НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Радіотехнічний факультет

Кафедра прикладної радіоелектроніки

До захисту допущено:
В.о. зав. кафедри
_____ Андрій МОВЧАНЮК
«13» 06 2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інтелектуальні технології радіоелектронної техніки»,

за спеціальністю 172 «Телекомунікації та радіотехніка»
на тему «ВПЛИВ РЕБ НА СТІЛЬНИКОВИЙ ЗВ'ЯЗОК»

Виконав:
студент IV курсу, групи РЕ-02:
Коваль Олексій Олександрович

Керівник: доцент, к.т.н., Приходько Ірина Олександрівна
Посада, науковий ступінь, вчене звання,
Прізвище, ім'я, по батькові

Рецензент: асистент каф. РІ Ванділовський Борис Валерійович
Посада, науковий ступінь, вчене звання,
Прізвище, ім'я, по батькові

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Радіотехнічний факультет
Кафедра прикладної радіоелектроніки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка», за

освітньо-професійною програмою «Інтелектуальні технології радіоелектронної техніки»

ЗАТВЕРДЖУЮ
В.о. зав. кафедри
_____ Андрій МОВЧАНЮК
«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу

Коваль Олексій Олександрович

1. Тема роботи: «Вплив РЕБ на стільниковий зв’язок»

Керівник роботи доцент кафедри прикладної радіоелектроніки Приходько Ірина Олександрівна, затверджена наказом по університету від «29» травня 2024 р. №2178-с.

2. Термін подання студентом роботи 10.06.2024 року

3. Вихідні дані до роботи: результати моделювання.

4. Зміст пояснювальної записки: вступ, актуальність тематики, загальна інформація про технологію РЕБ, завади радіоелектронної боротьби, принцип роботи стільникового зв’язку, моделювання та дослідження впливу завад на стільникову мережу, протидія завадам на стільниковий зв’язок від РЕБ, висновки.

5. Графічний матеріал: презентація

6. Дата видачі завдання: 17 квітня 2024 року

7. Календарний план

6.

№	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Актуальність тематики	1.05.24 – 13.05.24	
2	Загальна інформація про технології РЕБ	14.05.24 – 18.05.24	
3	Завади радіоелектронної боротьби	19.05.24 – 24.05.24	
4	Принцип роботи стільникового зв’язку	24.05.24 – 01.06.24	
5	Моделювання та дослідження впливу завад на стільникову мережу	01.06.24 – 08.06.24	
6	Протидія завадам на стільниковий зв’язок від РЕБ	08.06.24 – 10.06.24	

ВІДОМІСТЬ ДИПЛОМНОЇ РОБОТИ

№ з/п	Формат	Найменування	Кількість листів	Примітка
1	А4	Завдання на дипломну роботу	2	
2	А4	Пояснювальна записка	60	

Студент

Керівник

АНОТАЦІЯ

Дипломний проект «Вплив РЕБ на стільниковий зв’язок» розрахований на дослідження сучасних рішень в принципах роботи радіоелектронної боротьби проти стільникового зв’язку, проаналізувати різні типи РЕБ та їх вплив на роботу стільникових мереж, а також запропонувати методи захисту стільникових мереж від РЕБ. В сучасному світі стільниковий зв'язок відіграє важливу роль у житті людей. Він використовується для спілкування, доступу до інформації, ведення бізнесу та багато іншого. Радіоелектронна боротьба (РЕБ) може значно впливати на роботу стільникових мереж, що може призвести до перебоїв у зв'язку, втрати даних та інших проблем. В цій роботі буде проведено аналіз літературних джерел, демонстрація впливу завад на стільниковий зв’язок.

Ключові слова: РЕБ (радіоелектронна боротьба), стільникова мережа, аутентифікація.

ANNOTATION

The diploma project "The Impact of Electronic Warfare on Cellular Communications" is designed to study modern solutions in the principles of electronic warfare against cellular communications, analyze various types of electronic warfare and their impact on cellular networks, and propose methods to protect cellular networks from electronic warfare. In the modern world, cellular communications play an important role in people's lives. It is used for communication, access to information, business, and much more. Electronic warfare (EW) can significantly affect the operation of cellular networks, which can lead to communication outages, data loss, and other problems. This paper will analyze the literature and demonstrate the impact of jamming on cellular communications.

Keywords: EW (electronic warfare), cellular network.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи

на тему: ВПЛИВ РЕБ НА СТІЛЬНИКОВИЙ ЗВ’ЗОК

Київ – 2024 року

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ACK – Acknowledgement

AM – Amplitude Modulation

ARQ – Automatic Repeat Request

ASK – Amplitude Shift Keying

BASK – Binary Amplitude Shift Keying

BLER – Block Error Rate

BPSK – Binary Phase Shift Keying

CA – Carrier Aggregation

CC – Component Carriers

CDMA – Code Division Multiple Access

DBSCAN – Density-Based Spatial Clustering of Applications with Noise

DL – Downlink

DSSS – Direct Sequence Spread Spectrum

ECCM – Electronic Counter-Countermeasures

ECM – Electronic Countermeasures

ELINT – Electronic Intelligence

ESM – Electronic Support Measures

FDD – Frequency Division Duplex

FEC – Forward Error Correction

FM – Frequency Modulation

FSPL – Free Space Path Loss

GEOINT – Geospatial Intelligence

GPS – Global Positioning System

GSM – Global System for Mobile Communications

HARQ – Hybrid Automatic Repeat Request

ITU – International Telecommunications Union

LTE – Long Term Evolution

ML – Machine Learning

MTSO – Mobile Transport Switching Office

NACK – Negative Acknowledgement

OFDM – Orthogonal Frequency Division Multiplex

OFDMA – Orthogonal Frequency Division Multiple Access

PDCCH – Physical Downlink Control Channel

PSK – Phase Shift Keying

PSTN – Public Switched Telephone Network

PUSCH – Physical Uplink Shared Channel

QAM – Quadrature Amplitude Modulation

QoS – Quality of Service

RFID – Radio Frequency Identification

RSRQ – Reference Signal Received Quality

SC-FDMA – Single Carrier Frequency Division Multiple Access

SIGINT – Signal Intelligence

SINR – Signal-to-Interference-plus-Noise Ratio

SNR – Signal-to-Noise Ratio

SSC – Secondary Synchronization Code

TDD – Time Division Duplex

TECHINT – Technical intelligence

TWS – Tactical Warning System

UL – Uplink

VHF TV – Very High Frequency Television

БС – Базова Станція

ПЗ – Програмне Забезпечення

РЕБ – Радіоелектронна Боротьба

РПП – Радіолокаційний Поперечний Перетин

РЧ – Радіочастоти

ЦОС – Цифрова Обробка Сигналів

ШІ – Штучний Інтелект

ВСТУП

На сьогоднішній день, стільниковий зв’язок став невід’ємною частиною сучасного життя, надаючи людям можливість спілкуватися, отримувати доступ до інформації та вести бізнес за допомогою різних терміналів які підтримують дану технологію. При цьому стільниковий зв’язок не є стійким до всіх видів загроз. В даній роботі ми розглянемо як саме радіоелектронна боротьба (РЕБ) може впливати на роботу стільникової мережі, що може призвести до перебоїв у зв’язку, втрати даних та інших проблем. Проаналізуємо різні типи РЕБ та їх вплив на роботу стільникових мереж, а також запропоную методи захисту стільникових мереж від РЕБ. Мета даної роботи – отримати знання про вплив РЕБ на стільниковий зв’язок, дослідити методи захисту та підготувати рекомендації щодо підвищення стійкості стільникових мереж до РЕБ. Результати дослідження можуть бути використані для розробки методів захисту стільникових мереж від РЕБ, а також для підвищення стійкості стільникових мереж до різних видів загроз. Це може допомогти забезпечити безперебійну роботу стільникових мереж, навіть в умовах РЕБ, що має важливе значення для національної безпеки, економічного розвитку та загального добробуту людей.

1 АКТУАЛЬНІСТЬ ТЕМАТИКИ

У цьому розділі буде детально розглянуто актуальність дослідження впливу РЕБ на стільникову мережу. Метою розділу буде аналіз проблеми та підкреслення її важливості та необхідності в глибокому вивченні. Стільниковий зв'язок став невід'ємною частиною нашого сучасного життя. Він дозволяє користувачам здійснювати телефонні дзвінки, відправляти повідомлення і залишатись на зв'язку незалежно від місця розташування. Залежність від стільникового зв'язку особливо зросла в останні роки з розвитком мобільного інтернету. При цьому в теперішніх реаліях зростає розвиток і загроза радіоелектронної боротьби. РЕБ може використовуватись для перешкоджання зв'язку, відключення радарів, виведення з ладу систем наведення та інших цілей. Ці системи стають все більш поширеними і доступними і все більше країн володіють сучасними системи РЕБ. Характерно змінилося ведення теперішніх воєн. На сьогоднішній день, безпілотники стають все більш поширеними, і багато з них використовують саме стільниковий зв'язок для управління та передачі даних. Це робить безпілотники потенційними цілями для РЕБ. РЕБ може призвести до перебоїв у зв'язку, що може ускладнити або зробити неможливим спілкування людей. Це мати серйозні наслідки для особистого та ділового життя. Також може призвести до порушення роботи критично важливих систем, таких як системи екстреної допомоги, систем енергопостачання та систем управління повітряним рухом.

За даними Стокгольмського міжнародного інституту дослідження миру (SIPRI), світові витрати на військові дослідження у галузі РЕБ стрімко зростають. Держави все більше інвестують у розробку нових систем РЕБ. Також РЕБ стають все доступнішими для терористичних груп та злочинних організацій. Це пов'язано саме з тим, що ціни на компоненти РЕБ знижуються, а інформація про те, як їх використовувати, стає більш доступною в Інтернеті.

Разом з цим збільшився і попит на стільниковий зв'язок. За даними Міжнародного союзу електрозв'язку (ITU), у 2023 році кількість абонентів мобільного зв'язку у світі досягла 5,4 мільярда людей [1]. Це означає, що майже 67% населення Землі мають доступ до мобільного зв'язку. Зростання поширення

технології РЕБ та залежності від стільникового зв’язку робить дослідження впливу РЕБ на стільникову мережу ще більш актуальним. Розумінням цієї проблеми є важливим для розробки методів захисту стільникових мереж від РЕБ та забезпечення їх безперебійної роботи, навіть в умовах загрози. Кожна наступна військова сутичка все більше використовує РЕБ для різних цілей. В Сирії наприклад використовують для ускладнення роботи журналістів та активістів шляхом перешкоджання роботі мобільних мереж. Таку саму тактику застосовували у війні в Нагірному Карабасі у 2020 році Азербайджаном проти Вірменії [2]. Терористи застосовували РЕБ для ускладнення координації аварійно-рятувальних служб, блокування GPS-сигналів, перешкоджання роботі банкоматів та сигналізацій. І звісно, у війні України та росії обидві сторони застосовують РЕБ для різних цілей, в основному для приглушення сигналів безпілотних систем.

2 ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ТЕХНОЛОГІЮ РЕБ

2.1 Вступ

Радіоелектронна боротьба (РЕБ) – це використання електромагнітного випромінювання для деградації або виведення з ладу ворожих радіоелектронних систем. РЕБ може використовуватись для перешкоджання зв’язку, відключення радарів, виведення з ладу систем наведення та інших цілей. Також застосовується для відповідно захисту власних систем зв’язку [3][4].

2.2 Частотний спектр

Частотний спектр – це діапазон електромагнітних хвиль, які використовуються для передачі інформації. Він вимірюється в герцах (Гц) і поділяється на різні діапазони, такі як радіочастоти (РЧ), мікрохвилі, інфрачервоне випромінювання та видиме світло. Кожен пристрій, який використовує бездротовий зв’язок, наприклад, мобільний телефон, Wi-Fi роутер або радіостанція, потребує для роботи певної частини частотного спектру. Детально можна ознайомитись на рисунку 2.2.1

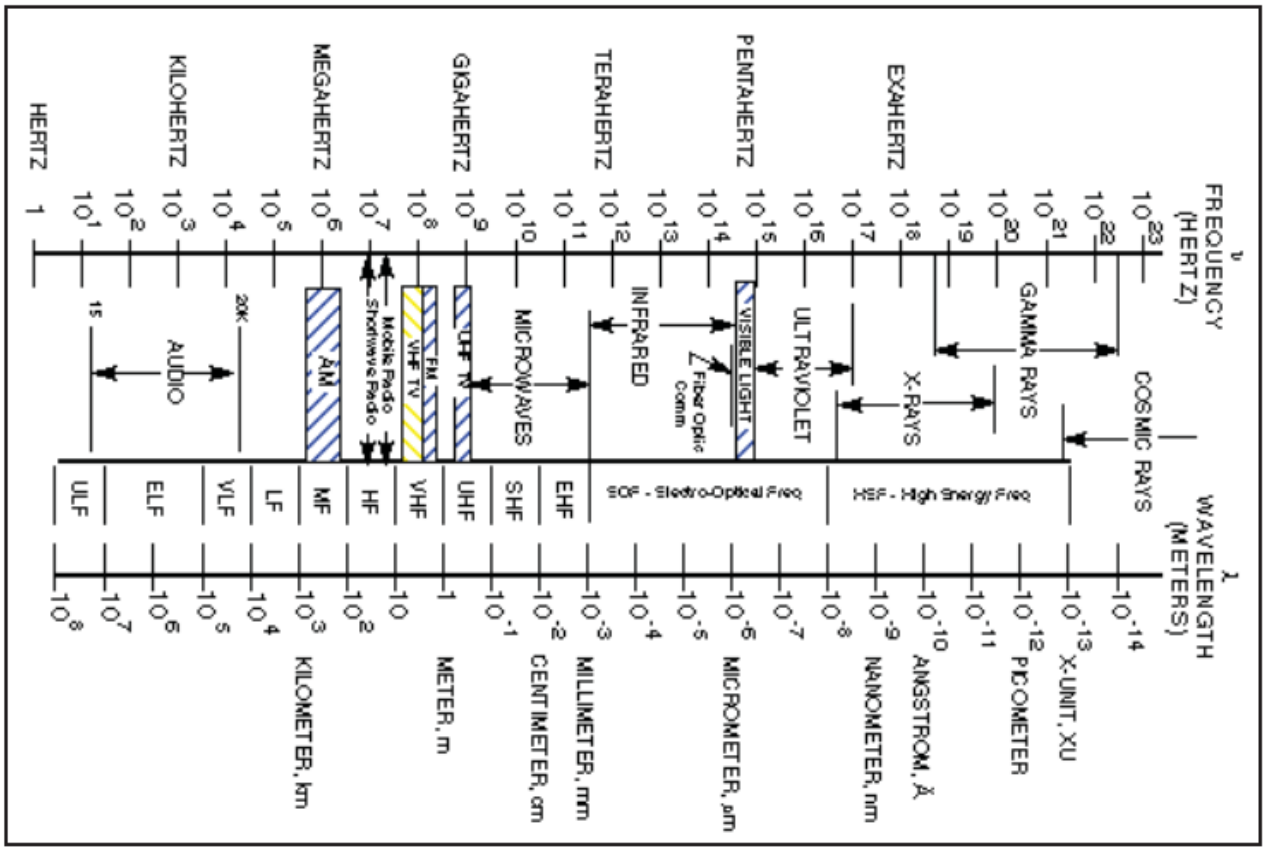


Рисунок 2.2.1 – Спектр електромагнітного випромінювання

На рисунку можна побачити на яких частотах використовуються різні технології, такі як: АМ-сигнал, високочастотна система телевізійного мовлення (VHF TV), FM-радіо, ультрависокочастотна система телевізійного мовлення. Також ми можемо побачити спектр мікрохвиль який знаходиться приблизно на $10^9 - 10^{12}$ Гц. Детальніше з ним можна ознайомитись на рисунку 2.2.2.

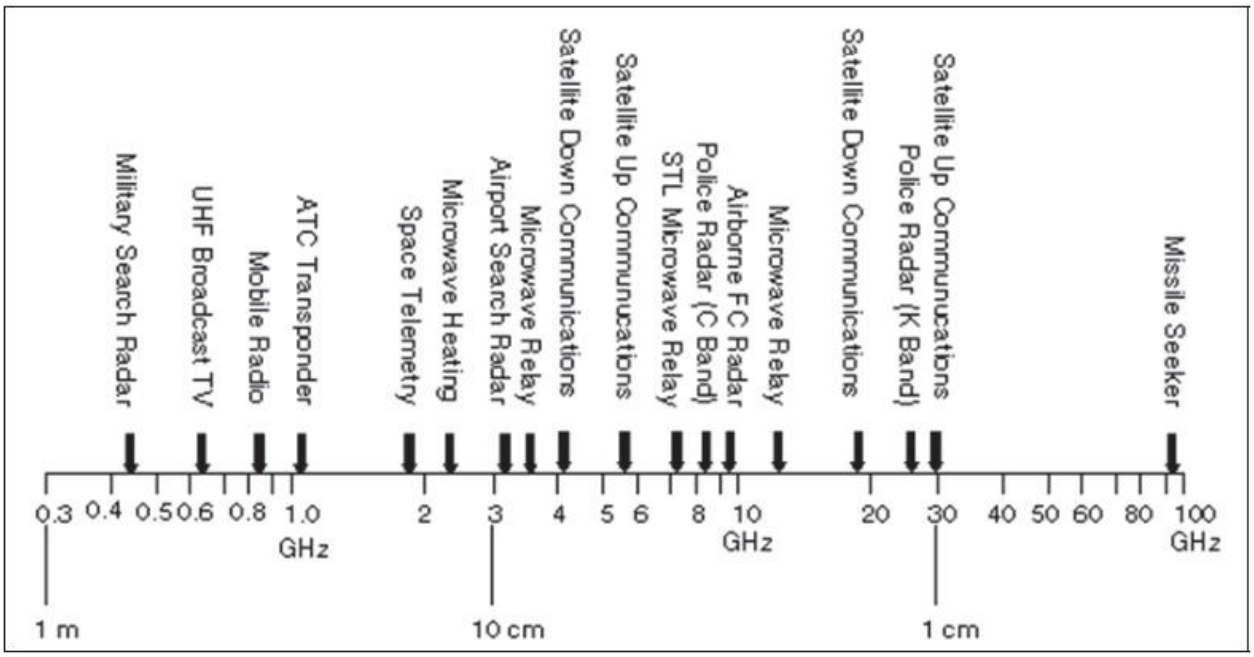


Рисунок 2.2.2. – Мікрохвильовий спектр

По цьому всьому спектрі може працювати технологія РЕБ створюючи перешкоди в сигналі шляхом генерації електромагнітних хвиль. [5]

2.3. Модуляція та демодуляція

Модуляція це процес накладання інформаційного сигналу на носій для передачі, а демодуляція – процес зняття сигналу з носія на приймальній стороні. Радіоелектронна боротьба використовує техніки модуляції та демодуляції для створення перешкод, перехоплення і спотворення сигналів. Існує цифрова та аналогова модуляція. Різновидом цифрової модуляції є ASK, PSK, QAM, а аналогової – AM та FM. Для аналізу використання РЕБ модуляції та демодуляції потрібно розуміти принципи роботи даних видів.

Amplitude Shift Keying (ASK) – це вид модуляції, при якій інформаційний сигнал передається зміною амплітуди носійної хвилі. Двійковий ASK (BASK) використовує дві амплітуди для представлення бітів 0 і 1. Амплітуда носійної

хвилі змінюється відповідно до передаваного двійкового сигналу. Для "1" амплітуда має одне значення, для "0" — інше або відсутня взагалі. Недоліком даної технології є те що вона являється нестійкою до шуму і перешкод, що може при ураженні призвести до спотворення сигналу. Будь-який модульований сигнал має високочастотну несучу. Двійковий сигнал, модульований ASK, дає нульове значення для низького входу, в той час як він дає несучу на високому вході. На наступному рисунку 2.3.1 показано форму сигналу з ASK-модуляцією разом з його входом. [6]

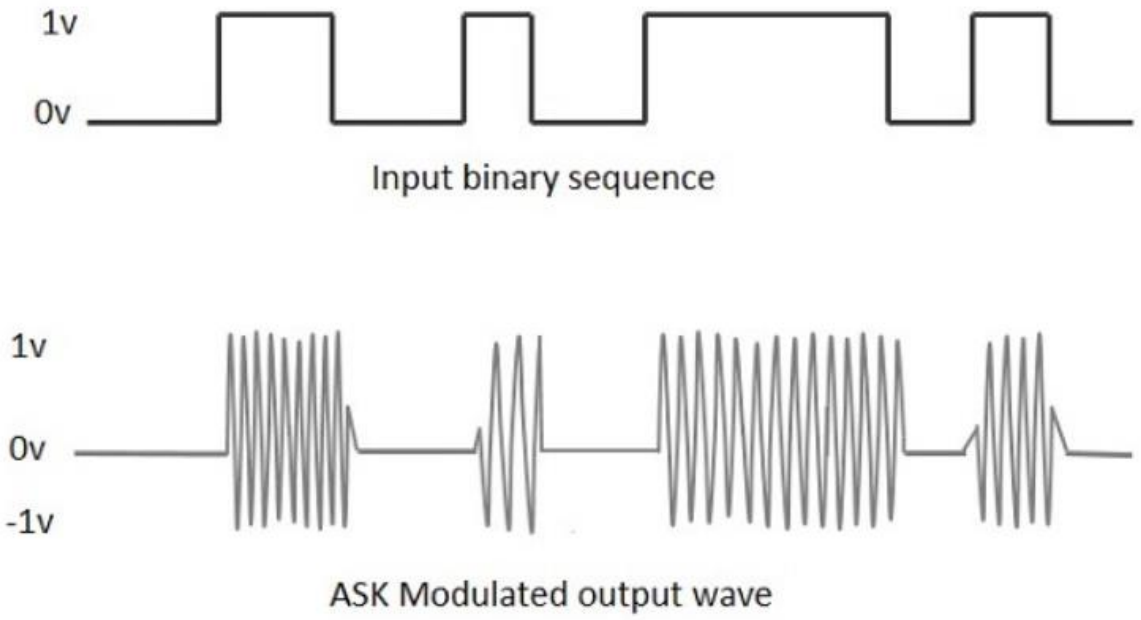


Рисунок 2.3.1 – Принцип роботи ASK

Phase Shift Keying (PSK) – це метод цифрової модуляції, в якому фаза несучого сигналу змінюється шляхом зміни синусоїдальних і косинусоідальних вхідних сигналів у певний момент часу. Техніка PSK широко використовується в бездротових локальних мережах, біометричних, безконтактних операціях, а також у технологіях RFID і Bluetooth-зв'язку. PSK буває двох типів, залежно від того, на скільки фаз зміщується сигнал. Бінарна фазова маніпуляція (BPSK), він також називається 2-фазним PSK або фазовим реверсивним ключем. У цій техніці синусоїдальна несуча приймає два реверси фази, наприклад, 0° і 180°.

