Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту)

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри)

Пояснювальна записка

до кваліфікаційної роботи

магістр
(ступінь вищої освіти)

на тему **Удосконалення роботи сенсорної мережі за допомогою каналів зв'язку з підвищеною завадостійкістю**

Виконав: студент 6 курсу, групи д6ТТ
спеціальності 172 «Телекомунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності)

Дюдюк І.М.
(прізвище та ініціали)

Керівник Фомін О.С
(прізвище та ініціали)

Рецензент Смоляр В.Г.
(прізвище та ініціали)

Полтава - 2025

2

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

ЗАТВЕРДЖУЮ

Завідувач кафедри
автоматики, електроніки та
телекомунікацій
_____ О.В. Шефер
"02" 09 2024 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Дюдюку Ігору Миколайовичу

1. Тема проекту (роботи) **Удосконалення роботи сенсорної мережі за допомогою каналів зв'язку з підвищеною завадостійкістю**
керівник проекту (роботи) Фомін Олександр Сергійович, к.т.н., доцент
затверджена наказом вищого навчального закладу від "09" 08 2024 року № 818-Ф,а

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

3. Вихідні дані до проекту (роботи) Технічна документація на телекомунікаційне обладнання сенсорних мереж.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Особливості безпроводових сенсорних мереж. Пропозиції для підвищення завадостійкості каналів зв'язку безпроводових сенсорних мереж. Аналіз методів модуляції сигналів у WSN. Вибір методів формування модуляційних символів OFDM. Експериментальне підтвердження працездатності методу спектрального детектування сигналу в умовах впливу вузькосмугової завади. Техніко-економічне обґрунтування прийнятих рішень.
Приклад реалізації розумного дому на основі Zigbee. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
1. Безпровідна сенсорна мережа.
2. Сенсори.
3. Типова структура мереж.

3

4. Спектр сигналу OFDM.
5. Завада міжсимвольної інтерференції.
6. Порівняння спектрів інформаційного сигналу, адитивного шуму, завади.
7. Висновок.

6. Дата видачі завдання 02.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін виконання етапів роботи			Примітка (плакати)
1	Аналіз літератури та джерел. Вступ.	07.10.24		15%	Пл. 1
2	Особливості безпроводових сенсорних мереж	16.10.24	I	30%	Пл. 2
3	Аналіз методів модуляції сигналів у WSN	05.11.24		40%	Пл. 4
4	Вибір методів формування модуляційних символів OFDM	12.11.24		50 %	Пл. 5
5	Експериментальне підтвердження працездатності методу спектрального детектування сигналу в умовах впливу вузькосмугової завади	19.11.24	II	60%	Пл. 6
6	Приклад реалізації розумного дому на основі Zigbee	26.1124		70%	Пл. 7,8
7	Висновки	11.12.24		90%	Пл. 9
8	Оформлення магістерської роботи	19.12.24	III	100%	Пл. 10

Магістрант _____ Дюдюк І.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Фомін О.С.
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АЦП - аналогово-цифровий перетворювач

БСМ (WSN) - бездротова сенсорна мережа

ДПФ - дискретне перетворення Фур’є

ЗШПФ - зворотнє швидке перетворення Фур’є

МНК - метод найменших квадратів

СКВ - середньо-квадратурне відхилення

ЦАП - цифро-аналоговий перетворювач

ШПФ - швидке перетворення Фур’є

BPSK - двійкова фазова маніпуляція

COFDM - ортогональне частотне розділення каналів з кодуванням

DSP - цифрова обробка сигналів

FSK - частотна маніпуляція

GFSK - частотна маніпуляція на основі фільтра Гауса

ISI - міжсимвольна інтерференція

LOS - лінія прямої видимості

MIMO - multiple input multiple output - множинний вхід, множинний вихід

MSK - маніпуляція з мінімальним частотним зсувом

NOFDM - неортогональний частотний розділ каналів

OFDM - ортогональний частотний розділ каналів

QAM - квадратурна амплітудна модуляція

QPSK - квадратурно-фазова модуляція

STC - просторове частотне кодування

ВСТУП

В наш час стає актуальною задача побудови універсальних мереж, які взмозі надавати послуги різних типів. До таких мереж відносять сенсорні мережі.

Відомо, що сенсорна мережа – це мережа невеликих за розміром обчислювальних пристроїв, оснащених сенсорними датчиками, трансиверами сигналу та мініатюрним джерелом живлення. Сенсори використовують у галузях для моніторингу екології, різних погодних параметрів, охорони та ін. В наш час удосконалення технологій та різних виробництв, зросла нагальна потреба в бездротових сенсорних мережах (WSN).

WSN (Wireless Sensor Networks) – це дуже перспективна технологія. В процесі розробки сенсорних мереж були виявлені недоліки каналів зв'язку WSN: нестабільність каналів, асиметричність каналів, залежність рівня прийнятого сигналу від температури, зміна рівня потужності сигналу на тривалих проміжках часу, непередбачуваність.

