org/standard/73597.html.
6. Guidelines for RFID-based Electronic Article Surveillance [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/gs1-releases-guidelines-for-rfid-based-electronic-article-surveillance.
7. IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://www.idtechex.com/.
8. L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80.
9. Methodology for Evaluating Security in Commercial RFID Systems / T.M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, L. Castedo., 2017.
10. OpenPCD Reader [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.meriac.com.
11. Vogt H. Efficient Object Identification with Passive RFID Tags / Harald Vogt. – Zürich: Department of Computer ScienceSwiss Federal Institute of Technology (ETH), 2002. – 98 с

12. Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28.

13. Fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States.