Та Квадратурна фазова маніпуляція QPSK – це метод фазової маніпуляції, в якому синусоїдальна несуча приймає чотири фазові інверсії, такі як 0°, 90°, 180° і 270°. Якщо цей тип методів буде розширено, то PSK можна буде виконувати за

восьмома або шістнадцятьма значеннями, залежно від вимог. [6]

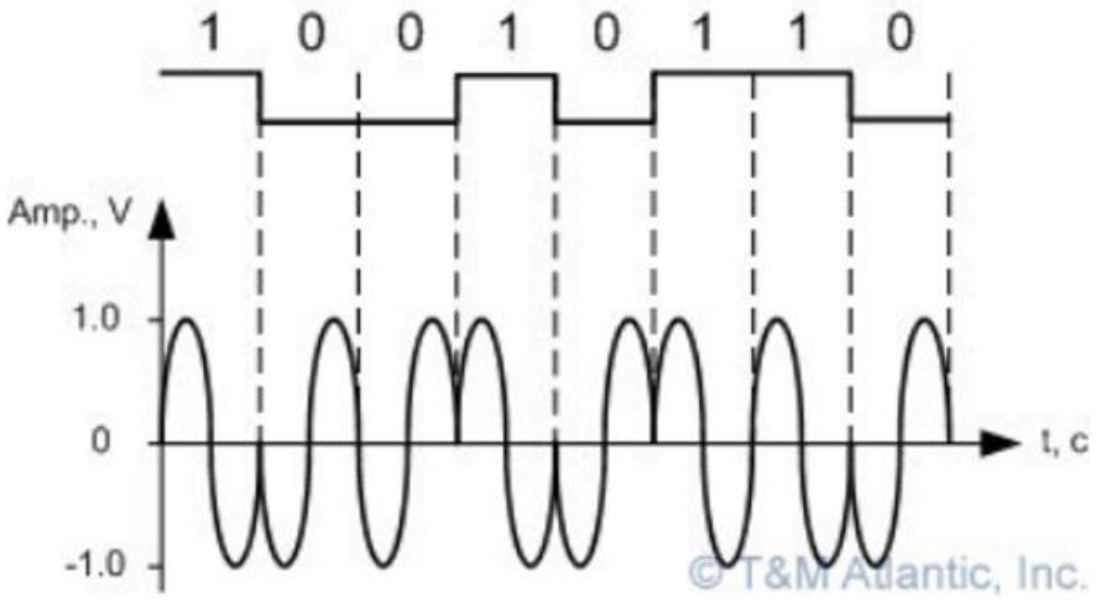


Рисунок 2.3.2 – Принцип роботи PSK

Quadrature Amplitude Modulation (QAM) – це вид модуляції, що поєднує зміну амплітуди і фази носійної хвилі для передачі інформації. QAM використовує кілька амплітуд і фазових станів, що дозволяє передавати більше бітів за один символ. Принципом роботи даної модуляції є те що носійна хвиля одночасно змінює свою амплітуду і фазу відповідно до передаваного сигналу. Наприклад, 16-QAM використовує 16 різних комбінацій амплітуд і фаз, що дозволяє передавати 4 біти на символ. Головною перевагаю є висока спектральна ефективність, що дозволяє передавати більше даних в одиниці спектра. При збільшенні кількості комбінацій, наприклад 64-QAM, 256-QAM, ми можемо спостерігати більш високу чутливість до шуму і перешкод. [7]

Найпростішим і найпоширенішим методом створення завад від РЕБ є модуляція білого шуму, коли в ефір подається широкосмуговий шум, що перекриває цільовий сигнал. Зазвичай, саме цей метод використовується для створення перешкод у широкому діапазоні частот, ускладнюючи прийому оригінального сигналу. Амплітудна модуляція (ASK) може використовуватись для створення перешкод в простих або застарілих системах зв’язку, що використовують амплітудну модуляцію. Але одним з найефективнішим способом заглушити стільниковий зв’язок є фазова модуляція (PSK). Вона є

більш стійкою до шуму та перешкод в порівнянні з ASK. Двійкова фазова модуляція (BPSK) та четвертна фазова модуляція (QPSK) також використовується для створення завад у супутникових системах. Для ефективного створення завад у зв'язку LTE та Wi-Fi використовують квадратурну амплітудну модуляцію (QAM). Саме такий вид модуляції використовується для перешкоджання високошвидкісних систем зв'язку, що використовують складні методи модуляції. QAM поєднує амплітудну та фазову модуляції, що робить її більш ефективною для передачі великого обсягу даних.

2.4. ESM, ECM та ECCM. Роль у РЕБ.

Методи роботи радіоелектронної боротьби поділяються на:

- Електронні засоби протидії
- Електронні контрзаходи
- Радіоелектронний захист

Ці комплекс заходів, спрямовані на зниження або унеможливлення роботи радіолокаційних та інших радіотехнічних систем противника, включаючи стільниковий зв'язок. На рисунку 2.4.1 показано як розподіляються ці методи в роботі.

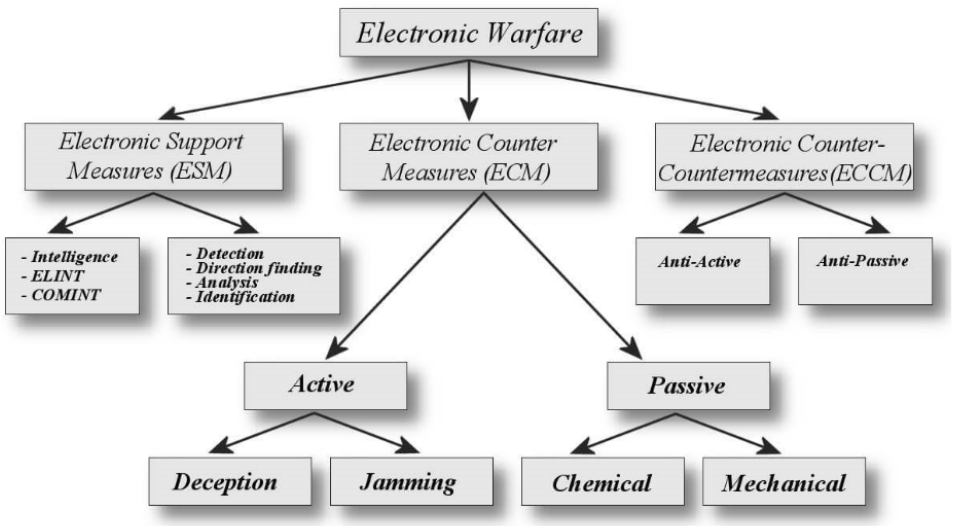


Рисунок 2.4.1 – Методи радіоелектронної боротьби

2.4.1. Електронні засоби протидії

ESM (Electronic Support Measures) - це комплекс заходів, спрямованих на виявлення, розпізнавання та локалізацію джерел радіовипромінювання противника. ESM-системи використовуються для збору інформації про

радіоелектронну обстановку на полі бою, що може бути використано для планування РЕБ-операцій та попередження про радіолокаційні загрози. ESM-дані допомагають визначити типи радіоелектронних систем, які використовує противник, їх місцезнаходження та режими роботи. Ця інформація може бути використана для розробки ефективних РЕБ-заходів. Також ESM-системи можуть виявляти радіолокаційні сигнали противника, що може допомогти власним силам уникнути виявлення. Такі спектральні дані можуть збиратися в повітрі, на морі і на землі в різних умовах по всьому світу.

Інформація, зібрана і перерозподілена командою радіоелектронної підтримки, забезпечує кожну місію ситуаційною обізнаністю, яка може варіюватися від виявлення іноземних сигналів до ідентифікації ворожих і дружніх сил, визначення місцезнаходження і характеристики тактичних загроз і багато іншого. Технології і послуги РЕБ є частиною загальної місії розвідки сигналів (SIGINT) і часто також використовують можливості радіоелектронної розвідки (ELINT), геопросторової розвідки (GEOINT), технічної розвідки (TECHINT) і багатопрофільної розвідки (Multi-INT).

Кожна така система має антену, приймач та процесор (рис.2.4.2). [8]

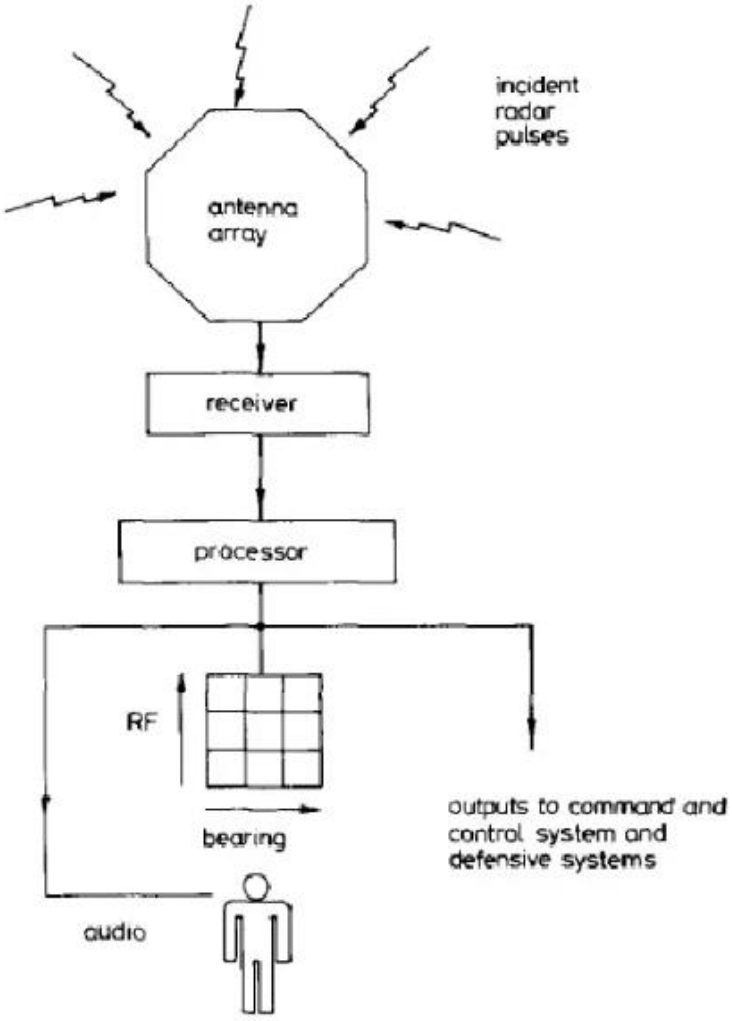


Рисунок 2.4.2 – Принцип роботи ESM

Розпочинається все з прийому імпульсів антеною з навколишнього середовища. Також антена вимірює пеленг джерела сигналу – це кут, який визначає, де на горизонті знаходиться джерело сигналу. Далі приймач виявляє радіочастотні імпульси, проводить цифрові вимірювання наступних характеристик: час приходу, ширина імпульсу, амплітуда, наявність модуляції. Процесор при цьому сортує вхідні імпульсні дані. Групує імпульси в набори, які називаються звітами про ланцюжок імпульсів. Сформовані набори використовуються для створення поточного файлу випромінювача. Поточний файл містить список всіх випромінювачів, що діють в даний час в навколишньому середовищі. Також зберігаються всі характеристики: частота, ширина смуги, тип модуляції, пеленг та сила сигналу. Далі ці всі дані ідуть на аналіз до системи управління та контролю яка вже відображає всю відому інформацію про випромінювачі оператору. Це дає змогу скласти актуальну картину повітря і поверхні разом з даними від інших датчиків. Ці всі дані можуть

бути надіслані іншим стратегічним цілям, наприклад кораблям, літакам або наземним станціям. [9]

2.4.2 Електронні контрзаходи

Електронні контрзаходи (ECM) - це військова технологія, яка використовує електричні або електронні пристрої для обману або введення в оману систем виявлення, таких як радари, сонари, інфрачервоні (ІЧ) системи або лазери. ECM може використовуватися як в нападі, так і в обороні, щоб не дозволити противнику отримати інформацію для націлювання. ECM є критично важливим інструментом для захисту військової техніки, особливо літаків, від нападу керованих ракет. Більшість військово-повітряних сил світу використовують ECM для захисту своїх літаків. Крім того, ECM розгортається на військових кораблях та деяких сучасних танках для протидії лазерним та інфрачервоним керованим ракетам. Існують такі три основні методи роботи ECM: заглушення, обман та комбінований.

Метод заглушення або джамінгу є найпоширенішим методом ECM. Він полягає у передачі потужних електронних сигналів, які виглядають як шум або "перешкоди" для приймача радара. Оскільки природні перешкоди (від землі, будівель тощо) є постійною проблемою для радарів, ефективне заглушення змушує приймач не розрізняти справжні цілі від штучних перешкод. Ефективність заглушення залежить від кількох факторів: сили сигналу, типу радарів та від радіолокаційного поперечного перетину цілі. При сильнішому сигналі заглушення, робота РЕБ є більш ефективною але при цьому і більш помітною. Також потрібно враховувати і знати на який тип радарів проводиться джамінг, адже кожен має свою стійкість.

Радіолокаційний поперечний перетин (РПП) - це міра того, скільки радіосигналів відбиває об'єкт назад до радара. Іншими словами, це "видимість" об'єкта для радара. РПП вимірюється в квадратних метрах ($м^2$). Чим менший РПП об'єкта, тим складніше його виявити радаром. Це робить об'єкт більш "малопомітним" (стелс). Малопомітні літаки, ракети та кораблі можуть уникнути виявлення противником, що дає їм значну перевагу. Для ECM чим менший РПП цілі, тим складніше її виявити навіть за наявності заглушення.

Обман - це більш складний метод ECM, ніж заглушення. Він полягає в

перехопленні сигналу радара, його маніпулюванні та повторній передачі назад до приймача. Це створює для радара хибні цілі, неправильне визначення цілей або їх розташування. Один з підходів до обману являється обманом з використанням сигналу. Перехоплений сигнал радара трохи змінюється (наприклад, за часом) та передається назад, щоб змусити радар думати, що ціль знаходиться в іншому місці. Іншим є метод імітації – створення повністю штучного сигналу, який імітує сигнал від цілі. Цей метод дозволяє створити фальшиві цілі, що ускладнює для радара визначення справжніх цілей. При цьому найефективнішим способ є комбінація цих методів. Це створює для радара противника ще складнішу картину, де справжні цілі важко відрізнити від хибних серед загальних перешкод. [10]

2.4.3 Радіоелектронний захист

Електронні контр-контрзаходи (ECCM) є частиною радіоелектронної боротьби (РЕБ). Вони включають різноманітні методи, спрямовані на зменшення або нейтралізацію впливу електронних контрзаходів (ECM) противника на роботу електронних датчиків літальних апаратів, кораблів, транспортних засобів, а також зброї, такої як ракети. В Європі ECCM часто називають електронними захисними заходами (EPM). На практиці EPM часто означає стійкість до заглушення. Більш детальне визначення ECCM – це дії РЕБ, які здійснює радар для нейтралізації контрзаходів противника. Системи попередження ECCM можуть виявляти сигнали заглушення противника та попереджати про їхню присутність. Це дозволяє операторам радарів вживати відповідних заходів, таких як зміна частоти або використання адаптивних фільтрів. Методи захисту ECCM спрямовані на зменшення впливу сигналів заглушення на сигнали цілей. Це може включати використання адаптивних антенн, які можуть фокусуватися на сигналах цілей та ігнорувати сигнали заглушення, а також використання цифрової обробки сигналу для видалення небажаних сигналів. Деякі системи ECCM можуть використовувати методи обману, щоб заплутати радари противника. Наприклад, вони можуть генерувати хибні сигнали, які виглядають як реальні цілі, або перехоплювати та повторно передавати сигнали радара противника з невеликим запізненням, щоб створити враження рухомих цілей. Основними методами ECCM є попередження, захист і

обман.

Системи попередження ЕССМ призначені для виявлення та ідентифікації сигналів ЕСМ противника. Це дозволяє операторам радарів та інших систем вживати відповідних заходів, таких як зміна частоти роботи, використання адаптивних фільтрів або активація систем захисту. Прикладом систем попередження ЕССМ є система радіоелектронної розвідки (SIGINT). Ця система перехоплює та аналізує радіосигнал противника, щоб виявити джерела ЕСМ. Та система про попередження про загрози (TWS) яка використовує алгоритми для автоматичного виявлення та класифікації сигналів ЕСМ, попереджаючи операторів про присутність.

Методи захисту ЕССМ спрямовані на зменшення або нейтралізацію впливу сигналів ЕСМ на сигнали цілей. Основними методами є використання адаптивних антен, які динамічно змінюють свою діаграму спрямованості, щоб фокусуватись на сигналах цілей та ігнорувати сигнали ЕСМ. Алгоритми цифрової обробки сигналів також можуть бути використані для видалення небажаних сигналів ЕСМ з сигналу цілі, роблячи його більш чітким. Прикладом ЦОС є:

- частотне фільтрування
- часове фільтрування
- фільтрування з адаптивною структурою
- фільтрування з адаптивною характеристикою.

Частотне фільтрування основується на використанні фільтрів, які пропускають сигнали певної частоти, блокуючи сигнал ЕСМ, які мають інші частоти. При цьому часове фільтрування використовує фільтри, які пропускають сигнали цілі з певною затримкою, блокуючи сигнали ЕСМ, які мають іншу затримку. Фільтрування з адаптивною структурою використовує адаптивну структуру фільтра, яка може змінюватися в залежності від типу ЕСМ. Це робить його ефективним проти широкого спектру загроз. Фільтрування з адаптивною імпульсною характеристикою заключається у динамічній зміні своєї імпульсної характеристики в залежності від характеристик сигналу ЕСМ. Це дозволяє йому ефективно видаляти ЕСМ, не впливаючи на сигнал цілі.

Також деякі системи ЕССМ використовують методи обману, щоб

заплутати атаки противника. Система ECCM може генерувати фальшиві сигнали, які виглядають як реальні цілі, щоб змусити радари противника витрачати час та ресурси на їх відстеження. Система ECCM може перехоплювати сигнали радара противника та повторно передавати їх з невеликим запізненням або зміною, щоб створити враження рухомих цілей. [11][12][13]

2.5. Тенденція розвитку РЕБ

Радіоелектронна боротьба (РЕБ) постійно розвивається, з'являються нові технології та методи, які роблять цю сферу все більш складною та динамічною. Розуміння цих тенденцій є ключовим для операторів РЕБ, які прагнуть бути готовими до майбутніх загроз та викликів, а також для інженерів які працюють над налаштуванням стільникової мережі в межах районів активного застосування РЕБ.

Штучний інтелект (ШІ) та машинне навчання (ML) вже зараз роблять значний вплив на РЕБ, автоматизуючи рутинні завдання, аналізуючи великі обсяги даних та приймаючи рішення в режимі реального часу. Ця тенденція, ймовірно, буде посилюватися в майбутньому, адже ШІ та ML можуть допомогти розробити більш досконалі системи РЕБ, які здатні динамічно адаптуватися до мінливих умов на полі бою. Застосування алгоритмів ШІ в системах РЕБ робить їх більш ефективними та автономними. Сучасні військові активно використовують автономні системи РЕБ, що значною мірою базуються на ШІ-алгоритмах.

Зростаюча потреба в автоматизації систем РЕБ стимулює дослідження нових алгоритмів ШІ для підвищення їхньої ефективності. ШІ може застосовуватися в різних сферах військової діяльності, таких як:

- Вибір та застосування зброї
- Підтримка прийняття рішень
- Аналіз загроз
- Інтерпретація розвідувальних даних
- Логістика

Вплив ШІ може стосуватися організації бойового порядку, розподілу

завдань військам, розробки військових стратегій, рішень щодо масштабування та ескалації конфлікту, обміну та інтерпретації розвідувальних даних, визначення характеру та масштабу війни, наслідків використання певних ресурсів. Застосування ШІ на оперативному рівні може суттєво вплинути на досягнення тактичних цілей, планування операцій, зниження невизначеності та підвищення ефективності підготовки до бойових дій. Алгоритми кластеризації, такі як DBSCAN та K-Means, можуть використовуватися для аналізу даних РЕБ з метою визначення розташування цілей (джерел сигналів). Це допомагає зосередити зусилля РЕБ на найбільш критичних зонах. Також існують алгоритми навчання які використовуються для оптимізації перешкоджання каналам зв'язку противника, навіть за відсутності попередніх знань про систему. Він дозволяє системі РЕБ навчатися та обирати найбільш ефективні стратегії перешкоджання. [14]

ВИСНОВОК ДО РОЗДІЛУ 2

Радіоелектронна боротьба (РЕБ) - це складна та динамічна сфера, яка відіграє все більш важливу роль у сучасних військових конфліктах. ECM, ESM та ECCM - це три ключові компоненти РЕБ, які мають значний вплив на роботу стільникових мереж. ECM може серйозно порушити роботу стільникових мереж, заглушуючи або спотворюючи сигнали базових станцій та мобільних пристроїв. ESM може допомогти операторам стільникових мереж виявити та відстежити джерела ECM, а також вирішити проблеми з безпекою. ECCM використовується для захисту стільникових мереж від ECM, забезпечуючи надійне обслуговування абонентів. Операторам стільникових мереж важливо розуміти принципи роботи РЕБ і ECM, ESM та ECCM, а також бути в курсі останніх розробок у цій сфері. Це допоможе їм захистити свої мережі та забезпечити безперебійну роботу стільникового зв'язку в умовах РЕБ. Боротьба за контроль над електромагнітним спектром є безперервною і потребує глибокого розуміння можливостей та методів противника. Успіх у цій боротьбі часто залежить від здатності своєчасно розпізнати і нейтралізувати загрози, а також від ефективності заходів електронного захисту. Розвиток технологій РЕБ та ЕЗ є ключовим фактором забезпечення надійності і безпеки військових радарних систем.