Ці явища впливають на роботу всієї мережі (втрата зв'язку, зниження зв'язності мережі, помилки в локалізації та ін.). Тому навіть використовуючи метод множинного доступу з виявленням несучої і уникнення колізій (CSMA/CA) як базовий режим доступу не гарантує усунення втрат значної кількості пакетів через колізії. Практика показала, що такі колізії відбуваються через особливості реалізації алгоритму CCA. При цьому губляться пакети тільки від вузлів з найбільш слабким рівнем сигналу. Вузли з більш сильним рівнем сигналу не мають таких колізій.

Працюючи в діапазоні 2,4 ГГц в залежності від трафіка, втрати пакетів можуть досягати до 90%, Це призводить до застосування спеціальних алгоритмів виявлення завад від мереж стандарту 802.11ax (Wi-Fi) і реалізації динамічного перемикання каналів у WSN.

Щоб захистити від завад WSN необхідно впроваджувати надширокосмугові системи зв'язку і технології передачі даних завадозахищені.

Актуальність теми дипломної роботи говорить про необхідність розробки

пропозицій щодо реалізації цифрової обробки багатопозиційних сигналів на основі N-OFDM (OFDM).

Остаточною **метою** є збільшення ефективності WSN за рахунок використання каналів зв'язку підвищеної завадостійкості. Щоб досягти цього необхідно вирішити наступні **задачі**.

1. Обґрунтування напрямів підвищення завадостійкості WSN.
2. Аналіз методів модуляції сигналів у WSN.
3. Використання багатопозиційних сигналів у WSN.
4. Технічне і економічне обґрунтування результатів.

Об'єкт дослідження – робота сенсорної мережі.

Предмет дослідження – цифрова обробка сигналів.

Метод дослідження – аналітика.

Практичне значення роботи це використати результати дослідження для удосконалення роботи сенсорних мереж.

Структура дипломної роботи складається з вступу, трьох розділів основної частини, висновків, списку використаних джерел, додатків, які містять лістинг програми обчислення функціонала методом найменших квадратів для методу спектрального детектування сигналу в умовах впливу вузькосмугової завади.

РОЗДІЛ 1.
ОСОБЛИВОСТІ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

1.1. Призначення сенсорних мереж

Новітні технології бездротового зв'язку та прогрес в області виробництва мікроелектроніки дозволили протягом останніх десятиліть перейти до практичної розробки та впровадженню нового класу розподілених комунікаційних систем – сенсорних мереж.

Бездротова сенсорна мережа (WSN) — це вид бездротової мережі , яка включає велику кількість самокерованих, мініатюрних малопотужних пристроїв, які називаються сенсорними вузлами або мотами (від англ. motes – порошинки) (Рисунок 1.1).

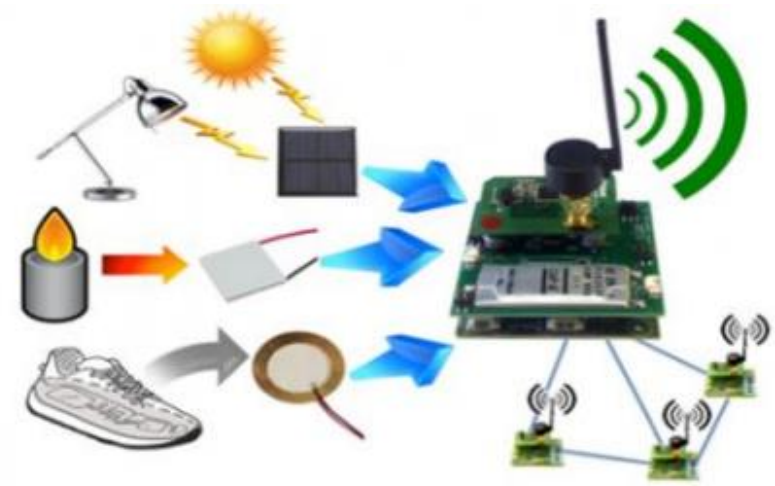


Рисунок 1.1 - Бездротова сенсорна мережа

Сенсорні мережі, звичайно, охоплюють величезну кількість просторово розподілених мініатюрних вбудованих пристроїв, що працюють від батареї живлення, які об’єднані в мережу для збору, обробки та передачі даних операторам, і вони контролюють можливості обчислення та обробки. Вузли — це мікронні комп’ютери, які спільно утворюють мережі. На дальність бездротового зв'язку впливає потужность рівня сигналу, а з збільшенням відстані між сенсорами зменшується пропускна спроможність.

Мот це маленька плата (Рисунок 1.2). На платі розміщуються: процесор, оперативна пам'ять, цифро-аналогові та аналого-цифрові перетворювачі (відповідно, ЦАП і АЦП), радіочастотний прийомо-передавач, джерело живлення та датчики. [19]

З досить великої кількості прикладів використання WSN виділимо два. Найбільш відомим є, мабуть, розгортання мережі на борту нафтового танкера компанії **British Petroleum** . За допомогою мережі, яка побудована на основі обладнання Intel, здійснювався моніторинг стану судна з метою організації його профілактичного обслуговування.

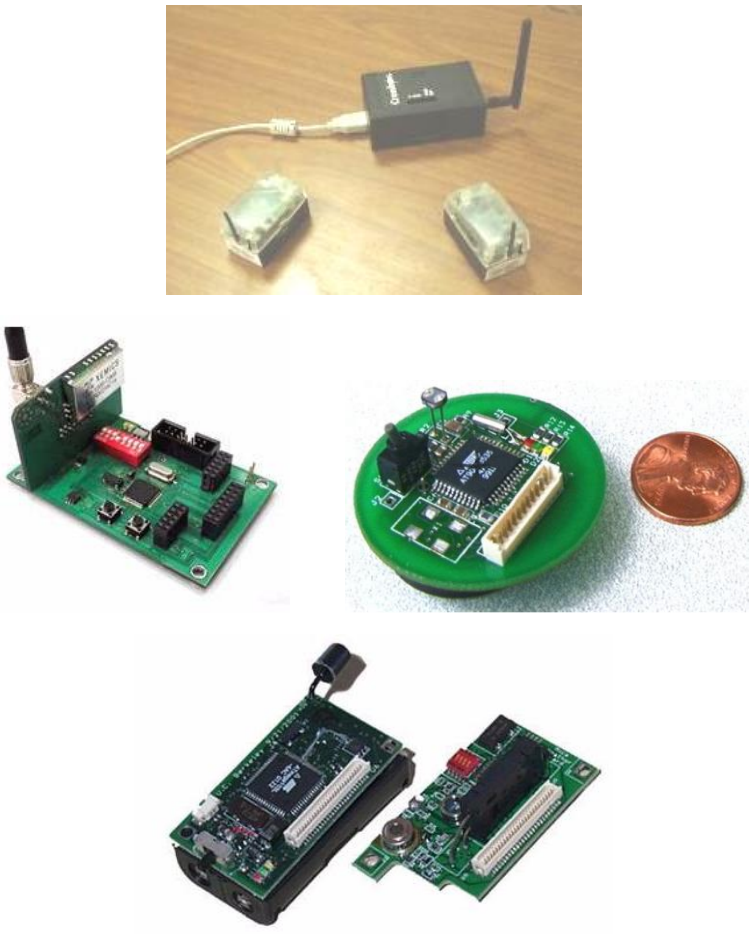


Рисунок 1.2 - Зовнішній вигляд мотів

Delta — національна військова система ситуаційної обізнаності, яку використовують Сили безпеки і оборони України; побудована за стандартами НАТО. Онлайн-система Delta в реальному часі показує оперативну ситуацію на полі бою за допомогою різних сенсорних пристроїв.

WSN застосовують у багатьох галузях. Однак, перед застосуванням сенсорної мережі треба перевірити її роботу практично , тому й потрібно проводити дослідження в цій області. [14]

На даний час, до основних переваг WSN слід віднести:

– повна відсутність кабелів;
– розміщення мотів в різних об’єктах простору;
– надійність елементів і системи;
– відсутність персоналу для розміщення та технічного обслуговування.

В цілому, можливо виділити наступні області застосування:

– моніторинг електропостачання;
– системи охорони та забезпечення безпеки;
– пожежна сигналізація;
– моніторинг за складськими приміщеннями;
– контроль персоналу.
– впровадження охоронних систем;
– спостереження за навколишнім середовищем;
– спостереження за противником на полі бою;
– спостереження за транспортуванням вантажів;
– моніторинг фізіологічного стану людини;

До складу кожного вузла мережі входять: мот, який оснащений радіотрансивером або іншим пристроєм бездротового зв'язку, невеликим мікроконтролером і джерелом енергії. Можливе використання батарей сонячного освітлення або інших альтернативних джерел енергії.

Дані від віддалених елементів передаються по мережі між найближчими вузлами по радіоканалу. У підсумку, з найближчого мота пакет з даними передається на шлюз. Шлюз з'єднаний, як правило, USB-кабелем із сервером. На сервері зібрані дані обробляються, зберігаються та можуть бути доступні через WEB-інтерфейс широкому колу користувачів.

Обладнання бездротового вузла забезпечується електроживленням для

тривалої експлуатації з автономними джерелами живлення. Вузол може працювати протягом кількох років в залежності від нагрузки роботи. Типова структурна схема мота з автономним живленням наведено на рисунку 1.3 зазвичай, використовуються датчики п’єзо-резистивні та тензорно-резистивні.

1.2. Архітектура та принцип роботи WSN

Вузли, розташовують по периметру спостереження. (Рисунок 1.4). Кожен вузол збирає і передає на центральний вузол або кінцевому користувачеві інформацію по найкоротшому маршруту.