3 ЗАВАДИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

3.1. Вступ

В даному розділі буде детально розглянуто які саме завади здатен РЕБ поширювати та як вони можуть впливати на стільникову мережу. на меті надати детальне розуміння різновидів завад, принципів їхньої роботи та потенційних загроз, які вони становлять для стільникових мереж. Завади РЕБ — це навмисні електромагнітні сигнали, що генеруються з метою зниження ефективності або повного припинення функціонування цільових систем зв'язку, радіолокації та інших електронних пристроїв. У цьому розділі ми розглянемо основні типи завад, пояснимо фізичні принципи їхнього функціонування та оцінюємо їхній вплив на стільникові мережі.

3.2. Види шумів

У системах радіоелектронної боротьби (РЕБ) для створення завад найчастіше використовується білий шум, який зазвичай описується нормальним (гаусовим) розподілом. Це пояснюється тим, що білий шум має рівномірний спектральний розподіл енергії в заданому частотному діапазоні, що дозволяє ефективно глушити різні види сигналів.

Білий шум — це вид шуму, енергія якого рівномірно розподілена по всьому частотному спектру. Іншими словами, білий шум має однакову потужність на всіх частотах у заданому діапазоні, що робить його ідеальним для різноманітних застосувань, включаючи генерацію перешкод у системах радіоелектронної боротьби (РЕБ). Білий шум характеризується широкосмуговим спектром і непередбачуваними амплітудами. Білий шум моделюється як гаусовий шум (шум з нормальним розподілом амплітуд). Це означає, що амплітуди сигналу мають нормальний розподіл, що добре описує випадкові процеси в природі та техніці. Гаусовий розподіл, також відомий як нормальний розподіл, є одним з найважливіших і найчастіше використовуваних розподілів ймовірностей у статистиці та теорії ймовірностей.

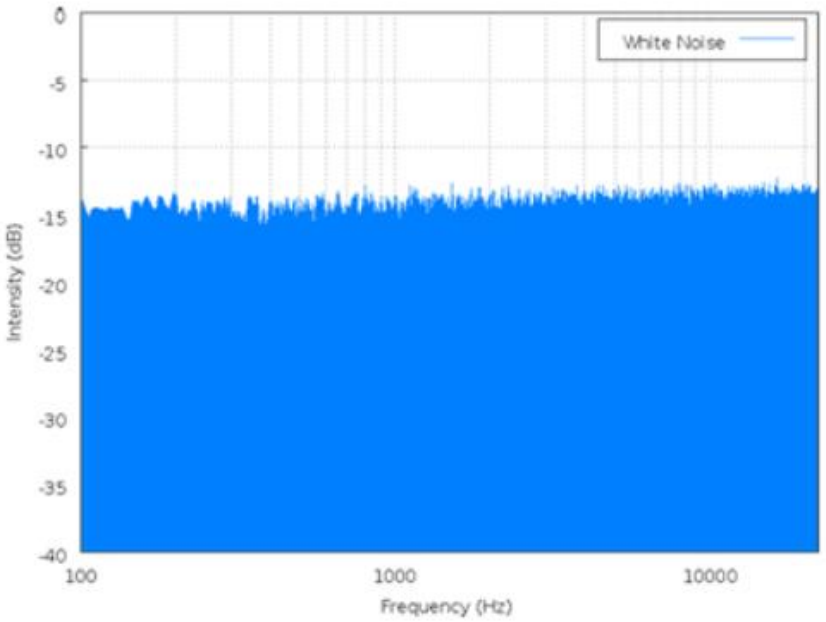


Рисунок 3.1. – Зображення білого шуму

Щільність ймовірності для амплітуд білого шуму описується наступною формулою 3.1.:

$$P(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}, \qquad (3.1.)$$

де, μ — середнє значення, де знаходиться пік (для білого шуму зазвичай μ=0), σ — стандартне відхилення, воно вимірює розсіювання даних навколо середнього значення; чим більше значення σ, тим ширший розподіл, P(x) — щільність ймовірності на точці x. В системах радіоелектронної боротьби (РЕБ) гаусовий розподіл має ключове значення при моделюванні та аналізі завад, особливо шумових. Амплітуди шуму мають нормальний (гаусовий) розподіл з середнім значенням, яке зазвичай дорівнює нулю, та певним стандартним відхиленням, що визначає потужність шуму. Білий шум, що моделюється гаусовим розподілом, має рівномірний спектральний розподіл енергії, що дозволяє ефективно глушити різні сигнали в широкому частотному діапазоні. Білий шум з гаусовим розподілом ефективно знижує SNR, що ускладнює або робить неможливим правильне приймання та обробку цільових сигналів. Завдяки своїм властивостям, білий шум з гаусовим розподілом амплітуд є ефективним засобом для створення перешкод, що значно ускладнюють роботу систем зв'язку та радіолокації.

Рожевий шум, також відомий як 1/f шум або спектральний шум, є видом випадкового шуму, енергія якого обернено пропорційна частоті. На відміну від

білого шуму, який має рівномірну потужність на всіх частотах, потужність рожевого шуму зменшується з підвищенням частоти. Це означає, що на низьких частотах амплітуда рожевого шуму більша, ніж на високих. Оскільки його потужність знижується з підвищенням частоти, він ефективніше впливає на нижчі частоти, що часто використовуються в стільникових мережах. За допомогою рожевого шуму можна створювати перешкоди на конкретних частотних діапазонах, що використовуються для передачі даних або голосових викликів у стільникових мережах. Рожевий шум також знижує співвідношення сигнал/шум (SNR). Формула спектральної щільності потужності така (3.2.):

$$S(f) \propto \frac{1}{f} \qquad (3.2.)$$

де, $S(f)$ – це спектральна щільність потужності на частоті f, а f – частота. Частотний спектр рожевого шуму стабільний і передбачуваний, що робить його корисним для калібрування і тестування систем.

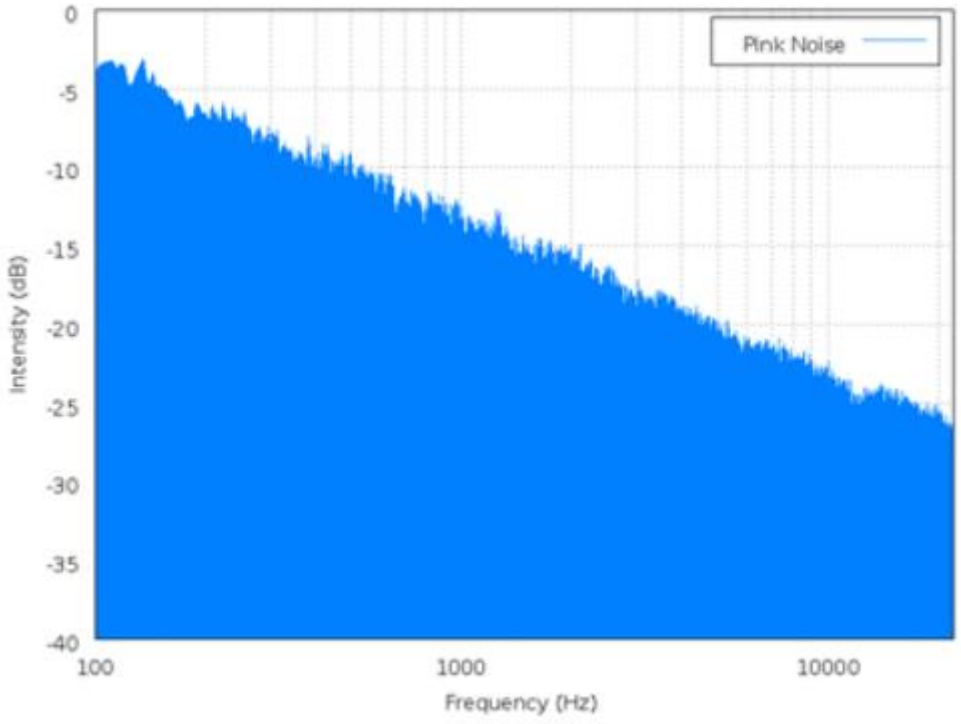


Рисунок 3.2. – Зображення рожевого шуму

Коричневий шум, також відомий як браунівський шум або шум Броуна, є видом випадкового шуму, енергія якого пропорційна $1/f^2$. Це означає, що потужність коричневого шуму зменшується з підвищенням частоти ще швидше, ніж у випадку з рожевим шумом. Назва "коричневий" походить від назви "браунівський рух", що описує випадковий рух частинок у рідині або газі, відкритий Робертом Броуном. Коричневий шум часто звучить глибше і менш

різко порівняно з білим або рожевим шумом. Коричневий шум можна розглядати як інтеграл білого шуму. Спектральна щільність потужності коричневого шуму пропорційна 1/f², що означає, що його енергія сильно зосереджена на низьких частотах і ще нижчих чим в рожевому шумі. Формула спектральної щільності потужності така (3.3.):

$$S(f) \propto \frac{1}{f^2} \tag{3.3.}$$

Потужність коричневого шуму швидко зменшується з підвищенням частоти, що робить його ефективним на низьких частотах.

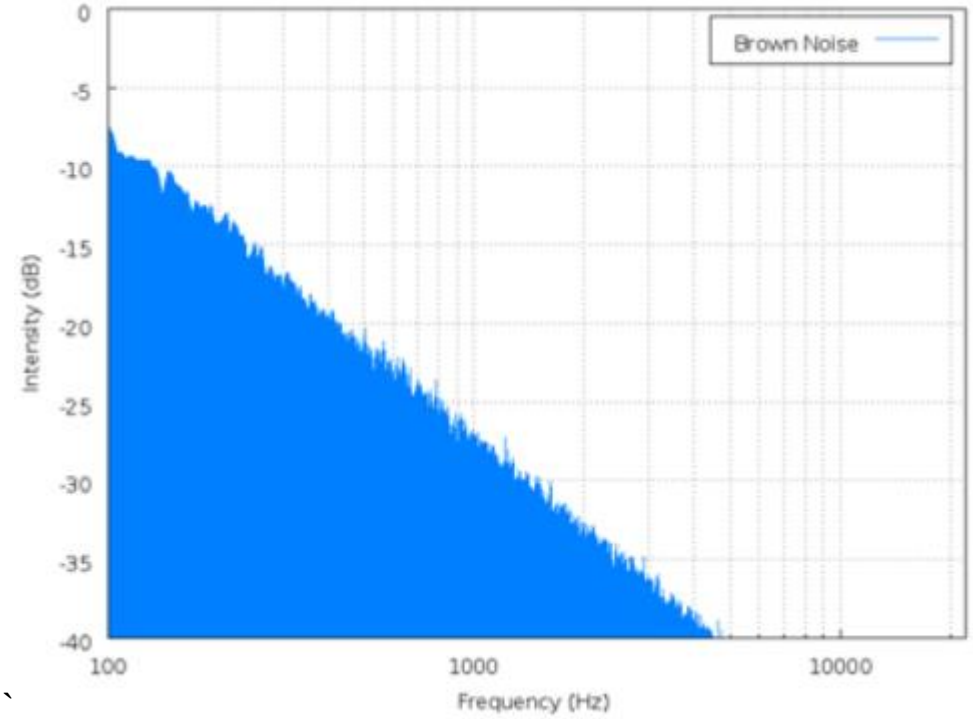


Рисунок 3.3. – Зображення коричневого шуму

Формули 3.1, 3.2, 3.3, це формули спектральної щільності які були досягнуті внаслідок застосування спрощенням і квадратичним перетворенням Фур'є. Отримане рівняння 3.4. спектральної щільності потужності відображається нижче:

$$PSD = \sqrt{(\sum x(t)\cos(\omega t))^2 + (\sum x(t)\sin(\omega t))^2} \tag{3.3.}$$

Виходячи з цього рівняння ми отримуємо формули які кваліфікують шум різних кольорів. В контексті представленого рівняння, якщо $x(t)$ є білим шумом, тоді суми двох частин рівняння будуть також мати рівномірний розподіл потужності по всьому частотному спектру. Якщо ми говоримо про рожевий шум, то суми двох частин рівняння будуть мати спектральну щільність

потужності, що зменшується зі збільшенням частоти пропорційно 1/f. При коричневому шумі будуть мати спектральну щільність потужності, що зменшується зі збільшенням частоти пропорційно $1/f^2$. [15]

3.3. Потужність сигналу-завади

Для створення завад правильної потужності оператору РЕБ треба врахувати багато факторів. Правильний аналіз допоможе точково вплинути на глушіння стільникової мережі в певній області. Радіоелектронна боротьба (РЕБ) використовує різні рівні потужності для створення перешкод у стільникових мережах. Потужність завадника залежить від кількох факторів, таких як: відстань до цілі, частотний діапазон, тип перешкод, оточуюче середовище. Чим далі завадник до цілі, тим більше потужний сигнал потрібно реалізувати для ефективнового спотворення. При високих частотах також потрібно збільшувати потужність перешкоди через більшу втрату сигналу при розповсюдженні. Важливою частиною аналізу також є аналіз місцевості, потрібно враховувати нерівності ландшафту, висоту будівель, лісистість тощо.

Для розрахування потрібної потужності використовують відповідну формулу 3.4:

$$P_{int} = P_s + L_{path} + G_s - G_{int} \quad (3.4.)$$

де, P_{int} – потужність потрібна для завади на ціль, P_s – потужність сигналу стільникового зв'язку, L_{path} – втрати при пропагації, G_s – коефіцієнт підсилення приймача, G_{int} – коефіцієнт підсилення антени завадника. Для розрахунку втрати при пропагації L_{path} розраховують за такою формулою 3.5[15]:

$$L_{path} = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) \quad (3.5)$$

де, d – відстань між приймачем і передавачем, f – частота сигналу, c – швидкість світла. Зазвичай до формули ще додають запас потужності, адже не слід забувати про методи контрзахисту, яка може також впливати на хвилю завадника. Але дана формула розраховує саме при створенні завад у вільному просторі, без природних перешкод. Формула розрахунку втрати при пропагації 3.5. використовується саме в моделі FSPL (Free Space Path Loss), тобто для відкритих просторів без перешкод. Існують також інші моделі пропагації для

різних умов середовища. Наприклад, для міської щільної забудови використовують модель Окамура-Хата. Вона також враховує висоту антен базових станцій і специфічні параметри середовища. Формула розрахунку втрат при пропагації моделі Окамура-Хата виглядає так (3.6.):

$$\mathrm{L} = 69.55 + 26.16\log_{10}(f) - 13.82\log_{10}(h_t) - \mathrm{a}(h_r) + (44.9 - 6.55\log_{10}(h_t))\log_{10}(d) \quad (3.6)$$

де, f – частота сигналу, яка має бути в межах 100-3000 МГц, h_t – висота передачі в метрах від 30 до 200 метрів, h_r – висота приймача від 1 до 100 метрів, $\mathrm{a}(h_r)$ – коригувальний фактор для висоти приймача, який залежить від середовища. Коригувальний фактор може бути виражений по різному, в залежності від середовища. Для приміської та сільської забудови формула має такий вигляд:

$$\mathrm{a}(\mathrm{h}_r) = (1.1\log_{10}(f) - 0.7)\mathrm{h}_r - (1.56\log_{10}(f) - 0.8) \quad (3.7)$$

для мегаполісу або великого міста:

$$\mathrm{a}(\mathrm{h}_r) = 3.2((\log_{10}(11.75\mathrm{h}_r))^2 - 4.97 \quad (3.8)$$

В системах радіоелектронної боротьби (РЕБ) модель Окамура-Хата використовується для оцінки ефективності створення завад в міських, приміських і сільських умовах. Це дозволяє правильно визначити необхідну потужність завадника та оптимальне розташування передавача, щоб максимізувати ефект завад на цільові стільникові мережі. Модель COST-231 Hata є розширенням моделі Окамура-Хата, розробленої для використання в частотному діапазоні від 1500 до 2000 МГц, що робить її особливо корисною для сучасних систем стільникового зв'язку, таких як GSM, LTE та 5G. Ця модель була розроблена в рамках європейського проєкту COST-231 (Cooperation in the field of Scientific and Technical Research) і враховує специфіку міських, приміських і сільських середовищ. Формула моделі виглядає так:

$$\mathrm{L} = 46.3 + 33.9\log_{10}(f) - 13.82\log_{10}(h_t) - \mathrm{a}(h_r) + (44.9 - 6.55\log_{10}(h_t))\log_{10}(d) + C \quad (3.9)$$

де додався новий параметр C — поправочний коефіцієнт для метрополітену (C=3) та приміських/сільських (C=0) середовищ. Застосування моделі COST-231 Hata в системах РЕБ дозволяє створювати ефективні завади, що призводять до значних втрат сигналу в цільових стільникових мережах. Це може викликати зниження якості зв'язку, збільшення кількості пропущених дзвінків, погіршення

якості передачі даних та інші негативні наслідки для користувачів мережі.

Також існує модель пропагації Лонглі-Райс, яка є комплексною моделлю для прогнозування втрат сигналу у системах радіозв'язку. Вона базується на поєднанні емпіричних і теоретичних підходів для врахування різних факторів, які впливають на поширення радіохвиль. Модель описується рядом формул і алгоритмів, які враховують вплив поверхні Землі, атмосферних умов і інших факторів. Загальна формула втрат цієї моделі виглядає наступним чином:

$$\mathrm{L}_t = \mathrm{L}_{fs} + \mathrm{L}_d + \mathrm{L}_s + \mathrm{L}_r \tag{3.10}$$

де, L_{fs} – втрати у вільному просторі, L_d – втрати через дифракцію, L_s – втрати через поверхневу хвилю, L_r – втрати через рефракцію та рефлексію. Втрати у вільному просторі описуються стандартною формулою 3.5. Втрати через рефракцію описуються так:

$$\mathrm{L}_{refr} = \frac{d}{k_{eff}} \tag{3.11}$$

де, k_{eff} – ефективний коефіцієнт рефракції. Рефлексій витрати розраховуються за формулою:

$$L_{refl} = 10\log_{10}(\frac{P_r}{P_t}) \tag{3.12}$$

для повної формули потрібно додати $\mathrm{L}_r = \mathrm{L}_{refr} + L_{refl}$.

Втрати через поверхневу хвилю є важливою складовою поширення радіохвиль на низьких частотах і на коротких відстанях, коли сигнал поширюється вздовж поверхні землі. Ці втрати залежать від таких факторів, як тип поверхні, електричні характеристики поверхні, висота передавача та приймача. Однією з часто використовуваних емпіричних формул для обчислення втрат через поверхневу хвилю є [16]:

$$\mathrm{L}_s = 8.68 \cdot (\frac{d}{\lambda}) \cdot (\frac{2}{\pi} \cdot (\frac{h_t + h_r}{d})^2) \tag{3.13}$$

де, d – відстань поширення, λ – довжина хвилі, h_t – висота передавача, h_r – висота приймач

$$\mathrm{L}_d = 6.9 + 20\log_{10}(\sqrt{(\frac{h\sqrt{2(d_1+d_2)}}{\lambda\sqrt{d_1 d_2}} - 0.1)^2 + 1} + \frac{h\sqrt{2(d_1+d_2)}}{\lambda\sqrt{d_1 d_2}} - 0.1) \tag{3.14}$$

де, h – це висота перешкоди над лінією зору між передавачем і приймачем, d_1 та d_2 – відстань від передавача і приймача до перешкоди, λ – довжина хвилі. Втрати значно залежать від висоти і відстані до перешкоди, а також від частоти

сигналу. Ці обчислення є важливими для точного моделювання поширення сигналу в складних умовах, коли пряме поширення хвилі порушується об'єктами на шляху сигналу. При плануванні систем радіоелектронної боротьби (РЕБ), яка створює завади для стільникових мереж, важливо враховувати всі ці компоненти для точного прогнозування ефективності завад. Знання втрат сигналу допомагає оптимізувати потужність передавачів завад, розташування передавачів та інші параметри, щоб забезпечити максимальну ефективність створення перешкод.[17]

ВИСНОВОК ДО РОЗДІЛУ 3

У даному розділі ми детально розглянули основні типи шумів, такі як білий, рожевий та коричневий шум, а також їх застосування в системах радіоелектронної боротьби (РЕБ). Білий шум, завдяки своєму рівномірному розподілу енергії по всьому частотному спектру, часто використовується для створення ефективних широкосмугових перешкод. Рожевий шум, з його спектральною щільністю, що зменшується з частотою, та коричневий шум, який має ще більший нахил спектру, знаходять своє застосування для специфічних типів завад, що вимагають більш цілеспрямованого впливу на певні частотні діапазони.

Моделі пропагації, такі як модель втрат у вільному просторі (FSPL), модель Окамура-Хата та модель COST-231 Hata, є критичними для точного прогнозування втрат сигналу та планування ефективних завад. Ці моделі дозволяють врахувати різноманітні фактори середовища, такі як відстань, частота, висота антен та особливості міських, приміських і сільських умов. Формули, що використовуються в цих моделях, забезпечують розуміння того, як сигнал поширюється в різних середовищах та як правильно налаштувати параметри РЕБ для максимального ефекту. Виведення та використання формул втрат при пропагації, а також розрахунок потужності завади є ключовими елементами для успішного створення перешкод у стільникових мережах. Правильне застосування теоретичних моделей і практичних підходів дозволяє забезпечити ефективну протидію стільниковому зв'язку, мінімізуючи його надійність та продуктивність.

Таким чином, розуміння характеристик різних шумів та моделей пропагації є основою для розробки і впровадження стратегій радіоелектронної боротьби, що дозволяє ефективно порушувати роботу стільникових мереж і забезпечувати виконання завдань в умовах сучасного радіоелектронного протистояння.

4 ПРИНЦИП РОБОТИ СТІЛЬНИКОВОГО ЗВ’ЯЗКУ

4.1. Вступ

Стільниковий зв'язок є складною системою, яка забезпечує передачу інформації за допомогою радіохвиль. З точки зору фізики, функціонування стільникових мереж базується на принципах електромагнітного випромінювання, модуляції сигналів, розповсюдження радіохвиль та інтерференції. Стільниковий зв'язок є невід'ємною частиною сучасного життя, забезпечуючи безперервний зв'язок мільйонам користувачів по всьому світу. З огляду на складність технологій, що лежать в його основі, важливо розуміти фізичні принципи, які дозволяють мобільним мережам функціонувати ефективно та надійно. Стільниковий зв'язок базується на передачі та прийомі радіохвиль, що використовуються для передачі голосових дзвінків, текстових повідомлень, даних та мультимедійного контенту. У цьому розділі розглядаються основні фізичні принципи, що лежать в основі роботи стільникових мереж.