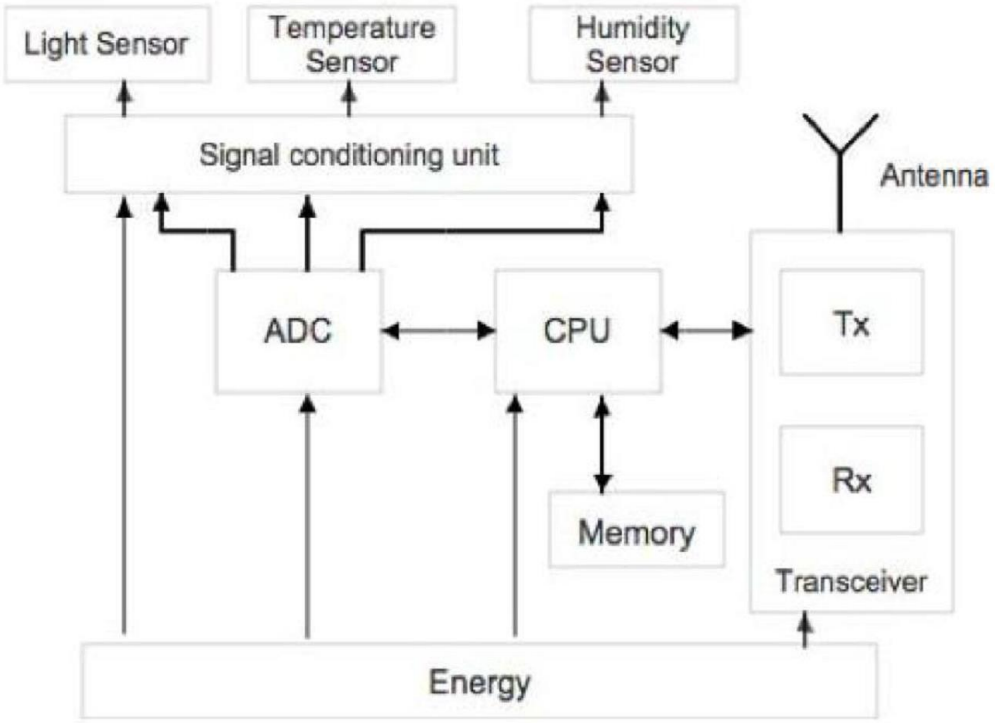


Рисунок 1.3 - Склад мота WSN

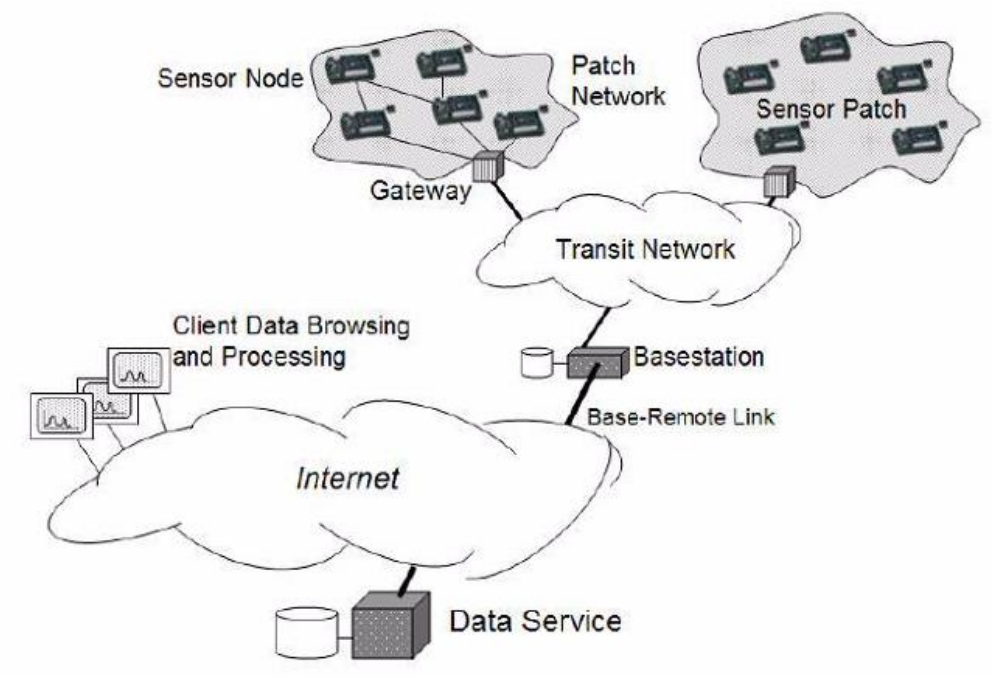


Рисунок 1.4 - Архітектура WSN

Стек протоколів містить інформацію про потужність і маршрути, дані про мережні протоколи та надає можливість спілкуватися через бездротове середовище. До стеку протоколів входить: фізичний рівень, канальний рівень, мережевий рівень, транспортний рівень, рівень додатків, також входять площини керування живленням, площина керування мобільністю таплощина плануванням завдань (Рисунок 1.5). [21]

Різні види прикладного ПЗ побудовані на рівні додатків.