4.2 Електромагнітне випромінювання

Електромагнітне випромінювання — це процес випромінювання енергії у вигляді електромагнітних хвиль, які складаються з осцилюючих електричних і магнітних полів. Ці хвилі поширюються у вакуумі зі швидкістю світла (приблизно 300,000 км/с) і можуть проходити через різні середовища, включаючи повітря, скло, воду тощо. Електромагнітний спектр охоплює широкий діапазон частот, від дуже низьких (радіохвилі) до дуже високих (гамма-випромінювання). У стільникових мережах використовуються радіохвилі в діапазоні від 700 МГц до 3,5 ГГц для технологій 4G LTE та до 100 ГГц для новітніх технологій 5G. У стільникових мережах електромагнітні хвилі використовуються для створення зв'язку між мобільними пристроями і базовими станціями. Мобільні телефони перетворюють голос або дані в електромагнітні сигнали, які потім передаються до найближчої базової станції. Базова станція приймає ці сигнали і передає їх через мережу до пункту призначення, де вони перетворюються назад у голос або дані. Основні характеристики

електромагнітних хвиль, що впливають на їх застосування в стільникових мережах це частота, довжина хвилі, амплітуда та швидкість поширення.

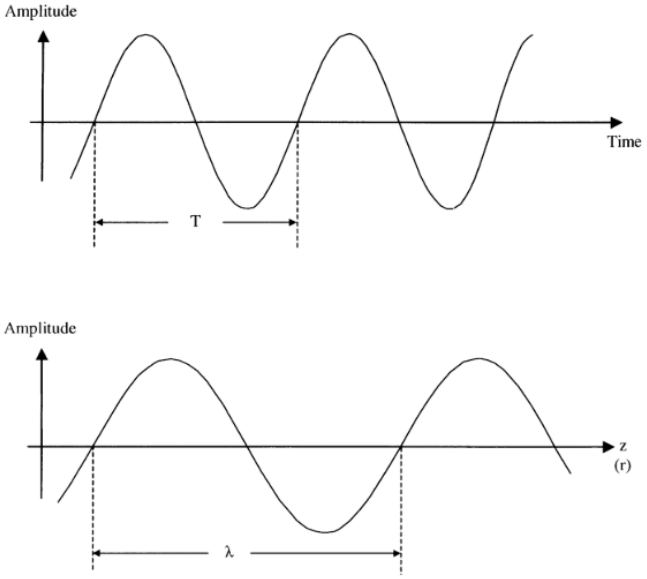


Рисунок 4.2.1 – Зображення періоду (T) та довжини хвилі (λ) на синусоїді хвилі.

При поширенні таких хвиль можуть відбуватись такі явища: затухання, розсіювання, рефракція, відбиття та дифракція.[18]

4.3. Структура стільникової мережі

Стільникова мережа забезпечує підключення терміналів до бездротового доступу до телефонної мережі загального користування, по іншому PSTN (Public Switched Telephone Network). Зона покриття забезпечується стільниками, на які діляться покриття базової станції (БС)

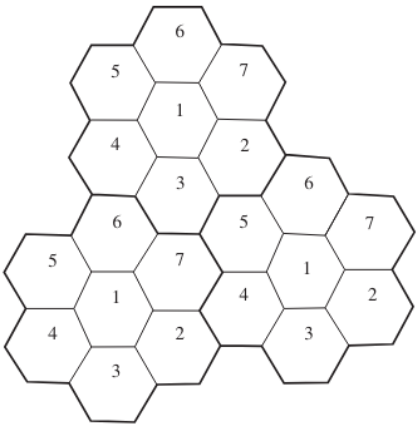


Рисунок 4.3.1. – Зона покриття поділена на стільники

БС є стаціонарною і з'єднана з центром комутації мобільного зв'язку (MTSO).

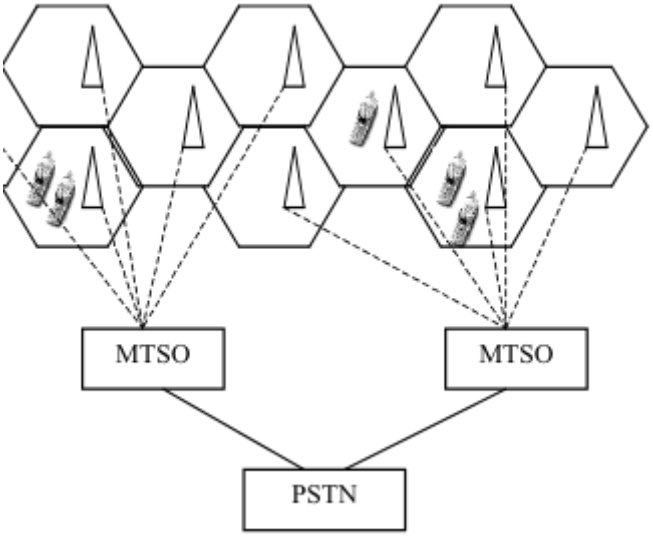


Рисунок 4.3.2. – З’єднання терміналів з MTSO та PSTN

Базові станції можуть містити різні конфігурації та набори антен. Одна базова станція може підтримувати одночасно 2G/3G/4G різних частот для кожної технології. Частотний спектр, виділений для стільникового зв'язку, дуже обмежений. Успіх сучасної стільникової мережі в основному пов'язаний з концепцією повторного використання частот. Саме тому зона покриття поділяється на стільники, кожна з яких обслуговується БС. Кожній БС (або комірці) призначена група частотних діапазонів або каналів. Щоб уникнути радіоінтерференції, група каналів, призначених для однієї комірки, повинна відрізнятися від групи каналів, призначених для сусідніх каналів, призначених сусіднім стільникам. Однак однакова група каналів може бути призначена двом коміркам, які знаходяться на достатній відстані одна від одної, щоб радіоканальна інтерференція між ними була в межах допустимої межі. Якщо для стільникового зв'язку виділено загалом M каналів, а зона покриття складається з N стільників, то на основі моделі повторного використання частот із сімома стільниками в зоні покриття одночасно доступно MN/7 каналів. Це й є пропускна здатність мережі на цій території. Через стрімке зростання кількості абонентів мобільного зв'язку, поточної пропускної здатності мережі може бути недостатньо. Одним із методів збільшення пропускної здатності мережі без виділення додаткового частотного спектру є розщеплення стільників. Ця технологія полягає у зменшенні розміру стільника шляхом зниження висоти розташування антени базової станції. [19][20]

4.4. Завади в стільниковій мережі

Завади у стільниковій мережі є результатом небажаного електромагнітного випромінювання, яке впливає на передачу сигналів між мобільними пристроями та базовими станціями. Такі завади можуть значно погіршити якість зв'язку, призводячи до втрат сигналу, збільшення кількості помилок, зниження швидкості передачі даних та навіть повної втрати зв'язку. Існують кілька механізмів за якими розрізняють вид завад який був накладений на сигнал БС. Затухання це поглинання енергії внаслідок проходження через різні середовища, наприклад будівлі, дерева або гори. Розсіювання це відбиття напрямку хвилі через взаємодію з дрібними перешкодами або нерівностями на їхньому шляху хвилі. Відбивання електромагнітних хвиль від поверхонь, таких як будівлі або земля, створює множинні шляхи для сигналу і може викликати інтерференцію. Згинання хвиль навколо кутів або країв перешкод призводить до зміни амплітуди та фази сигналу.

Інтерференція — це явище, при якому два або більше електромагнітних сигналів перекриваються в просторі, що призводить до утворення нового сигналу, амплітуда та фаза якого залежать від амплітуди та фази складових сигналів. Це явище має значний вплив на якість зв'язку у стільникових мережах. Інтерференція може бути конструктивною та деструктивною. Конструктивна відбувається, коли сигнали, що накладаються, перебувають у фазі один з одним, що призводить до збільшення амплітуди результуючого сигналу. Деструктивна відбувається, коли сигнали, що накладаються, мають протилежні фази, що призводить до зменшення амплітуди або повного погашення результуючого сигналу.

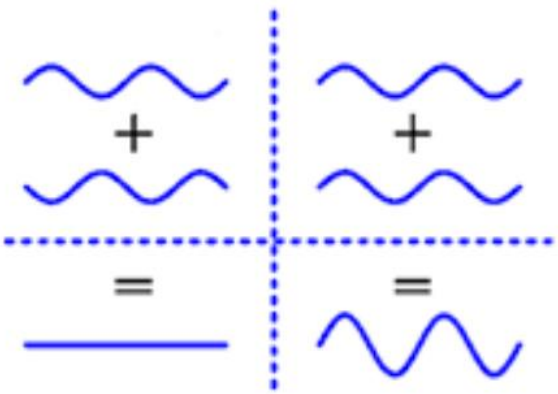


Рисунок 4.3.1 – Деструктивна та конструктивна інтерференція

Також види інтерференції поділяються на:

- Внутрішньоканальну
- Міжканальну
- Інтерсимвольну

Внутрішньоканальна відбувається, коли два або більше передавачів використовують однакову частоту. Це типово для стільникових мереж, де частоти можуть повторно використовуватися у різних сотах.

Частотний спектр – це цінний ресурс, який поділений на неперекривні частотні смуги, які присвоюються різним коміркам. Проте, після певної географічної відстані, ці частотні смуги повторно використовуються, тобто одні й ті ж смуги частот присвоюються іншим віддаленим коміркам. Саме через це явище повторного використання частот виникає внутрішньоканальне заважання в стільникових мобільних мережах. Таким чином, крім бажаного сигналу зсередини комірки, на приймач з небажаних передавачів, розташованих (далеко) в інших комірках, на тих самих частотах (внутрішньоканальні сигнали) приходять сигнали, що призводить до погіршення роботи приймача. [21]

Міжканальна інтерференція – виникає, коли сигнали з сусідніх каналів перекриваються через недостатню фільтрацію, що призводить до змішування сигналів і створення завад. Недосконалі фільтри на стороні приймача дозволяють сигналу суміжної частоти змішуватися з фактичною смугою пропускання. Якщо сила сигналу суміжного каналу стає занадто високою, базовій станції буде складно відрізнити фактичний сигнал мобільного телефону від потужного сигналу сусіднього мобільного телефону.

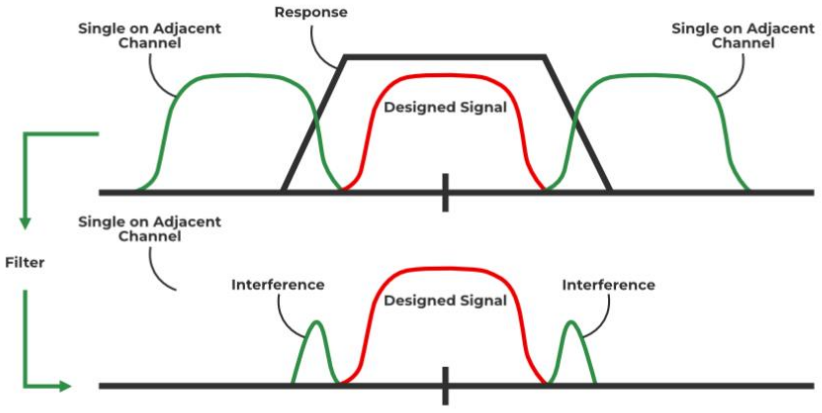


Рисунок 4.3.2. – Демонстрація роботи міжканальної інтерференції

Сусідні канали використовують близькі частоти, що може призвести до того, що сигнали з цих каналів будуть заважати один одному.[22]

Інтерсимвольна інтереференція виникає, коли символи, що передаються, накладаються один на одного через багатопроменеве поширення або недостатню ширину каналу, що призводить до спотворення сигналу.[23]

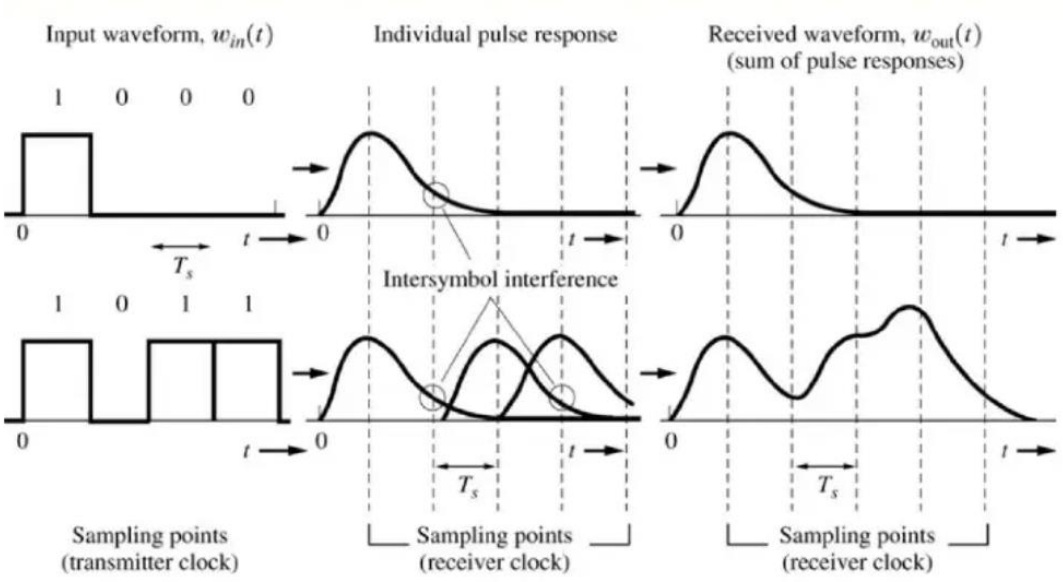


Рисунок 4.3.3. – Інтерсимвольна інтереференція

ВИСНОВОК ДО РОЗДІЛУ 4

У цьому розділі було описано основні аспекти роботи стільникового зв’язку. Розглянута структура з якої складається стільникова мережа та як сигнал передається між її складовими. Також Стільникові мережі постійно розвиваються, щоб відповідати зростаючим потребам користувачів. Нові технології, такі як 4G і 5G, пропонують більш високі швидкості передачі даних та більшу ємність мережі, що робить можливим нові програми та послуги. Але присутні і мінуси стільникової мережі, які також були описані, це саме внутрішньомережева інтерференція, зовнішні завади та природні завади. Вони значно можуть впливати на роботу стільникової мережі та доступність сервісів. Сучасні стільникові мережі використовують різноманітні алгоритми для оптимізації використання ресурсів, управління навантаженням, поліпшення якості обслуговування та забезпечення надійності мережі.

5 МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ВПЛИВ ЗАВАД НА СТІЛЬНИКОВУ МЕРЕЖУ

5.1. Вступ

Для моделювання та впливу завад на стільникову мережу я буду використовувати ПЗ Atoll. Atoll є потужним інструментом для планування і оптимізації бездротових мереж, що дозволяє детально аналізувати вплив різних факторів на якість зв'язку. В цьому розділі будуть розглядатись наступні аспекти:

- Основи стільникового зв'язку: Розгляд принципів роботи стільникових мереж, фізичних процесів передачі даних та основних компонентів мережі.
- Теоретичні аспекти завад та РЕБ: Аналіз видів завад, які можуть виникати в стільникових мережах, та основних методів радіоелектронної боротьби.
- Методологія моделювання: Опис підходів до моделювання завад у ПЗ Atoll, налаштування параметрів для імітації впливу РЕБ, та використання різних сценаріїв для дослідження.
- Результати моделювання та аналіз: Представлення отриманих результатів, їх аналіз та висновки щодо впливу завад на роботу базових станцій і якість обслуговування користувачів.

5.2. Створення стільникової мережі

Для дослідження я буду використовувати базову станцію яка буде розташована на плоскій місцевості. Це буде показувати об’єктивну оцінку впливу завад, адже програма не буде враховувати перешкоди ландшафту та будівель. Місцерозташування м. Київ, ТЦ “SkyMall”, він розташований на виїзді з Північного мосту. Будівля розташована навколо дуже низької забудови, навколо розташована паркова зона. На цьому півострові відсутні багатоповерхівки та будь-які зміни висоти ландшафту. З розміщенням БС можна ознайомитись на рис. 5.2.1.

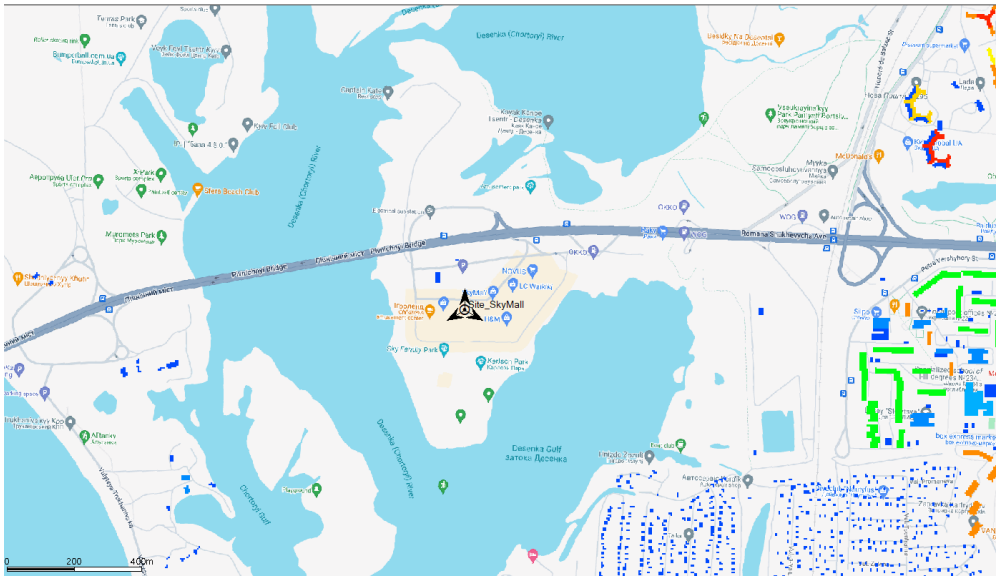


Рисунок 5.2.1. – Розташування БС

Для початку буде проводитись аналіз частоти 2100 МГц. Налаштуванням БС (рис. 5.2.2.) прості, висота кожного стільника 50 м, кут нахилу 4 °.

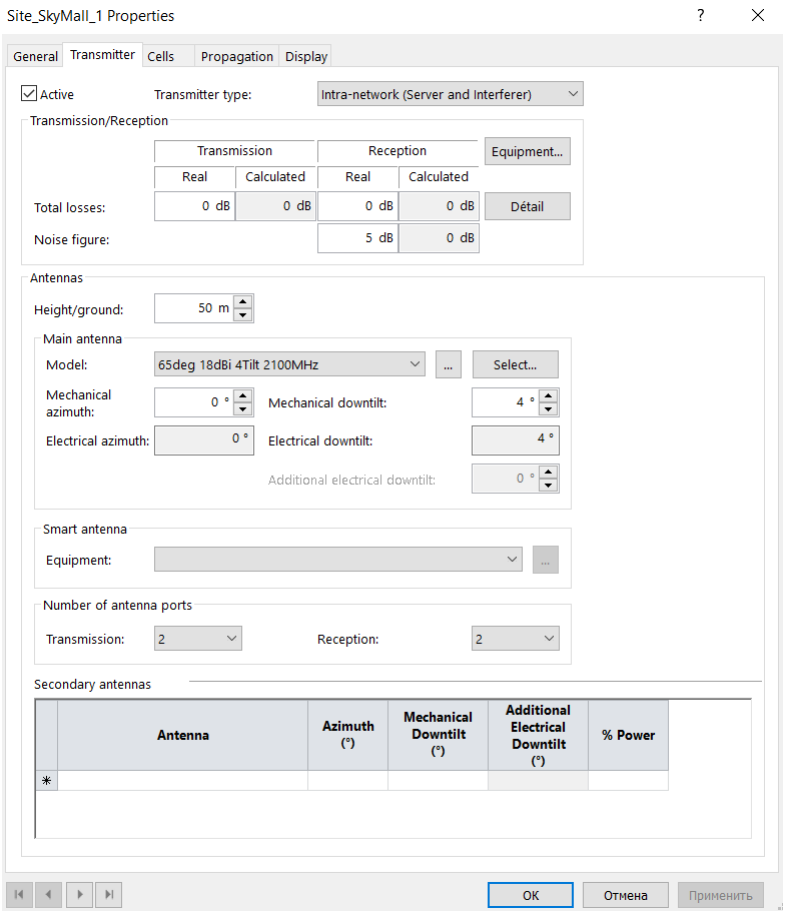


Рисунок 5.2.2. – Налаштування БС

Дані налаштування є стандартними і є об’єктивними для даної місцевості і дослідження. Розрахувавши покриття без всіляких завад можна побачити що БС покриває потрібну місцевість і на дані прорахунки можна опиратись в подальших дослідженнях (рис. 5.2.3).

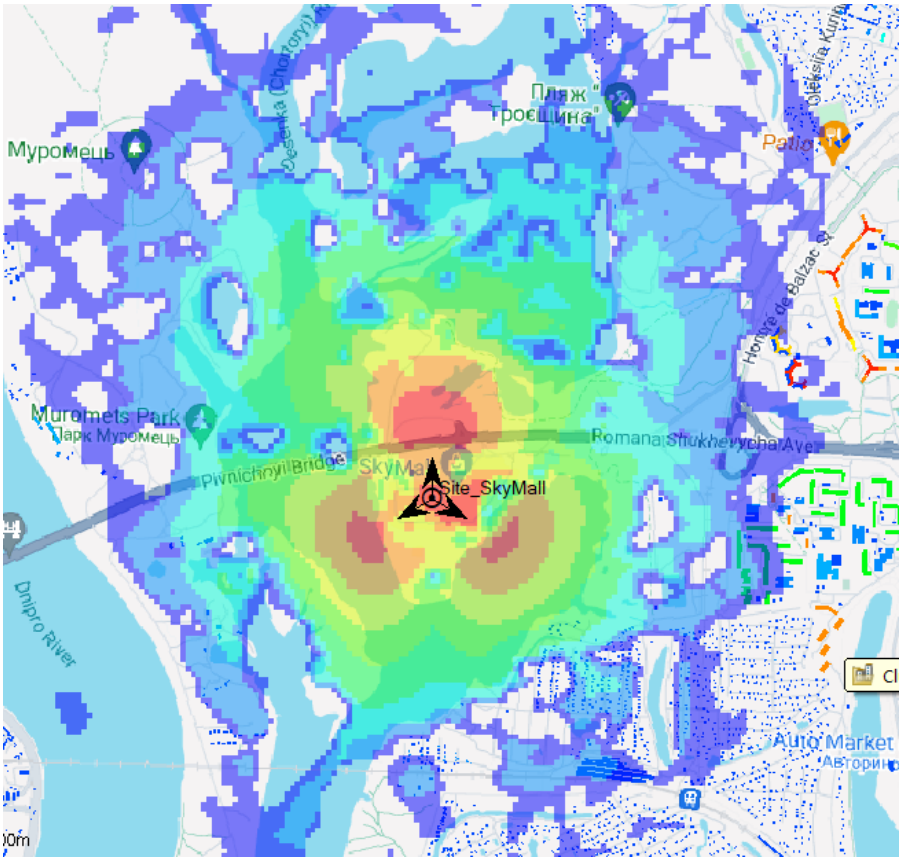


Рисунок 5.2.3. – Розраховане покриття БС

5.3. Дослідження впливу завад на мережу

Щоб показати вплив завад ПЗ Atoll забезпечує детальним налаштуванням параметрів стільників. Розрахунок Coverage by Quality Indicator (DL) в програмному забезпеченні Atoll демонструє покриття мережі за якістю сигналу у низхідному каналі (Downlink, DL). Цей показник дозволяє оцінити, наскільки добре базові станції покривають територію з точки зору якості сигналу, яку отримують мобільні пристрої користувачів. Він показує рівень якості сигналу, що передається від базових станцій до мобільних пристроїв. Це включає параметри, такі як SINR (Signal-to-Interference-plus-Noise Ratio) або RSRQ (Reference Signal Received Quality). Для демонстрації цього розрахунку ПЗ використовує BLER (Block Error Rate) - це відношення кількості помилкових блоків до загальної кількості переданих блоків. BLER вимірює відсоток блоків, які були передані з помилками та потребують повторної передачі для коректного прийому. Спочатку потрібно зробити розрахунок без моделювання завад на мережу. Оптимальні значення повинні бути 0.02-0.05 цього показника. При таких значеннях зберігається висока якість обслуговування та ефективне використання радіоресурсу.

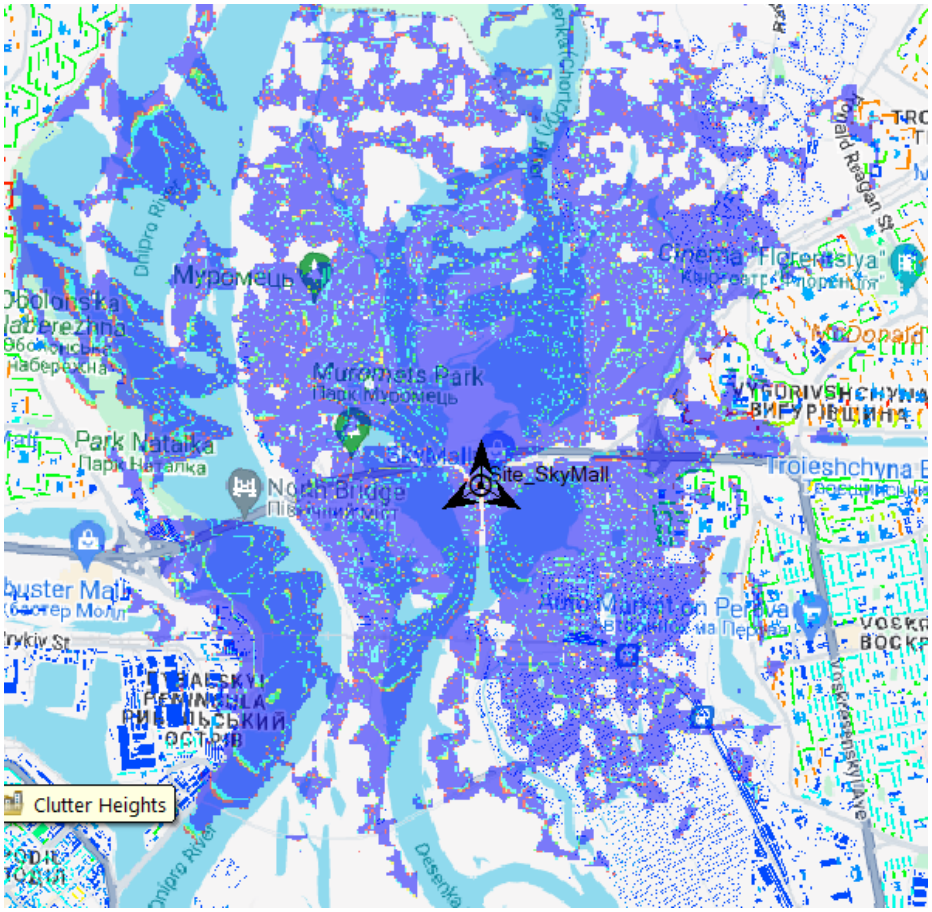


Рисунок 5.3.1. – Розрахунок покриття по показнику якості

Для імітації завад потрібно змінити параметри базової станції. В запропонованих налаштуваннях потрібно змінити параметри стільників які будуть відповідати за стійкість БС до завад. Потрібно змінити параметр Inter-technology UL Noise Rise (дБ) та Inter-technology DL Noise Rise (дБ) вони відповідають за рівень шуму між технологіями у висхідному та низхідному каналах. Inter-technology UL/DL Noise Rise (дБ) відображає зростання шуму в висхідній/нисхідній лінії зв'язку внаслідок впливу інших технологій, що працюють у тій самій частотній смузі або поруч з нею. Це зростання рівня шуму в висхідній лінії зв'язку, спричинене втручанням від інших технологій або систем, які працюють у тій самій або сусідній частотній смузі. Ці параметри важливі для моделювання завад у мережах, що підтримують кілька технологій одночасно. Для зрозумілої візуалізації буде змінено цей показник по різному на кожному стільнику. При ідеальних умовах цей показник має значення 0, тому буде обрано значення 10, 20 та 30.

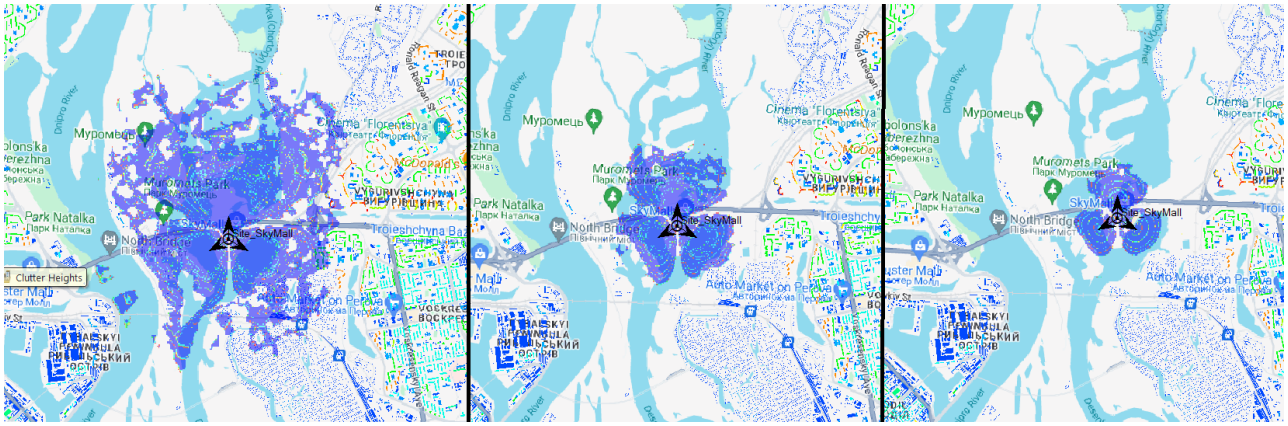


Рисунок 5.3.2. – Якість покриття після зміни показнику Inter-technology DL Noise Rise на 10, 20 та 30.дБ

Для точного порівняння були зроблені гістограми по кожному з випадків:

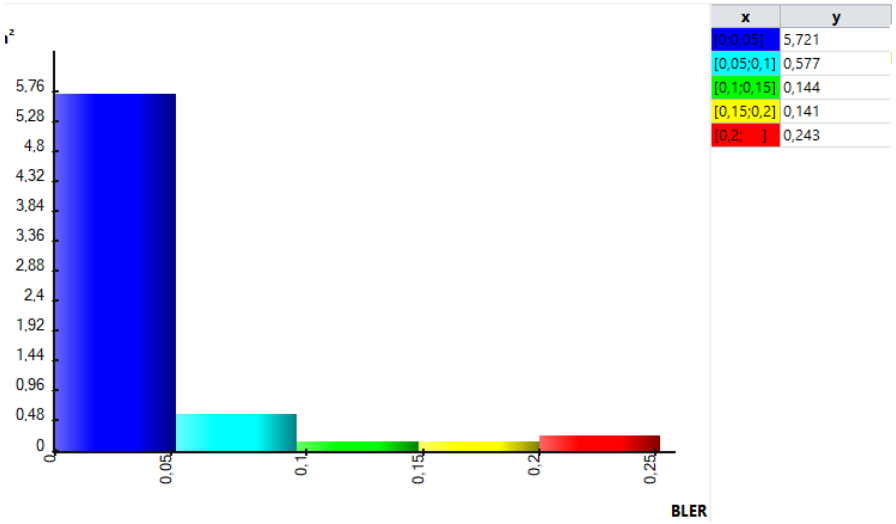


Рисунок 5.3.3. – Гістограма розрахунку при значенні 10 дБ

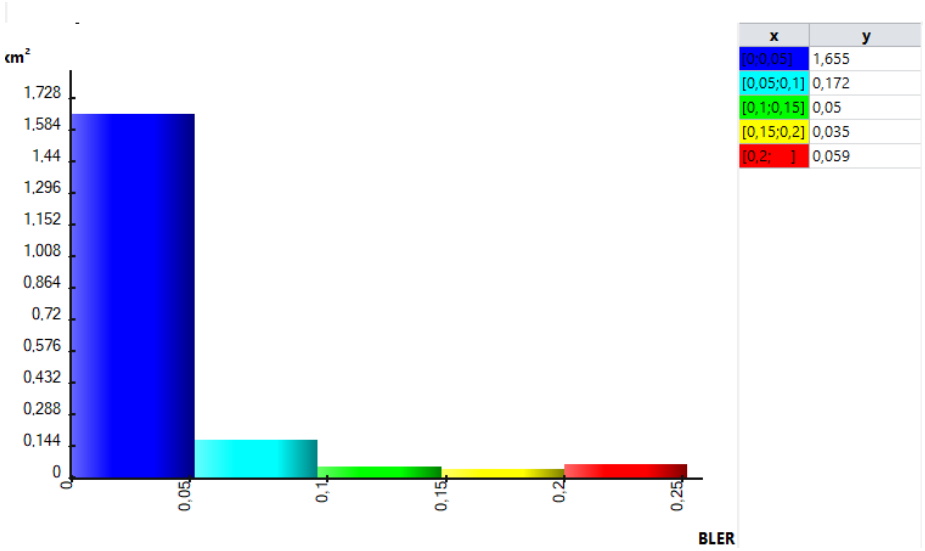


Рисунок 5.3.4. – Гістограма розрахунку при значенні 20 дБ

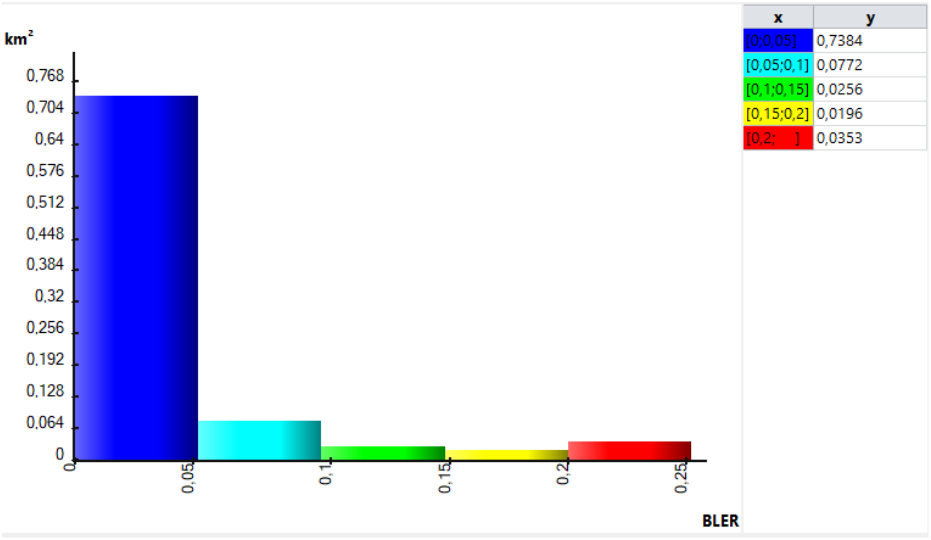


Рисунок 5.3.4. – Гістограма розрахунку при значенні 30 дБ

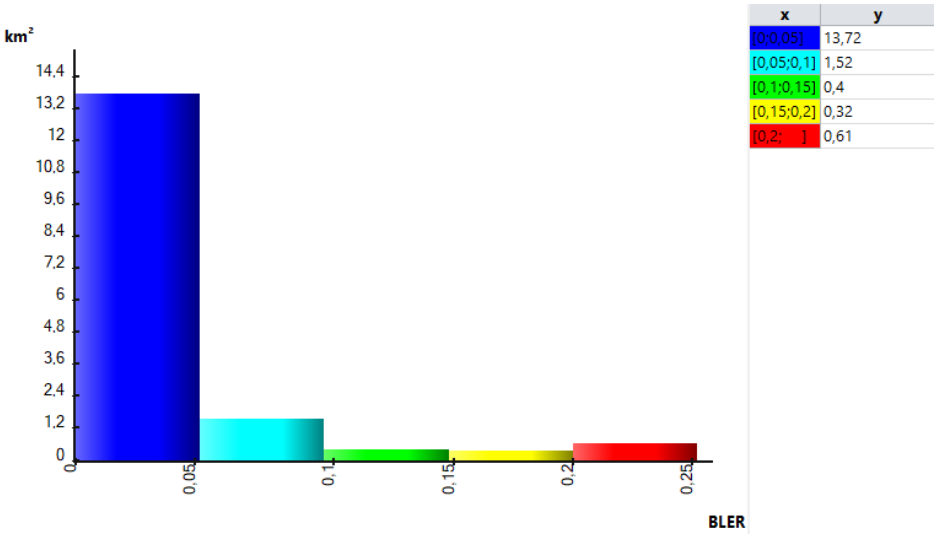


Рисунок 5.3.5. – Гістограма розрахунку при значенні 0 дБ

У порівнянні з початковою якістю покриття можна провести аналітику по показнику BLER який складає від 0 до 0,05 і взяти область покриття при якому показник має саме такі значення.

Таблиця 5.1. – Порівняння якості покриття.

Inter-technology DL Noise Rise (dB)	Відхилення від початкового значення 0
0	1
10	2,40
20	8,31
30	18,8

По таблиці 5.1 видно що різниця між 0 дБ та 10 дБ по області якісного покриття становить 2,4 разів , 0 дБ та 20 дБ – 8,31 разів та різниця між 0 дБ та 30 дБ – 18,8 разів. Це показує що чим більше значення рівню шуму задіяні на БС тим гірше якість покриття.

Також завади від РЕБ впливають на потужність БС, тому доцільно провести дослідження при якому буде зменшено потужність і перевірено якість покриття. Завади РЕБ можуть зменшити ефективне покриття базової станції. Через зниження SNR та інтерференцію, базова станція може не встигати обслуговувати користувачів на віддалених відстанях. Для LTE 2100 максимальне допустиме значення потужності це 50 дБм і при таких умовах базова станція буде забезпечувати стабільний зв'язок і доступність сервісів. При зменшенні потужності, покриття також буде зменшуватись. Проведемо аналіз в ПЗ Atoll. Для цього потрібно обрати розрахунок покриття по рівню сигналу в трьох випадках. В першому потужність залишається 50 дБм, в другому 46 дБм та в третьому 43 дБм (рис. 5.3.6.).

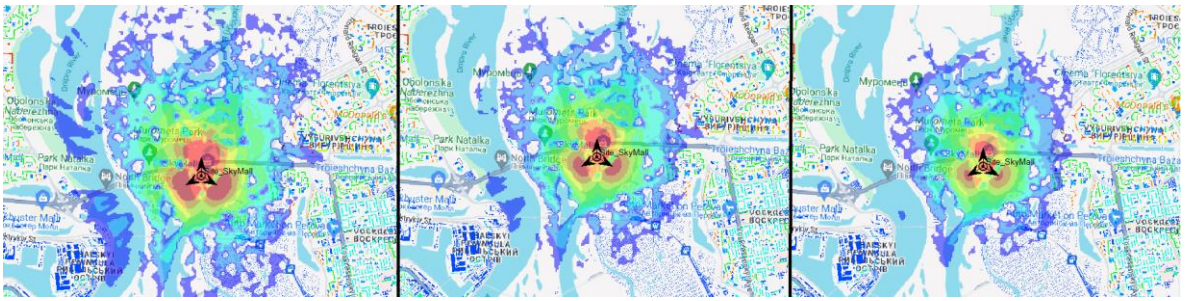


Рисунок 5.3.6. – Покриття за рівнем сигналу при 50 дБм, 46 дБм та 43 дБм потужностях

Згідно рисунку 5.3.6 можна спостерігати як покриття зменшилось. Для статистичного порівняння були створені гістограми за областю покриття.

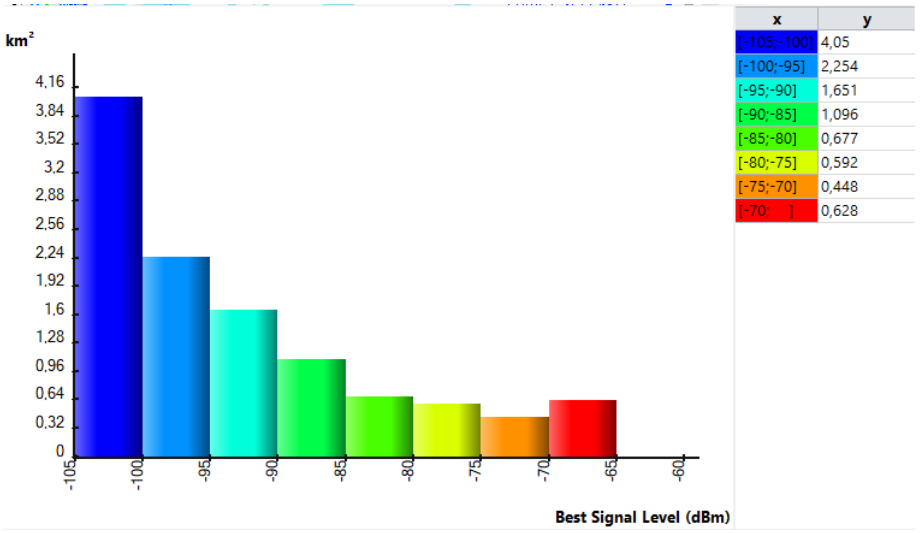


Рисунок 5.3.7. – Гістограма найкращого сигналу в області покриття при 50 дБм.

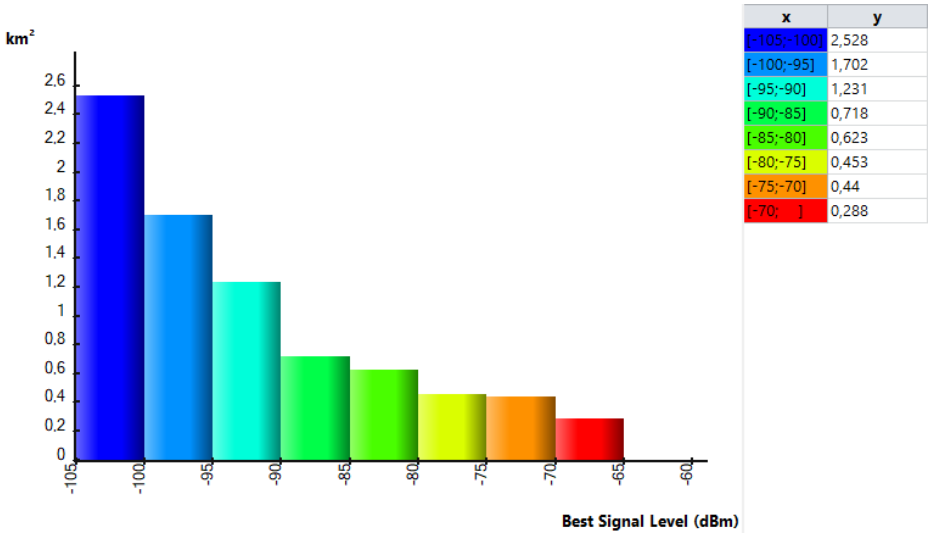


Рисунок 5.3.8. – Гістограма найкращого сигналу в області покриття при 46 дБм.

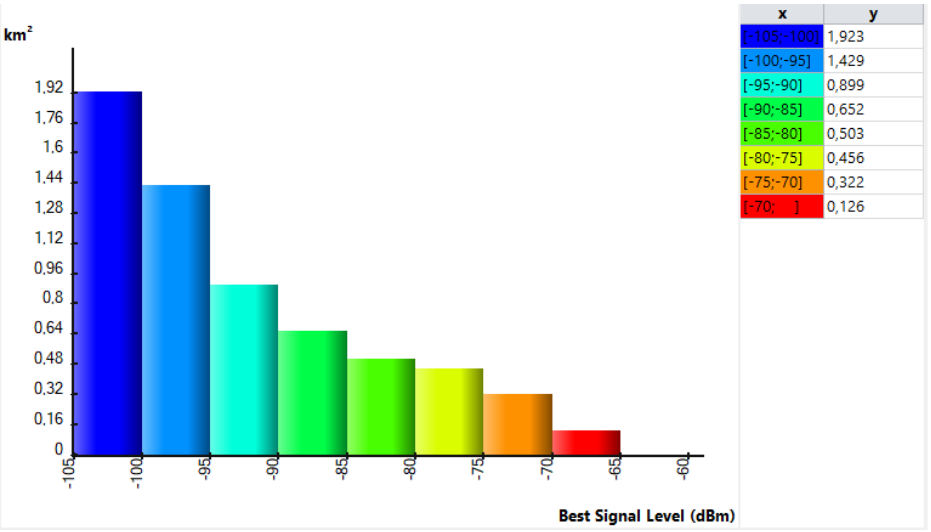


Рисунок 5.3.9. – Гістограма найкращого сигналу в області покриття при 43 дБм.