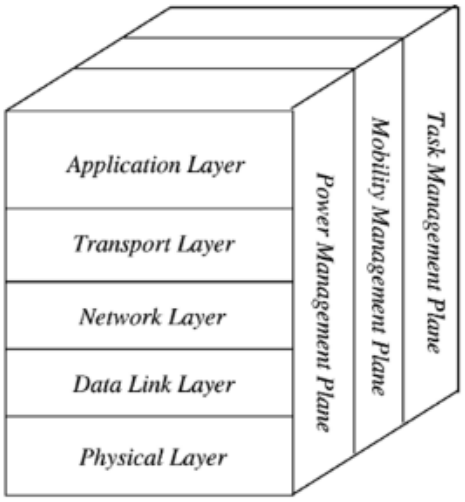


Рисунок 1.5 - Стек протоколів

Фізичний рівень передає фізичні сигнали від джерела до отримувача.

На мережному рівні створюється маршрутизація трафіку котрий забезпечується на транспортному рівні.

Транспортний рівень забезпечує передачу даних мережею.

Три перехресні шари включають наступне:

1. Площина керування живленням.
2. Площина управління мобільністю.
3. Площина управління завданнями.

Площина керування живленням показує як вузол використовує енергію. Приклад, вузол відключить приймач, щоб не дублювати повідомлення від нших вузлів. Вузол з низьким рівнем батареї, буде використовувати енергію для збору даних і передасть сусіднім вузлам, що не зможе передавати повідомлення.

Площина керування мобільністю виявляє та реєструє зміну місця розташування вузлів. Тому знаючи розташування сусідніх вузлів вузол розподілить енергію відповідно.

Площина управління завданнями розподіляє та встановлює розклади оброблення данних для окремого сектору.

Ці площини використовуються для спільної роботи вузлів і ефективного використання їхньої енергії.

Узагальнюючі відомості про WSN, за моделлю OSI можливо виділити наступні використовувані протоколи.

1. Рівень додатків – Modbus TCP, IEC 60870-5, MQTT.

2. Мережевий рівень (NWK) –Directed Diffusion, Rumour, LEACH, TEEN, APTEEN, SPEED, 6LoWPAN.

3. Канальний рівень (MAC) – S-MAC, T-MAC, SS-TDMA, ZigBeeMAC та ін.

4. Фізичний рівень (PHY) – ISM діапазон (433, 868 МГц – Європа, 902÷928 МГц – Америка, 2,4÷2,4835 ГГц – в усьому світі).

Таким чином, до основних завдань WSN слід віднести:

– періодичне вимір показника;

– детектування події;

– вимірювання показника за запитом.

1.3. Аналіз номенклатури WSN

Найбільш поширені варіанти схемо-технічних рішень WSN:

DASH7 – технологія WSN, що використовує неліцензований діапазон частот і є відкритою.

Insteon – бездротова та проводова сенсорна мережа. Використовується електропроводка об’єктів для передачі інформації по проводам. Діапазон робочих частот 902 - 924 МГц. Дальність зв’язку до 45 м при прямій видимості. Середня швидкість 180 біт/с.

ISA100.11a – використовується в промислових сенсорних мережах. Має низьке енергоспоживання. Робоча частота 2,4 ГГц. Має низьку швидкість передачі даних.

Enocean – використовується для автоматизації приміщень. Робоча частота 868 МГц. Швидкість передачі даних 120 кбіт/с. Дальність зв’язку до 300м при прямій видимості.

Miwi – використовують низьку швидкість передачі на малі відстані. Робоча частота 2,4 ГГц. Швидкість передачі даних до 250 кбіт/с. Технологія Miwi має максимум до 1024 вузлів.

6Lowpan – використовується для автоматизації приміщень. Робочий діапазон частот 2,4ГГц. Дальність зв’язку до 200м при прямій видимості. Швидкість передачі даних до 200 кбіт/с. Має до 100 вузлів.

One-Net – використовують для автоматизації приміщень. Робочий діапазон частот має не ліцензований. Дальність зв’язку до 100 м в приміщенні і до 500 м при прямій видимості. Швидкість передачі даних до 230 кбіт/с. Має до 4096 вузлів.

Rubee – використовується в об'єктах підвищеної небезпеки. Робоча частота 131 кГц і використовуються магнітні хвилі. Швидкість передачі даних до 1200 біт/с. Дальність зв’язку до 30 м.

Wavenis – використовується для персональних мереж і мереж датчиків. робочі частоти 433; 868; 915 МГц. Дальність зв'язку до 200 м у приміщенні та до 1км при прямій видимості. Швидкість передачі даних до 100 кбіт/с.

WirelessHART – використовують в промисловості на базі протоколу HART. Робоча частота 2,4 ГГц. Дальність зв'язку до 200м при прямій видимості . Швидкість передачі даних до 250 кбіт/с.

Z-Wave – використовується в основному для домашньої автоматизації (розумний будинок). Робоча частота 908,42 МГц в США та 868,42 МГц в Європі. Дальність зв'язку до 40 м при прямій видимості. Швидкість передачі даних 100 кбіт/с. Передбачена ретрансляція.

Надалі, доцільно більш детально розглянути Zigbee, як найбільш поширену технологію WSN.

1.4. WSN на основі Zigbee

Zigbee –використовує невеликі, трансивери з малою потужністю, для бездротових персональних мереж.

Особливістю технології ZigBee є слідуюче при низькому енергоспоживанні підтримує топології мережі: точка-точка, дерево, зірка, а й самоорганізуючу і самовідновлювану коміркову (mesh) топологію з маршрутизацією повідомлень і ретрансляцією.