Для порівняння візьмемо область найкращого покриття при якому рівень сигналу становить -70 дБм і нижче.

Таблиця 5.2. – Порівняльна таблиця покриття за рівнем сигналу.

Потужність БС, дБм	50	46	43
50	1	2,18	4,98

Згідно таблиці 5.2. можна побачити що при зменшенні потужності з 50 дБм на 46 дБм зона найкращого пориття зменшується 2,18 разів, а при зменшенні з 50 дБм до 43 дБм зона зменшується в 4,98 разів. При збільшенні потужності базової станції виникають проблеми з живленням, адже збільшується споживання електроенергії. БС потребує в удосконаленні системи живлення в таких випадках. При цьому, система охолодження також має бути модернізована щоб охолоджувати надпотужну базову станцію. Потрібно використовувати кабеля з більшою пропускною здатністю та встановлювати більш потужні трансформатори. В сучасних реаліях оператори зв’язку застосовують для LTE 2100 саме потужність від 43 дБм до 50 дБм що еквівалентно 20 – 80 Вт. Ці значення потужності забезпечують стабільну роботу стільників, при якому станція не потребує додаткового живлення та не перевантажує лінії електроживлення і не потребує додаткових систем охолодження.

Далі потрібно дослідити вплив на швидкість передачі даних в умовах підвищення інтерференції та шуму. Для цього потрібно використовувати налаштування БС Max PUSCH C/(I+N) в dBm. Де PUSCH - Physical Uplink Shared Channel, є одним із основних каналів для передачі користувацьких даних у висхідному напрямку. C/(I+N) - співвідношення потужності сигналу до інтерференції та шуму. Зменшення цього параметру може імітувати підвищений рівень інтерференції та шуму, який створюється засобами РЕБ. Це призведе до зниження якості прийому сигналу від мобільних пристроїв, що може проявитися у вигляді зниження швидкості передачі даних, збільшення затримок та частоти помилок. Він відповідає за максимальне співвідношення сигналу до інтерференції та шуму на фізичному каналі висхідного зв'язку.

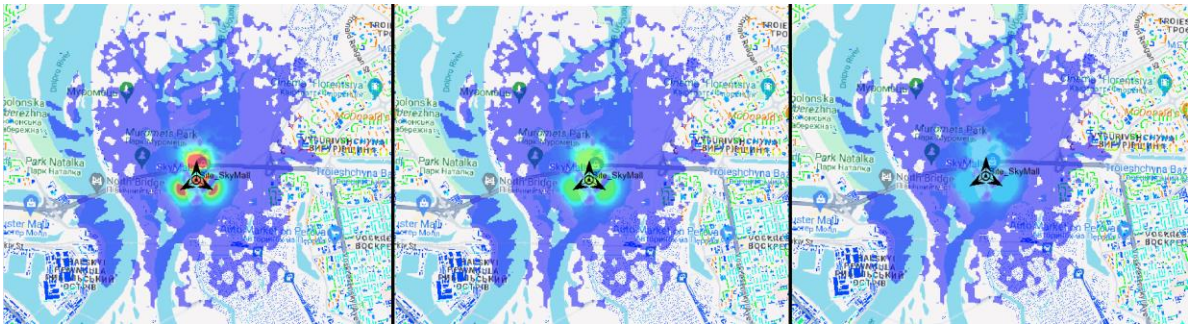
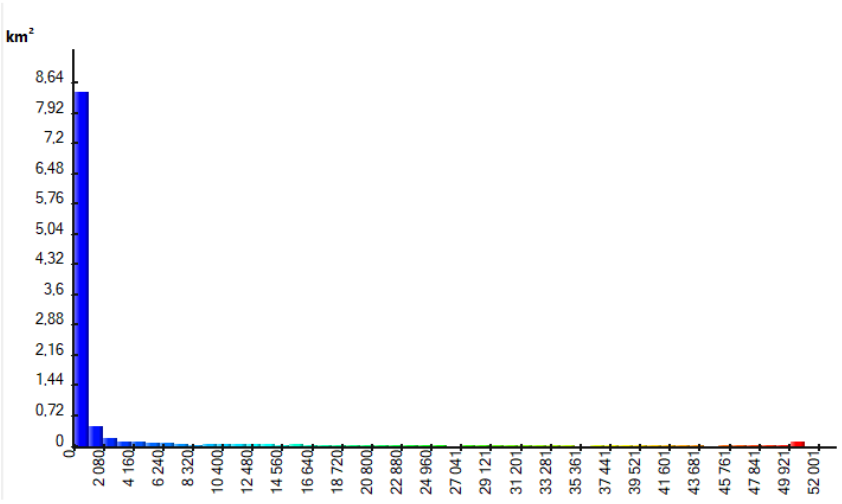
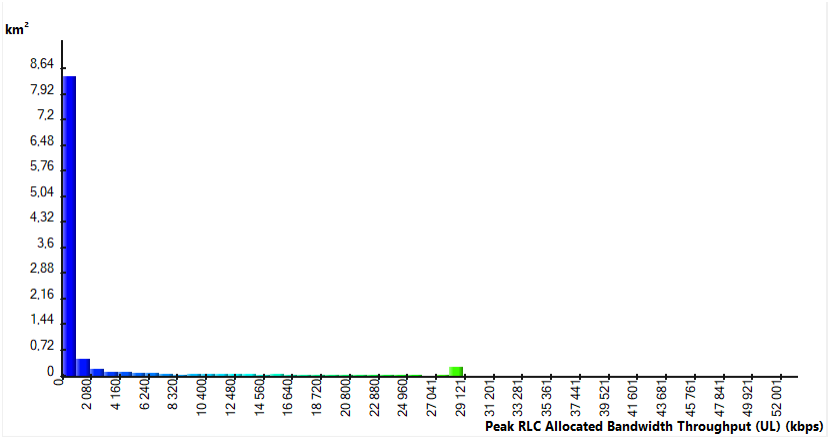


Рисунок 5.3.10 – Рівень пропускної здатності



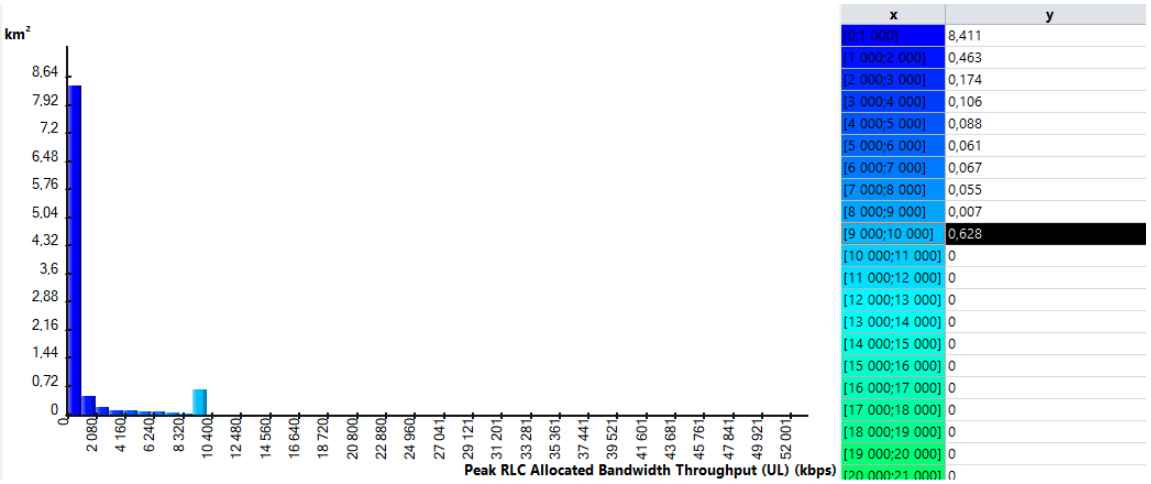
x	y
[31 000;32 000]	0,012
[32 000;33 000]	0,008
[33 000;34 000]	0,006
[34 000;35 000]	0,011
[35 000;36 000]	0
[36 000;37 000]	0,006
[37 000;38 000]	0,008
[38 000;39 000]	0,005
[39 000;40 000]	0,006
[40 000;41 000]	0,006
[41 000;42 000]	0,006
[42 000;43 000]	0,004
[43 000;44 000]	0,004
[44 000;45 000]	0
[45 000;46 000]	0,006
[46 000;47 000]	0,006
[47 000;48 000]	0,002
[48 000;49 000]	0,006
[49 000;50 000]	0,004
[50 000;]	0,106

Рисунок 5.3.11 – Гістограма пропускної здатності при Max PUSCH C/(I+N) 20 дБ



x	y
[15 000;16 000]	0,029
[16 000;17 000]	0,018
[17 000;18 000]	0,006
[18 000;19 000]	0,018
[19 000;20 000]	0,019
[20 000;21 000]	0,013
[21 000;22 000]	0,019
[22 000;23 000]	0,012
[23 000;24 000]	0,016
[24 000;25 000]	0,012
[25 000;26 000]	0,009
[26 000;27 000]	0
[27 000;28 000]	0,006
[28 000;29 000]	0,238
[29 000;30 000]	0
[30 000;31 000]	0
[31 000;32 000]	0
[32 000;33 000]	0
[33 000;34 000]	0
[34 000;35 000]	0
[35 000;36 000]	0

Рисунок 5.3.12 – Гістограма пропускної здатності при Max PUSCH C/(I+N) 15 дБ



x	y
[0;1 000]	8,411
[1 000;2 000]	0,463
[2 000;3 000]	0,174
[3 000;4 000]	0,106
[4 000;5 000]	0,088
[5 000;6 000]	0,061
[6 000;7 000]	0,067
[7 000;8 000]	0,055
[8 000;9 000]	0,007
[9 000;10 000]	0,628
[10 000;11 000]	0
[11 000;12 000]	0
[12 000;13 000]	0
[13 000;14 000]	0
[14 000;15 000]	0
[15 000;16 000]	0
[16 000;17 000]	0
[17 000;18 000]	0
[18 000;19 000]	0
[19 000;20 000]	0
[20 000;21 000]	0

Рисунок 5.3.13 – Гістограма пропускної здатності при Max PUSCH C/(I+N) 10 дБ

За гістограмами пікові значення зменшується в залежності зменшення показника. При 10 дБ максимальна пропускна здатність становить 9000-10000 Кбит/с, при 15 дБ – 28000-29000 Кбит/с та при 20 дБ – більше ніж 50000 Кбит/с. Показник 20 дБ є оптимальним значенням, які забезпечують високу якість сигналу та стабільність зв'язку у більшості випадків. Значення більше за 20 використовуються за умови мінімальної інтерференції і зебезпечують найвищу якість зв’язку.

В наступному дослідженні буде імітовано роботу радіоелектронної боротьби шляхом направленого сигналу високої потужності. Для першого дослідження розташуємо РЕБ на відстані 6 км від базової станції. Та налаштуємо сигнал на частоту 2100 Мгц та встановимо потужність сигналу 60 дБм що еквівалентно потужності 1 кВт. Розрахуємо покриття за показником співвідношення інтерференція/шум без впливу РЕБ (рис. 5.3.14) та з впливом (рис. 5.3.15).

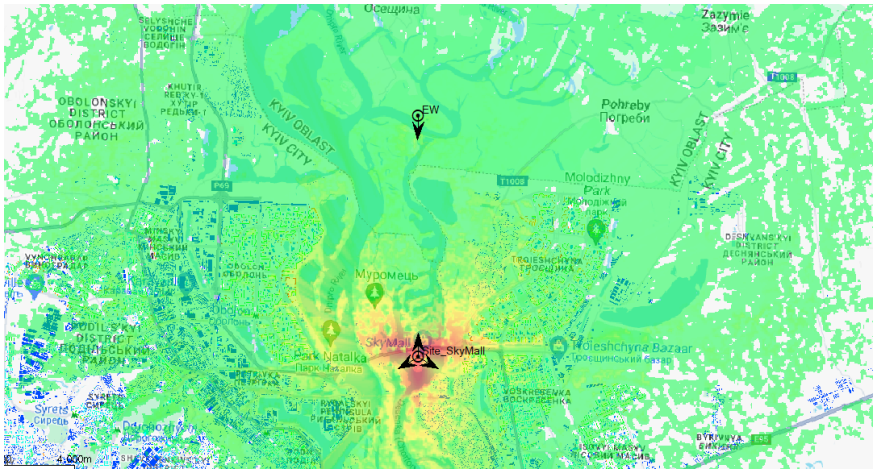
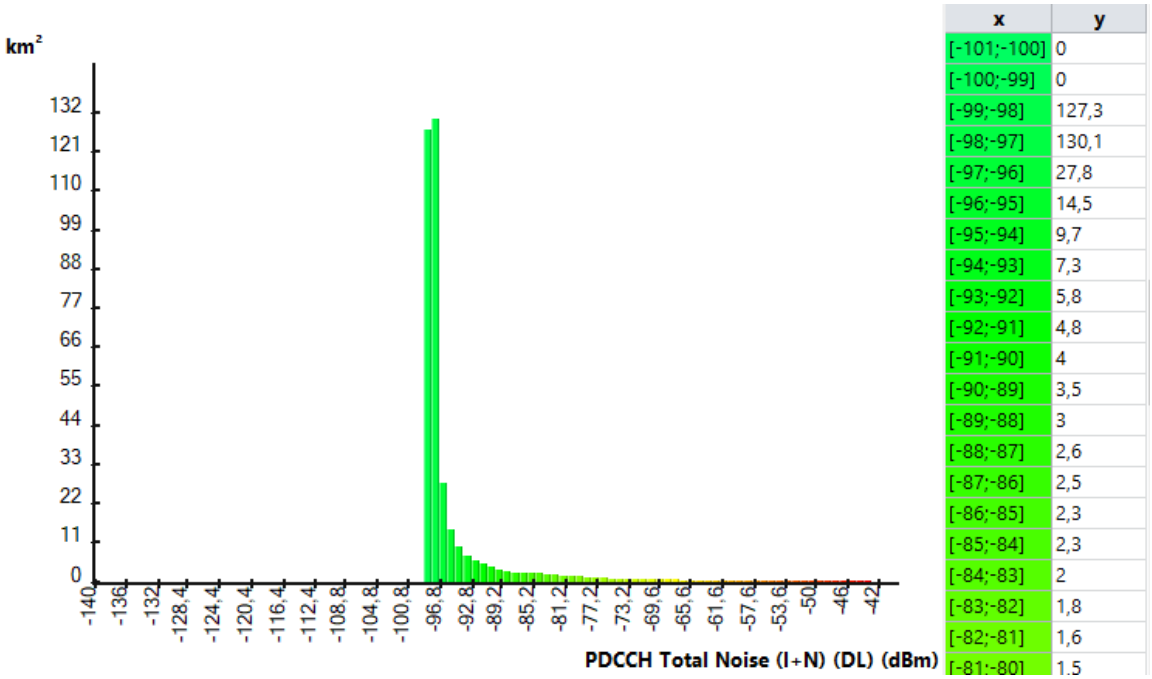


Рисунок 5.3.14 – Розрахунок покриття без впливу завад



x	y
[-101;-100]	0
[-100;-99]	0
[-99;-98]	127,3
[-98;-97]	130,1
[-97;-96]	27,8
[-96;-95]	14,5
[-95;-94]	9,7
[-94;-93]	7,3
[-93;-92]	5,8
[-92;-91]	4,8
[-91;-90]	4
[-90;-89]	3,5
[-89;-88]	3
[-88;-87]	2,6
[-87;-86]	2,5
[-86;-85]	2,3
[-85;-84]	2,3
[-84;-83]	2
[-83;-82]	1,8
[-82;-81]	1,6
[-81;-80]	1,5

Рисунок 5.3.15 – Гістограма розрахунку покриття за відношенням інтерференції/шум без впливу завад.

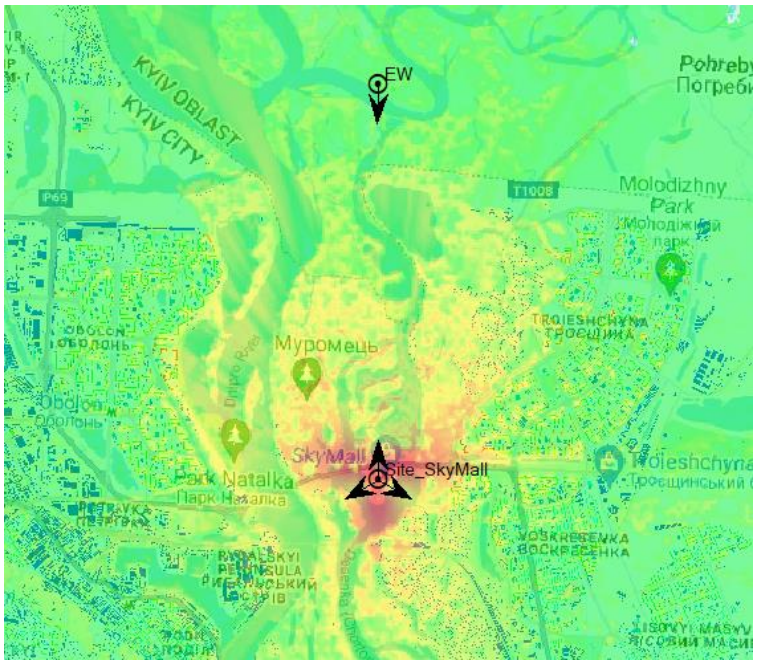


Рисунок 5.3.16 – Розрахунок покриття з впливом завад з розташуванням РЕБ на відстані 6 км.

Для об’єктивної оцінки відфільтрую покриття тільки по БС стільникової мережі і розрахую гістограму даного дослідження (рис. 5.3.15).

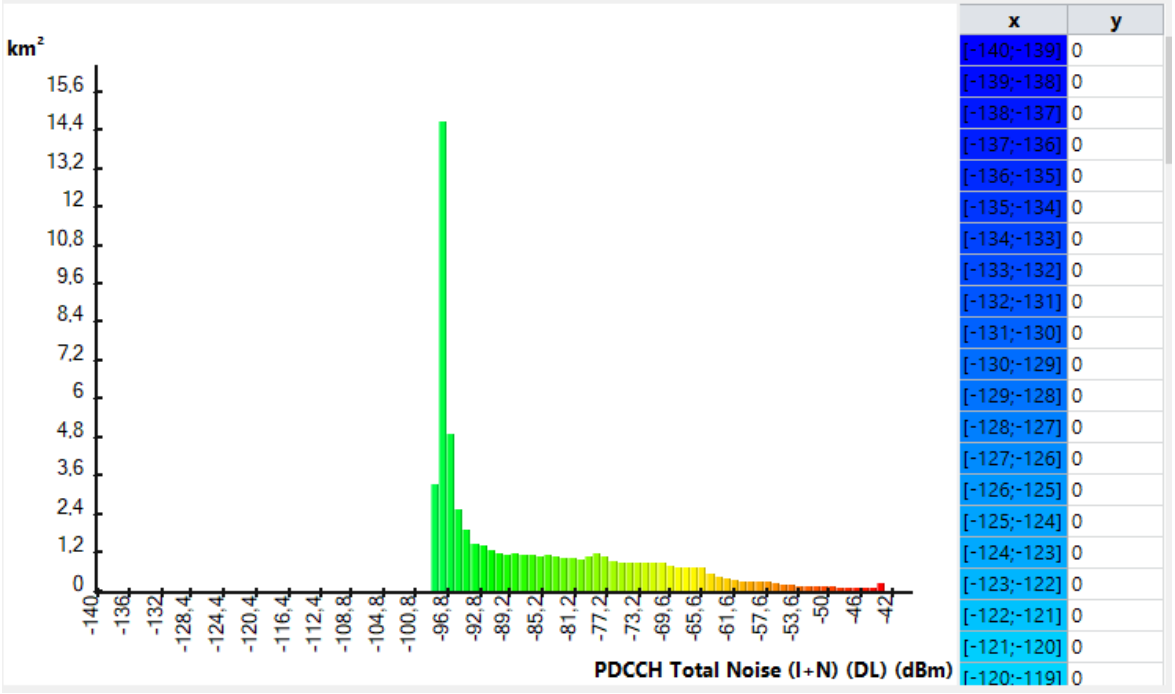


Рисунок 5.3.17 –Гістокрама покриття з впливом завад з розташуванням РЕБ на відстані 6 км.

В результаті ми отримуємо дещо збільшений процент шумів, якщо порівнювати рисунок 5.3.15 та 5.3.17. На гістограмі видно що покриття зменшилось у 8.8 разів, а відсоток шумів збільшився, це видно з показника PDCCH Total Noise (I+N) в області від -73,2 до 61,6. Далі розташуємо РЕБ на розташуванні 10 км. Параметри завади не змінюються.