Альянс Zigbee дозволяє сумісні продукти створювати виробникам. Список профілів додатків:

- розумний дім;
- додатки телекомунікації;
- корисне енергоспоживання;
- домашній і медичний нагляд;
- іграшки;
- комерційне будівництво автоматизоване.

Співробітництво між IEEE 802.15.4 і Zigbee подібно тому, що існує між IEEE 802.11 і Wi-Fi. Специфікація Zigbee 1.0 була юридично затверджена 14 грудня 2004р. і була доступна для вхожих до альянсу Zigbee. Специфікація Zigbee була розміщена 30 жовтня 2007р.

Zigbee має робочі частоти: 915 МГц в США та в Австралії, 868 МГц в Європі, а також 2,4 ГГц в інших країнах. Як правило, у продажі є чипи Zigbee, що є об'єднаними радіо- і мікроконтролерами. Радіомодуль використовується роздільно з будь-яким мікроконтролером чі процесором.

Zigbee активується переходячи зі сплячого до активного режиму за 15 мс, а затримка відгуку пристрою може бути дуже низькою. Перебуваючи в сплячому режимі Zigbee більшість часу, тому рівень енергоспоживання дуже низьке.

Реалізація Zigbee 2007 на цей час є поточною, вона містить 2 профілі стека:

– профіль стека №1 - просто Zigbee для домашнього та дрібного комерційного використання Zigbee - займає менше місця в пам'яті.

– профіль стека №2 - Zigbee Pro.

Zigbee Pro має більше функцій: маршрутизацію виду «точка-багатоточка», високу безпеку з використанням симетричного ключа (SKKE) і широкомовлення. Ці два профілі дозволяють розгорнути повномасштабну мережу з комірковою топологією та працюють з всіма профілями додатків Zigbee.

Протоколи Zigbee розроблені для використання у вбудованих додатках, що вимагають низьку швидкість передачі даних і низьке енергоспоживання.

Zigbee мають за мету – створення недорогих мереж, що самоорганізовуються, з комірчастою топологією для широкого кола задач. Мережа може використовуватися в домашній та будівельній автоматизації, вбудованих датчиках, промисловому контролі, оповіщенні про задимлення та іншому. Створена мережа споживає дуже мало енергії – індивідуальні пристрої працюють з батареями до 2 років. Типовими прикладами впровадження Zigbee є:

– домашнє оповіщення – датчики доступу й переговорів, датчики води й електрики, датчики задимлення й пожежі, моніторинг енергії;

– домашні контроль й розваги – фільми, музика, безпека й охорона, температурний контроль, раціональне висвітлення;

– мобільні служби – мобільні оплата, моніторинг і контроль, охорона й контроль доступу, охорона здоров'я й теледопомога;

– комерційне будівництво – моніторинг енергії, HVAC (опалення, вентиляція, кондеціонування), світла, контроль доступу;

– промислове встаткування – керування енергією й майном, контроль процесів, промислових пристроїв.

Протоколи побудовані на алгоритмі AODV (протокол динамічної маршрутизації для мобільних ad-hoc мереж (MANET) і інших бездротових мереж) і Neurfon, що призначені для створення мереж ad-hoc (децентралізована бездротова мережа, що утворена випадковими абонентами) або вузлів. У більшості випадків, мережа є скупченням скупчень. Вона також може ухвалювати форму мережі або одиночного скупчення. Поточні профілі виходять із протоколів Zigbee і підтримують мережі з включеними або з відключеними маячками.

У мережах з відключеними маячками (де порядок маячків становить 15) використовується механізм доступу до каналів. У цій мережі маршрутизатори Zigbee підтримують свої приймачі включеними довго, що потребує більшої енергії. Бездротовий ламповий вимикач є прикладом різнорідної мережі. У лампі вузол Zigbee приймає постійно, коли підключений до живлення, а ключ, що з'єднує лампу з батареєю в сплячому режимі, в той час як вимикач відключений. Потім ключ активується, посилає лампі команду, очікуючи підтвердження, і повертається в сплячий режим. Вузол лампи у мережі повинен бути, маршрутизатором Zigbee, або координатором, вузол ключа, звичайно, цей кінцевий пристрій.

У мережах з маячками, маршрутизатори Zigbee, передають періодичні маячки, чим підтверджують свою присутність на вузлах мережі.

Протоколи Zigbee скорочують енергоспоживання та знижують час включення радіопередавачів. У маячкових мережах вузли повинні бути активними тільки під час здійснення маячком передачі. Витрата енергії більш нерівномірна у

безмаячкових мережах, завжди активні окремі пристрої, одночасно інші знаходяться сплячому режимі.

Специфікація Zigbee RF4CE. 3 березня 2009 р. концерн RF4CE Zigbee RF4CE розроблено для дистанційно керованої аудіо- відеопродукції, такій як телевізори та телеприставки.