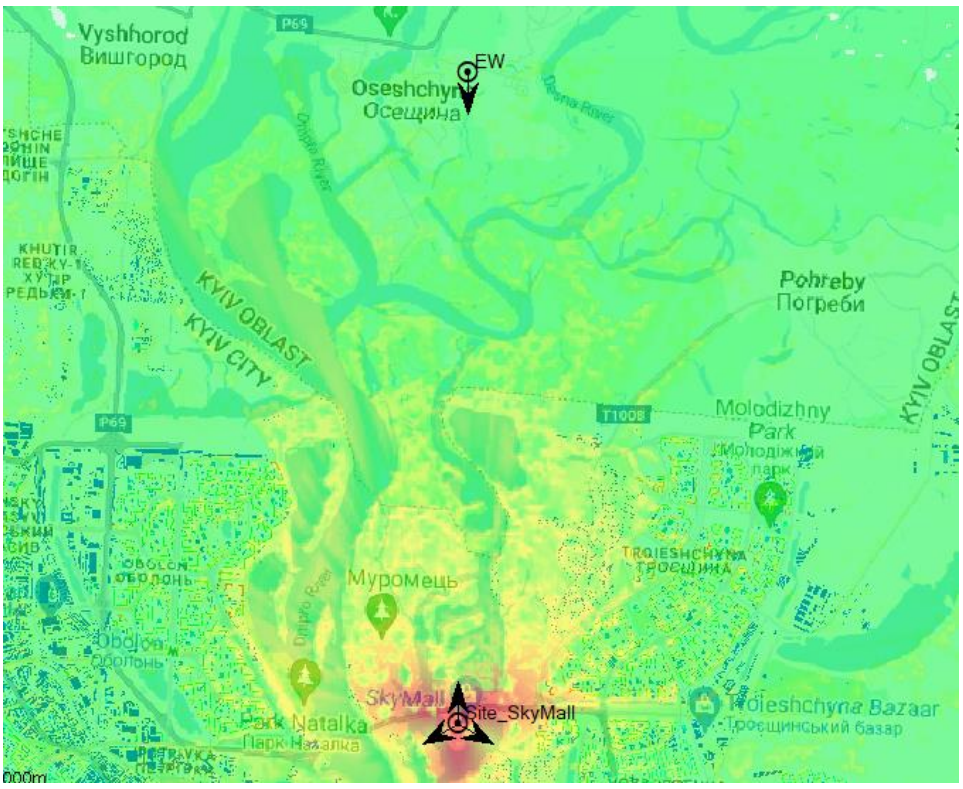
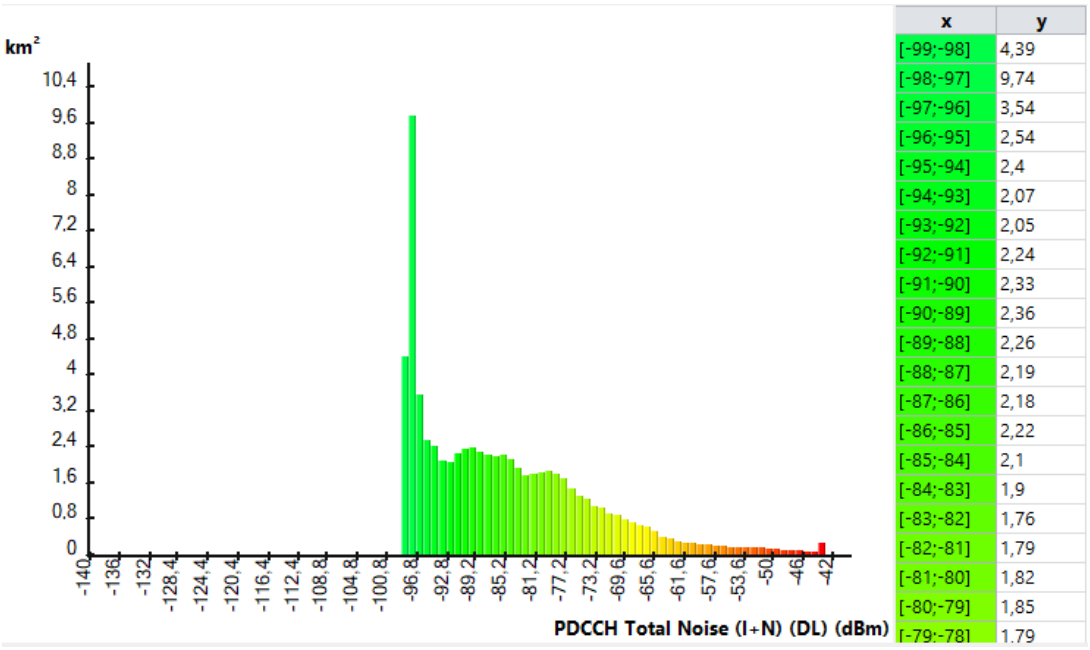


Рисунок 5.3.18 – Розрахунок покриття з впливом завад з розташуванням

РЕБ на відстані 10 км.



x	y
[-99;-98]	4,39
[-98;-97]	9,74
[-97;-96]	3,54
[-96;-95]	2,54
[-95;-94]	2,4
[-94;-93]	2,07
[-93;-92]	2,05
[-92;-91]	2,24
[-91;-90]	2,33
[-90;-89]	2,36
[-89;-88]	2,26
[-88;-87]	2,19
[-87;-86]	2,18
[-86;-85]	2,22
[-85;-84]	2,1
[-84;-83]	1,9
[-83;-82]	1,76
[-82;-81]	1,79
[-81;-80]	1,82
[-80;-79]	1,85
[-79;-78]	1,79

Рисунок 5.3.19 –Гістокрама покриття з впливом завад з розташуванням РЕБ на відстані 10 км.

Покриття зменшилось в 10 разів, базова станція продовжує піддаватись впливом завад та має значну кількість шумів.

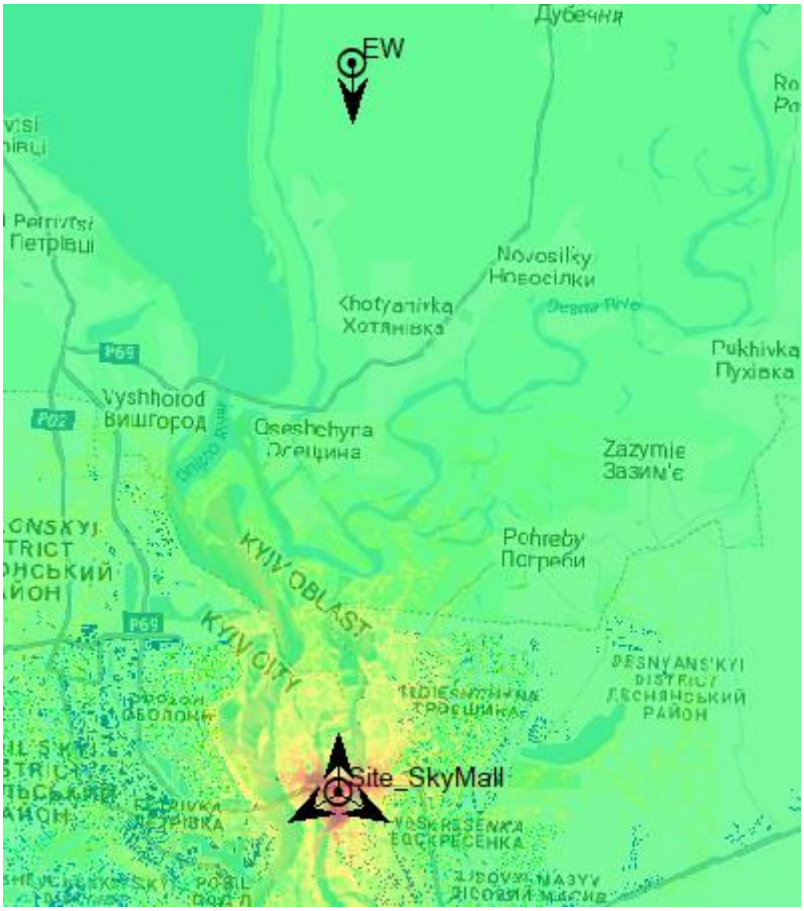


Рисунок 5.3.20 – Розрахунок покриття з впливом завад з розташуванням РЕБ на відстані 20 км.

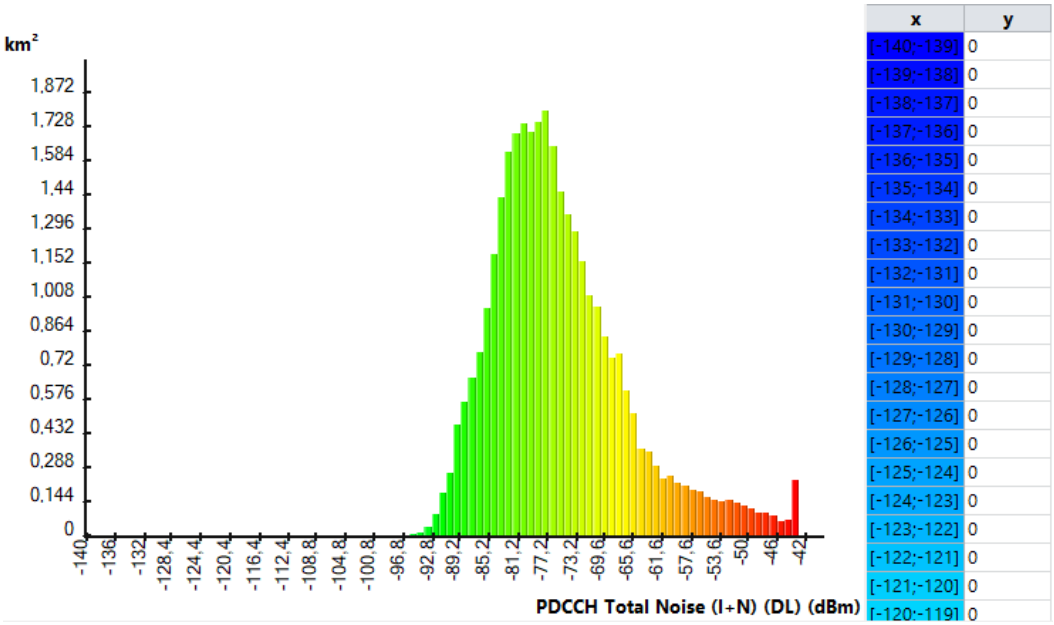


Рисунок 5.3.21 – Гістокрама покриття з впливом завад з розташуванням РЕБ на відстані 20 км.

Для наступних досліджень я буду використовувати модель пропагацій Лонглей-Райса на РЕБ заваді, на БС пропагація буде залишатись Окамуро-Хата. Перше дослідження при таких умовах буде здійснено при заваді на відстані 10 км.

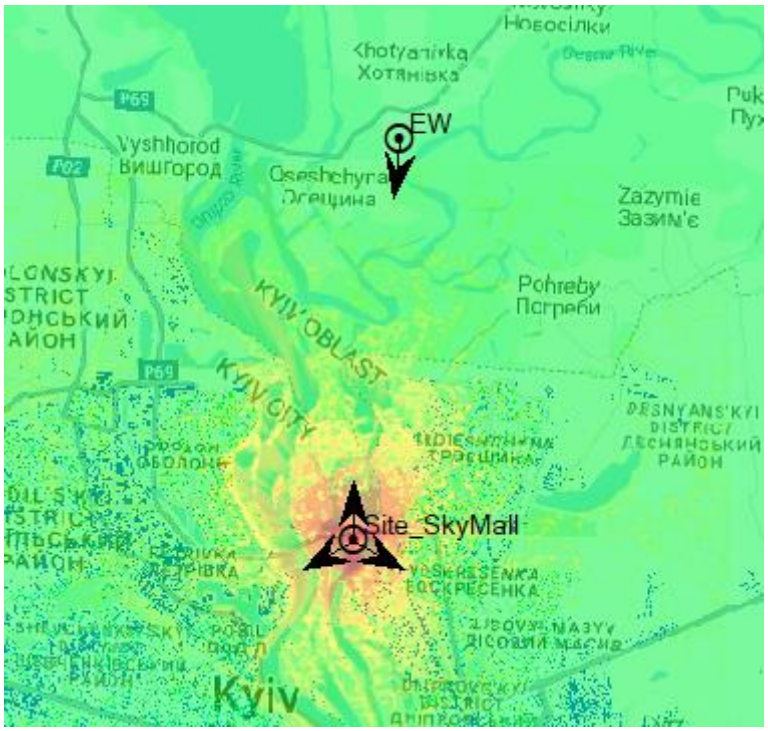


Рисунок 5.3.22 – Розрахунок покриття з впливом завад з розташуванням РЕБ на відстані 10 км з моделлю пропагації Лонглей-Райса.

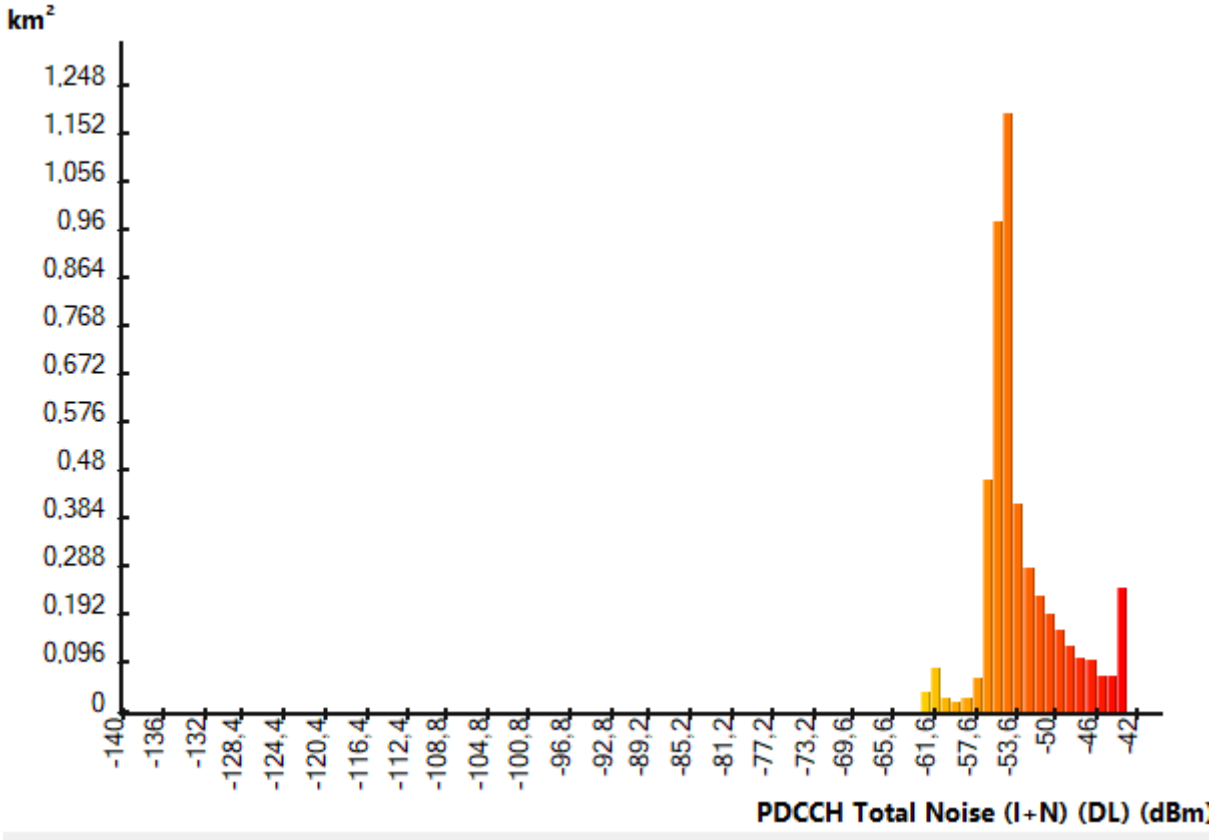


Рисунок 5.3.23 – Гістограма покриття з впливом завад з розташуванням РЕБ на відстані 10 км з моделлю пропагації Лонглей-Райса.

Після фільтрації по БС, можна спостерігати деградацію покриття та значне збільшення шумів. Середнє значення PDCCH Total Noise (I+N) дорівнює -53,08 дБм. Далі розташуємо на відстані 20 км і порівняємо результати.

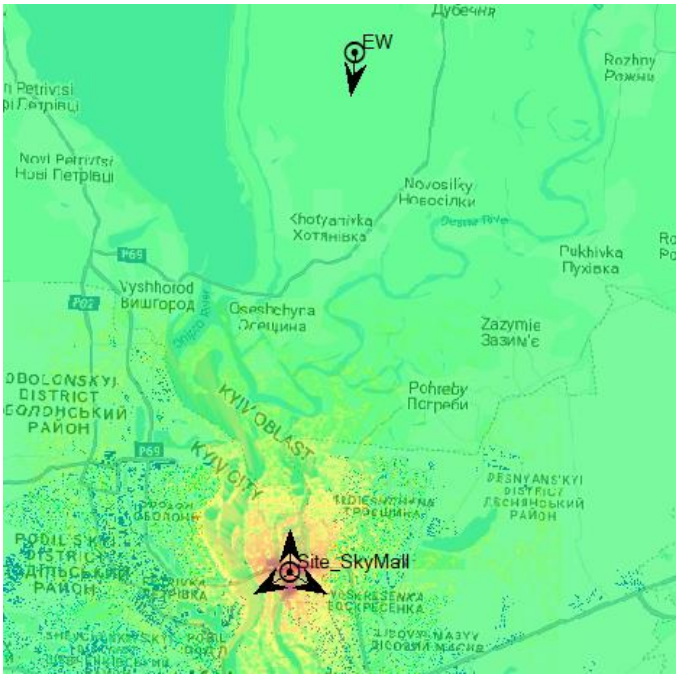


Рисунок 5.3.24 – Розрахунок покриття з впливом завад з розташуванням РЕБ на відстані 20 км з моделлю пропагації Лонглей-Райса.

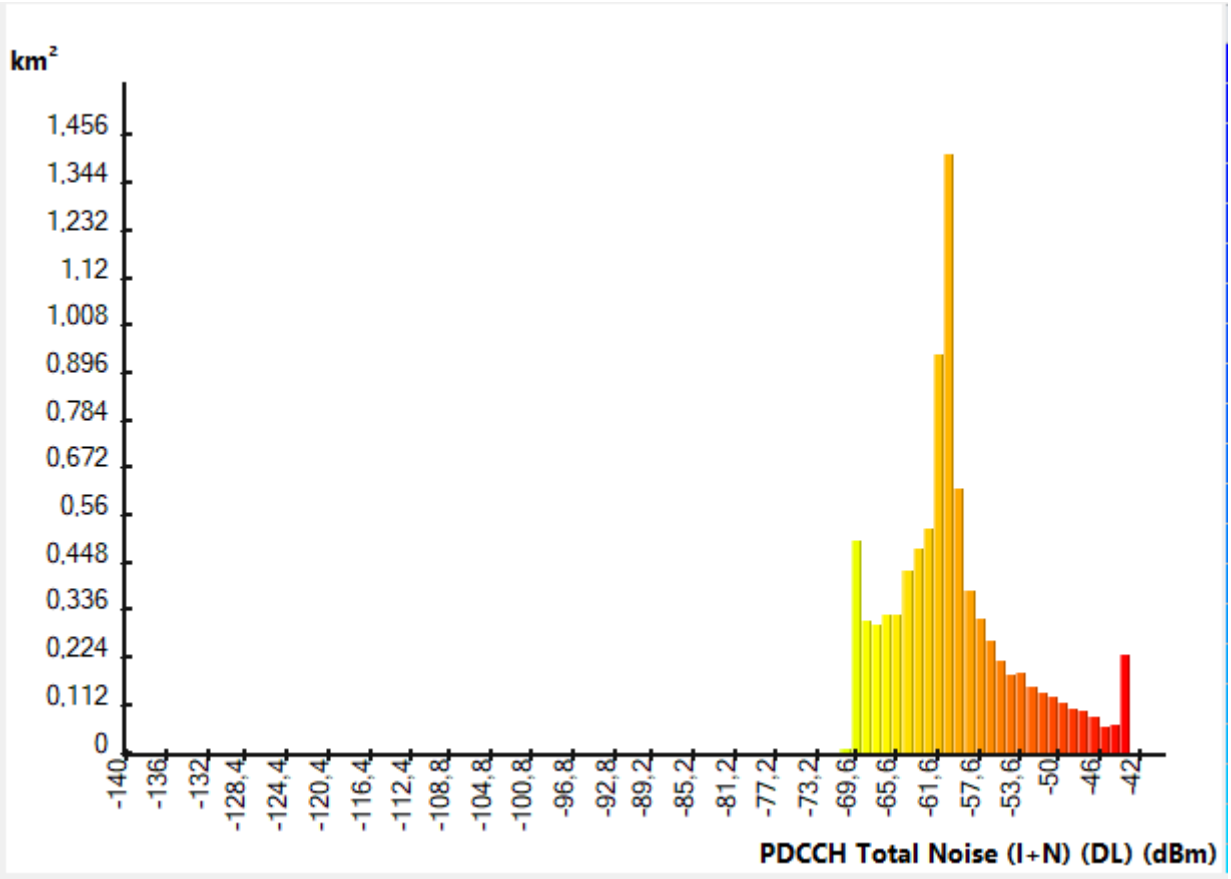


Рисунок 5.3.25 – Гістокрама покриття з впливом завад з розташуванням РЕБ на відстані 20 км з моделлю пропагації Лонглей-Райса.

Середнє значення показника PDCCH Total Noise (I+N) дорівнює -60,03 дБм. Модель пропагація Лонглей-Райса являється більш впливовою і деградації стають більш помітними. Під час аналізу втрат сигналу та ефективності створення завад на стільникову мережу, були розглянуті дві моделі поширення сигналу: Лонглей-Райса та Окамуро-Хата. Виявилося, що в моделі Лонглей-Райса кількість шуму та інтерференції на базовій станції значно більша, ніж у моделі Окамуро-Хата. Це пов’язано з різними підходами та компонентами втрат, які враховують ці моделі

ВИСНОВКИ ДО РОЗДІЛУ 5

У розділі, присвяченому дослідженню завад та їх впливу на базову станцію стільникового зв'язку, було проведено комплексний аналіз методів створення завад та моделей пропагації, які використовуються системами радіоелектронної боротьби (РЕБ). Розглянуто кілька моделей пропагації, зокрема модель Окамуро-Хата та Лонглей-Райса. Ці моделі допомагають прогнозувати втрати сигналу при різних умовах розповсюдження, що є критично важливим для оцінки ефективності РЕБ у створенні завад. Як завади РЕБ впливають на якість обслуговування в стільникових мережах, зокрема на показники, такі як BLER (Block Error Rate), інтерференція та рівень сигналу. Виявлено, що моделі пропагації, такі як Лонглей-Райса, можуть показувати більший вплив шуму та інтерференції порівняно з моделлю Окамуро-Хата, що вказує на важливість правильного вибору моделі для аналізу та протидії завадам.