ПЗ розроблене з метою побудови недорогих мікропроцесорів. Радіорозробки, що використані в Zigbee оптимізовані, щоб досягти низької ціни серед продукції. Є кілька аналогових каскадів, де можливо використовуються цифрові контури.

Хоча радіопередавачі самі по собі недорогі, процес кваліфікації Zigbee містить у собі повну перевірку вимог на фізичному рівні. Проблеми, що проявляються в перекрученій зменшеній реакції Zigbee, радіосхеми мають тверді інженерні обмеження, що відносяться до енергоживлення та ширини діапазону. Існують рішення, що поєднують мікроконтролер і радіопередавач в одному корпусі, наприклад, мікроконтролери серії STM32W від компанії Stmicroelectronics.

1.5. Аналіз особливостей функціонування WSN

Навіть використання CSMA/CA в якості базового режиму доступу не гарантує усунення втрат значної кількості пакетів через колізії. Експерименти показали, що такі колізії відбуваються через особливості реалізації алгоритму CCA. Через особливості інформаційного трафіку в сенсорних мережах часто відбувається конкурентна передача. Існує загальна думка, що колізії в сенсорних мережах побудованих із застосуванням алгоритму CSMA/CA можуть відбуватися тільки в разі «прихованого терміналу». Однак, експерименти з вузлами сенсорної мережі стандарту 802.15.4 показали, що значна кількість колізій відбувається навіть коли немає прихованого терміналу.

Як наслідок, при такому типі колізій губляться пакети тільки від вузлів з більш слабким сигналом. Вузли з більш сильним сигналом стійкіші до таких колізій. В цілому, що зниження кордону чутливості (CCA Threshold) ближче до рівня шуму дозволяє значно зменшити кількість колізій.

Втрати пакетів до 90% можуть бути на частоті 2,4 ГГц. Це спонукає до застосування спеціальних алгоритмів для виявлення завад від мереж стандарту 802.11x (Wi-Fi) і реалізації динамічного перемикання каналів у WSN (Рисунок 1.6).

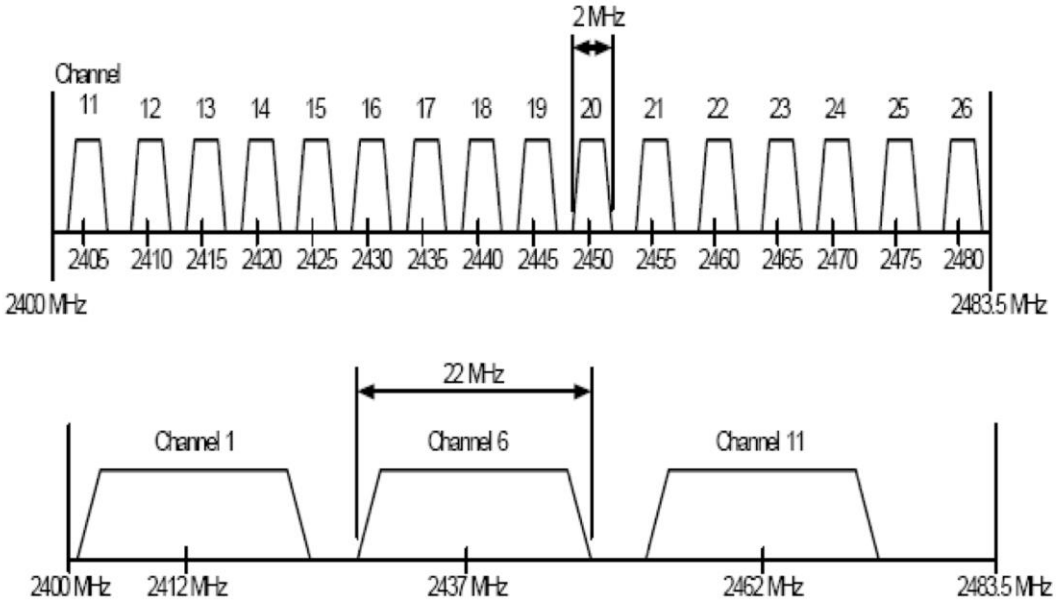


Рисунок 1.6 - Спільна робота мереж Wi-Fi і WSN в діапазоні 2,4 ГГц

Вході досліджень встановлено, що канали зв'язку WSN мають ефекти та явища:

– несиметричність каналів;

– нестабільність каналів;

– зміна потужності сигналу на проміжках часу;

– залежність RSSI від температури (Received Signal Strength Indicator, RSSI) зміни порядку 2 дБ на кожні 10град., а також при підвищенні температури знижується і рівень вихідної потужністі передавача і чутливість приймача;

– непередбачуваність.

Вони мають сильний вплив на роботу всієї мережі в цілому (втрата зв'язку, зниження зв'язності мережі, помилки в локалізації та ін.). Наявність підсилювача потужності (Power Amplifier, PA) і малошумлячого підсилювача (Low Noise Amplifier, LNA) вимагає термокомпенсації.

В свою чергу, зазначені ефекти впливають на протоколи верхніх рівнів.