6 ПРОТИДІЯ ЗАВАДАМ НА СТІЛЬНИКОВИЙ ЗВ’ЯЗОК ВІД РЕБ

6.1. Вступ

В цьому розділі будуть розібрані та проаналізовані методи протидії завадам на стільниковий зв’язок. Як було виявлено з розділу 5, завади можуть всебічно впливати на базову станцію, на доступність, покриття та на якість сигналу. Важливо знати як пом’якшувати або запобігати завади, потрібно враховувати різні фактори при виборі методів захисту. Буде проведений аналіз найсучасніших методів запобіганню та майбутнє захисту стільникового зв’язку від завад.

6.2. Метод розширення спектру

Метод розширення спектру DSSS (Direct Sequence Spread Spectrum) - це метод модуляції, який використовується для покращення стійкості до завад та безпеки в системах зв'язку. DSSS працює шляхом множення початкового сигналу на псевдовипадкову послідовність (шумоподібний код), що призводить до розширення його спектра. DSSS робить сигнал більш стійким до завад, оскільки завада також має бути розширена по всій частотній смузі, що робить її менш потужною. DSSS розподіляє потужність сигналу по широкій частотній смузі, що робить його менш помітним. Але при цьому цей метод також зменшує пропускну здатність сигналу при такому виді розширення. Він використовується в таких стандартах як GSM та CDMA. Псевдовипадкова послідовність - це бінарний код, який має властивості шуму, але генерується детермінованим способом. Ця послідовність відома як код поширювання спектра (SSC). Початковий сигнал множиться на псевдовипадкову послідовність, це призводить до розширення спектра сигналу. Далі цей сигнал передається на канал зв’язку. На приймальній стороні розширений спектр сигналу деміксується шляхом ділення на ту ж псевдопослідовності, яка використовувалась на стороні передавача. Це призводить до відновлення початковго сигналу. [24]

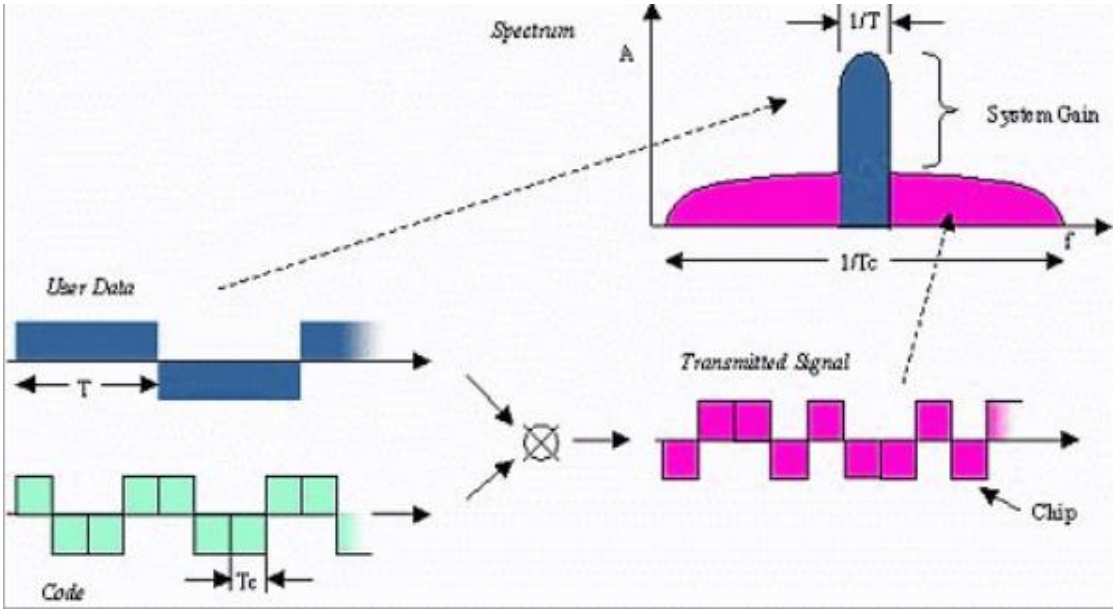


Рисунок 6.2.1 – Принцип роботи DSSS

6.3. Агрегація частот

Агрегація несучих частот (Carrier Aggregation, CA) — це техніка, яка використовується в мобільних мережах для підвищення швидкості передачі даних, та забезпечувати більш надійний та стійкий сигнал. Вона дозволяє одночасно використовувати декілька несучих частот для створення ширшого каналу для передачі даних, що збільшує пропускну здатність і зменшує затримку. Це робить мобільну мережу більш ефективною та швидкодійною. https://inseego.com/resources/5g-glossary/what-is-carrier-aggregation/

Це техніка, яка використовується в LTE-Advanced для збільшення частотної смуги пропускання шляхом об'єднання двох або більше компонентних носіїв (Component Carriers, CC). На початку цієї техніки було дозволено об'єднувати максимум 5 CC, що призводило до загальної смуги пропускання до 100 МГц (5 x 20 МГц). Нині існують пристрої, здатні агрегувати набагато більше CC, що призводить до набагато більшої пропускної здатності. CA можна використовувати в обох способах реалізації передачі даних у LTE: FDD (Frequency Division Duplex) та TDD (Time Division Duplex). Для висхідних (UL) і низхідних (DL) каналів у TDD смуги пропускання кожного CC, а також їх кількість зазвичай будуть однаковими. У FDD кількість CC для UL є такою ж

або меншою, ніж кількість DL CC. [25]

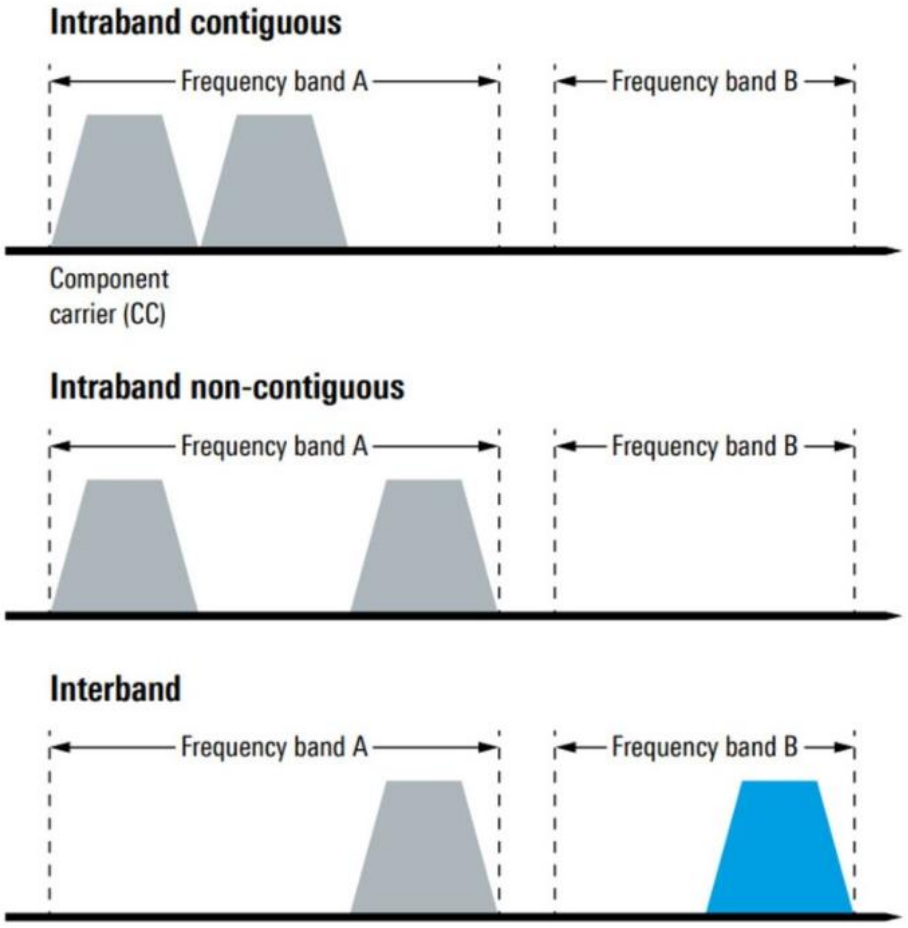


Рисунок 6.2.1 – Демонстрація роботи агрегації частот

CA розширює спектр, який використовується для передачі даних, роблячи його більш стійким до завад, сконцентрованих на певних частотах. Завдяки цьому завадам РЕБ стає складніше блокувати весь канал зв'язку, що дозволяє мобільним пристроям підтримувати зв'язок навіть у складних умовах. Термінал який підключений може перемикатись між компонентами частот, якщо якийсь з компонентів піддається завадам. Це робить зв’язок більш стійким до динамічних загроз.

6.3. Частотне рознесення

Використання кількох частот для передачі одного сигналу дозволяє знизити ймовірність того, що завада вплине на весь сигнал. LTE спирається на OFDM (Orthogonal Frequency Division Multiplex) як базову технологію модуляції та використовує пов'язані з нею схеми доступу OFDMA (Orthogonal Frequency Division Multiple Access) та SC-FDMA (Single Carrier Frequency Division Multiple

Access). OFDM розбиває сигнал на безліч вузькосмугових несучих, які модулюються даними з низькою швидкістю. Завдяки ортогональності несучих, їхні спектри не перекриваються, що усуває взаємну інтерференцію. Це досягається за рахунок чітко визначеного інтервалу між несучими, який дорівнює зворотній величині періоду символу.

При демодуляції сигнали OFDM мають цілу кількість циклів в рамках одного символу, що робить їхні взаємні впливи нульовими. Дані розподіляються по всіх несучих, що дозволяє використовувати методи корекції помилок для відновлення інформації, навіть якщо деякі несучі втрачаються через багатопроменевість. Низька швидкість передачі даних на кожній несучій робить OFDM стійкою до відбиття та міжсимвольної інтерференції. Це також відкриває можливість для одночастотних мереж, де всі передавачі можуть використовувати один канал.

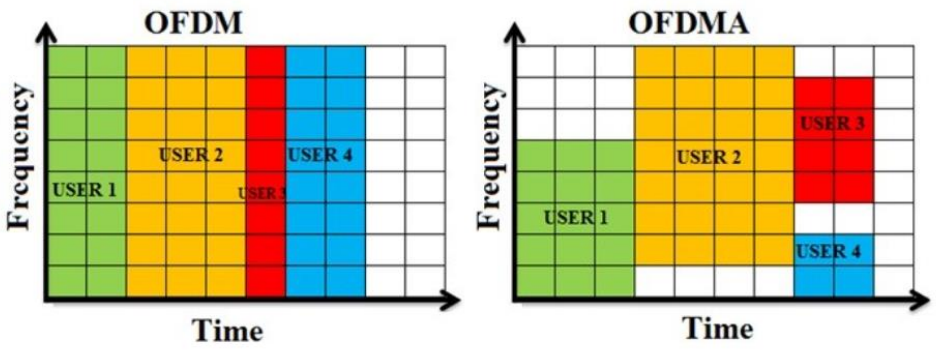


Рисунок 6.3.1 – Демонстарція роботи OFDM та OFDMA

В OFDMA піднесучі групуються в більші одиниці, які називаються підканалами, а ці підканали далі групуються в пакети, які можуть бути розподілені між користувачами бездротового зв'язку. Кожен розподіл пакети може змінюватися від кадру до кадру, а також в межах порядку модуляції. Це дозволяє базовій станції динамічно регулювати використання смуги пропускання відповідно до поточних системних вимог.

Крім того, оскільки кожен користувач споживає лише частину загальної смуги пропускання, потужність кожного користувача також може бути модульована відповідно до поточних системних вимог. Якість обслуговування (QoS) - це ще одна функція, яка може бути адаптована для різних користувачів в залежності від їх конкретного застосування, наприклад, для передачі голосу,

потокового відео або доступу до Інтернету. [26]

6.4. Функція HARQ

Функція HARQ (Hybrid Automatic Repeat Request) – ця функція допомагає виявляти та виправляти помилки, викликані завадами, шляхом повторного запиту пошкоджених пакетів. HARQ забезпечує надійність передачі даних, навіть в умовах сильних завад. Техніка повторного запиту з автоматичною перевіркою помилок (Hybrid Automatic Repeat Request, HARQ) - це потужний інструмент для підвищення надійності та ефективності передачі даних у мережах LTE. HARQ поєднує методи виявлення та виправлення помилок, гарантуючи точну передачу та отримання інформації.

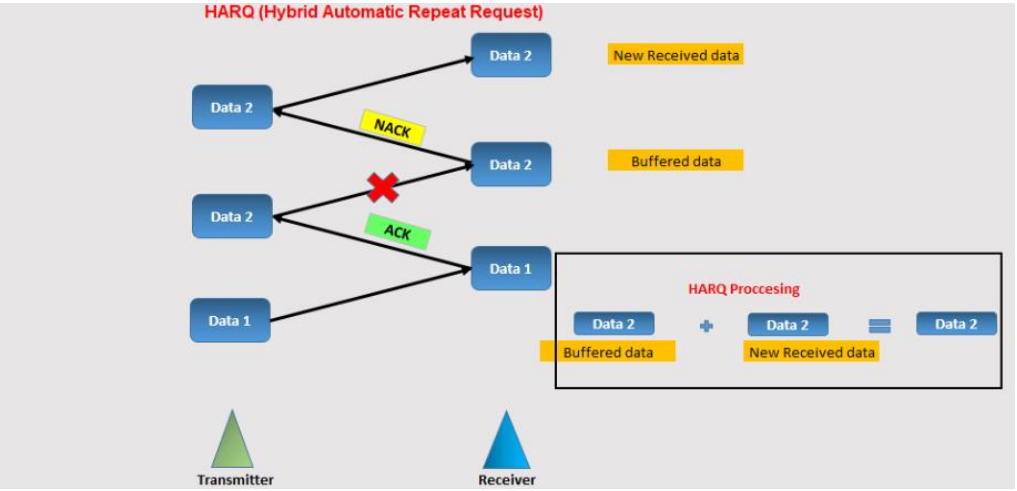


Рисунок 6.4.1 – Принцип роботи функції HARQ

Ця функція складається з ARQ та FEC. ARQ (Automatic Repeat Request) - це протокол передачі даних, який використовується в системах зв'язку, в тому числі в мережах LTE, для забезпечення надійної доставки даних. Це метод виявлення та виправлення помилок, які можуть виникнути під час передачі даних. Якщо помилок немає, отримувач надсилає відправнику повідомлення про підтвердження (ACK - Acknowledgement). Якщо виявлено помилки, отримувач надсилає відправнику повідомлення про негативне підтвердження (NACK - Negative Acknowledgement). Якщо отримано ACK, відправник переходить до наступного пакета, а якщо отримано NACK, відправник повторно надсилає той самий пакет (рис.6.4.1.). Цей процес повторюється, доки отримувач не підтвердить успішне отримання пакета без помилок. FEC - це процес, під час якого надлишкові дані додаються до оригінальних даних перед передачею.

Додаткові дані дозволяють приймачу виявляти і виправляти помилки без необхідності повторної передачі. Хоча додавання цих бітів збільшує розмір переданих даних, воно значно підвищує надійність. Завдяки спільній роботі цих двох функцій в HARQ, користувачі LTE можуть насолоджуватися швидким, безперебійним та надійним мобільним інтернетом. [27]

ВИСНОВОК ДО РОЗДІЛУ 6

У цьому розділі ми розглянули різні методи, які використовуються для захисту стільникового зв'язку від завад РЕБ. Важливо зазначити, що не існує єдиного універсального підходу до захисту стільникового зв'язку від завад РЕБ. Для досягнення максимального рівня безпеки необхідно використовувати комплексний підхід, який включає в себе різні методи та технології. Всі ці методи можна використовувати в комбінації для забезпечення ще більшого захисту. Сучасні технології, такі як частотне рознесення та агрегація несучих частот, забезпечують значну стійкість до завад шляхом використання широкого спектра частот і динамічного адаптивного управління ресурсами. Використання просторової диверсифікації за допомогою HARQ допомагає підвищити надійність передачі даних і зменшити вплив завад.

ВИСНОВОК

Дослідження, проведене в даній дипломній роботі, спрямоване на аналіз впливу радіоелектронної боротьби (РЕБ) на стільниковий зв’язок, виявило ряд важливих аспектів, які мають значення для забезпечення надійності та безпеки сучасних стільникових мереж. Розглянуті питання дозволили не лише глибше зрозуміти механізми впливу завад на роботу стільникових мереж, але й запропонувати ефективні методи захисту від цих завад. Проаналізовано вплив різних видів завад на якість зв'язку, включаючи природні явища та штучні. Особлива увага приділена аналізу методів РЕБ. Встановлено, що такого роду завади можуть призводити до значних перебоїв у зв'язку, втрати даних та порушення роботи стільникових мереж. Дослідження показало, що завади можуть значно знижувати рівень сигналу, що впливає на швидкість передачі даних та стабільність з'єднання. Встановлено, що цілеспрямовані атаки на базові станції можуть викликати перебої в роботі всієї мережі, створюючи ризики для критичної інфраструктури. Для зменшення впливу потрібно проводити розробку і впровадження адаптивних антенних систем, які можуть знижувати вплив завад на рівні обладнання, аналізувати та налаштовувати згідно небезпек. Використовувати алгоритми обробки сигналів, які дозволяють виявляти та мінімізувати вплив завад, покращуючи стійкість мережі до атак. Посилення захисту даних шляхом застосування сучасних методів шифрування та автентифікації для запобігання підміні та перехопленню сигналів. Результати даного дослідження можуть бути використані для покращення захисту стільникових мереж від РЕБ, що сприятиме забезпеченню безперебійної роботи комунікаційної інфраструктури, важливої для національної безпеки, економічного розвитку та добробуту громадян.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Statistics [Електронний ресурс] // International Telecommunications Union – Режим доступу до ресурсу: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

2. Які засоби РЕБ і як використовувались у війні за Нагірний Карабах [Електронний ресурс] // Defense Express. – 2021. – Режим доступу до ресурсу: https://defence-ua.com/army_and_war/jaki_zasobi_reb_i_jak_vikristovuvalis_u_vijni_za_nagirnij_karabah-5653.html

3. A.E. Spezio. Electronic warfare systems / A.E. Spezio // IEEE Transactions on Microwave Theory and Techniques / A.E. Spezio., 2002. – (IEEE). – С. 633 – 644.

4. Electromagnetic warfare [Електронний ресурс] // NATO. – 2023. – Режим доступу до ресурсу: https://www.nato.int/cps/en/natohq/topics_80906.htm#:~:text=The%20NATO%20JEWCS%20is%20based,Allied%20Commander%20Europe%20(SACEUR).

5. S. O'NEIL. Electronic Warfare and Radar Systems / S. O'NEIL. – California: Naval Air Warfare Center Weapons Division. – 455 с.

6. Digital Communication - Phase Shift Keying [Електронний ресурс] // tutorialspoint – Режим доступу до ресурсу: https://www.tutorialspoint.com/digital_communication/digital_communication_phase_shift_keying.htm.

7. Quadrature amplitude modulation [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Quadrature_amplitude_modulation.

8. What is electronic support? [Електронний ресурс] – Режим доступу до ресурсу: https://www.baesystems.com/en-us/definition/what-is-electronic-support#:~:text=Electronic%20Support%20(ES)%20%E2%80%93%20also,or%20other%20electronic%20warfare%20systems.

9. Slt R. D. ELECTRONIC SUPPORT MEASURES [Електронний ресурс] / R. D. Slt, K. G. Slt – Режим доступу до ресурсу: https://www.scribd.com/presentation/79872115/ESM-final?language_settings_changed=English.

10. Electronic countermeasure military technology [Електронний ресурс] – Режим доступу до ресурсу: https://www.britannica.com/technology/electronic-countermeasure.

11. Electronic counter-countermeasure [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Electronic_counter-countermeasure.

12. Chi-Hao C. An Introduction to Electronic Warfare; from the First Jamming to Machine Learning Techniques. / C. Chi-Hao, T. James. – Oxon: CRC Press, 2021. – 188 с.

13. McArthur C. Operations Analysis in the United States Army Eighth Air Force in World War II, Vol. 4 / Charles W McArthur., 1990. – 349 с.

14. Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications [Електронний ресурс] / P. SHARMA, K. KUMAR SARMA, N. MASTORAKIS. – 2020. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9292960.

15. Woolf P. Моделювання шуму - білий, рожевий та коричневий шум, попси та тріски [Електронний ресурс] / Peter Woolf // University of Michigan. – 2022. – Режим доступу до ресурсу: http://surl.li/ulgrv.

15. Free-space path loss [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Free-space_path_loss.

16. MBX Model for Macro Cell [Електронний ресурс] – Режим доступу до ресурсу: https://www.ee.bilkent.edu.tr/~microwave/programs/wireless/prop/MBXMacro.htm.

17. Cost 231 Hata Model [Електронний ресурс] – Режим доступу до ресурсу: https://www.ee.bilkent.edu.tr/~microwave/programs/wireless/prop/CostHata.htm.

18. Chang K. RF and Microwave Wireless Systems / Kai Chang., 2000. – 331 с.

19. Telecommunications: Wireless [Електронний ресурс] // Standard & Poor's. – 2000. – Режим доступу до ресурсу: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a358102f1369c180707d6d4b9eaf7ad1115945a4.

20. Cellular Networks / J. Zhang, I. Stojmenovic // WL041/Bidgoli / J. Zhang, I. Stojmenovic., 2005. – С. 654–662.

21. Co-channel interference [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Co-channel_interference.

22. Co-Channel and Adjacent Channel Interference in Mobile Computing [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/co-channel-and-adjacent-channel-interference-in-mobile-computing/.

23. Intersymbol Interference [Електронний ресурс] – Режим доступу до ресурсу: https://www.siue.edu/~yadwang/ECE375_Lec9.pdf.

24. Варакин Л. Є. Системи зв'язку з шумоподібним сигналами. - М. «Радіо і зв'язок», 1985. - 384 с

25. CARRIER AGGREGATION – WHAT IT IS AND HOW IT WORKS [Електронний ресурс] – Режим доступу до ресурсу: https://www.quwireless.com/post/carrier-aggregation-what-it-is-and-how-it-works#:~:text=In%20simple%20words%20Carrier%20Aggregation,(5%20x%2020%20MHz).

26. Tadrous G. Understanding OFDMA, the interface for 4G wireless systems. [Електронний ресурс] / George Tadrous. – 2019. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/understanding-ofdma-interface-4g-wireless-systems-george-tadrous.

27. HARQ (Hybrid Automatic Repeat Request) in LTE [Електронний ресурс] // TechLTE World. – 2023. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/harq-hybrid-automatic-repeat-request-lte-techlte-world.