Так, швидкість прийому пакетів (Packet Reception Rate, PRR) залежить не тільки від відстані і навколишніх умов, але і від використовуваної схеми корекції помилок. Невеликі пакети менш схильні до помилок (менше бітів в пакеті – менше ймовірність помилки пакета). Вузли використовують короткі пакети, не можуть точно визначити PRR при використанні більш довгих пакетів. Як наслідок, використання коротких пакетів, для збільшення дальності передачі. Наприклад, контрольні пакети короткі і мають велику ймовірність правильного прийому.

Для забезпечення належного рівня захисту WSN, необхідна розробка алгоритмів шифрування, орієнтованих на використання в вузлах з обмеженими обчислювальними можливостями, реалізації змінної довжини блоку, в т. ч. з урахуванням енергоспоживання вузла. Крім того, потрібна розробка алгоритмів автентифікації вузлів мережі з урахуванням їх обмежених обчислювальних можливостей та автентифікації трафіку (забезпечення цілісності даних).

Таким чином, можливо сформувати наступні вимоги до WSN.

1. Стійкість до активних радіозавад.

2. Виявлення підміни вузлів.

3. Наявність резервних маршрутів передачі даних.

4. Виявлення та запобігання спробам реконфігурації мережі, підміни адресної інформації, несанкціонованої «перепрошивки» пристроїв,

5. Стійкість до викривлення та фільтрації кадрів.

Подальші дослідження доцільно спрямувати на підвищення завадостійкості каналів зв’язку WSN.

1.6. Загальна постановка задачі

Аналіз шляхів щодо збільшення ефективності роботи WSN за рахунок використання каналів зв’язку підвищеної завадостійкості, установив задачу досліджень, а саме було запропоновано реалізацію цифрової обробки багатопозиційних сигналів на основі N-OFDM (OFDM).

Як наслідок, в роботі необхідно вирішити наступні задачі досліджень:

1. Обґрунтування напрямів підвищення завадостійкості WSN.
2. Аналіз методів модуляції сигналів у WSN.
3. Розробка пропозицій щодо використання багатопозиційних сигналів у WSN.
4. Технічні і економічні обґрунтування прийнятих рішень.

Висновок

Актуальність досліджень WSN очевидна. Їх використовують в багатьох галузях: це моніторинг ситуативної обстановки військ, погоди, екології, та ін. З удосконалюванням технологій та різних виробництв, потреба використання БСМ зростатиме. Основними завданнями WSN є: періодичний вимір показника; детектування події; вимірювання показника за запитом.

До найбільш поширених варіантів схемо-технічних рішень WSN слід віднести: DASH7, Z-Wave, Insteon, Enocean, ISA100.11a, Wirelesshart, Miwi, 6Lowpan, One-Net, Wavenis, Rubee, Zigbee (Pro).

Основна особливість ZigBee полягає в тому, що при низькому енергоспоживанні підтримує прості топології мережі і mesh-топологію з маршрутизацією повідомлень і ретрансляцією. Також, специфікація ZigBee дає вибір алгоритму маршрутизації, кінцеві точки, прив'язки, гнучкий механізм безпеки і забезпечує простоту обслуговування, розгортання та модернізації.

На жаль, використання CSMA/CA в якості базового режиму доступу не гарантує усунення втрат значної кількості пакетів через колізії. Експерименти з вузлами сенсорної мережі стандарту 802.15.4 показали, що значна кількість колізій відбувається навіть коли немає прихованого терміналу при такому типі колізій губляться пакети тільки від вузлів з більш слабким рівнем сигналу. Вузли з більш сильним сигналом стійкіші до таких колізій.

Втрати пакетів до 90% можуть бути на частоті 2,4 ГГц. Це призводить до застосування спеціальних алгоритмів для виявлення завад від мереж стандарту 802.11ax (Wi-Fi) і реалізації динамічного перемикання каналів у WSN.

Вході досліджень встановлено, що для каналів зв'язку WSN властиві наступні ефекти та явища: несиметричність каналів; нестабільність каналів; зміна потужності сигналу на проміжках часу; залежність RSSI від температури; непередбачуваність.

Вони мають сильний вплив на роботу всієї мережі в цілому (втрата зв'язку, зниження зв'язності мережі, помилки в локалізації та ін.), а саме головне – впливають на протоколи верхніх рівнів.

Таким чином, можливо сформувати наступні вимоги до WSN.

1. Стійкість до активних радіозавад.

2. Виявлення підміни вузлів.

3. Наявність резервних маршрутів передачі даних.

4. Виявлення та запобігання спробам реконфігурації мережі, підміни адресної інформації, несанкціонованої «перепрошивки» пристроїв,

5. Стійкість до викривлення та фільтрації кадрів.

Подальші дослідження доцільно спрямувати на підвищення завадостійкості каналів зв’язку WSN.

РОЗДІЛ 2.
ПРОПОЗИЦІЇ ДЛЯ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ КАНАЛІВ ЗВ'ЯЗКУ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

2.1. Обґрунтування напрямів підвищення завадостійкості БСМ

Проходячи по каналу зв'язку сигнал піддається спотворенням (Рисунок 2.1).

Всі завади умовно можна розділити на дві групи: адитивні і мультиплікативні

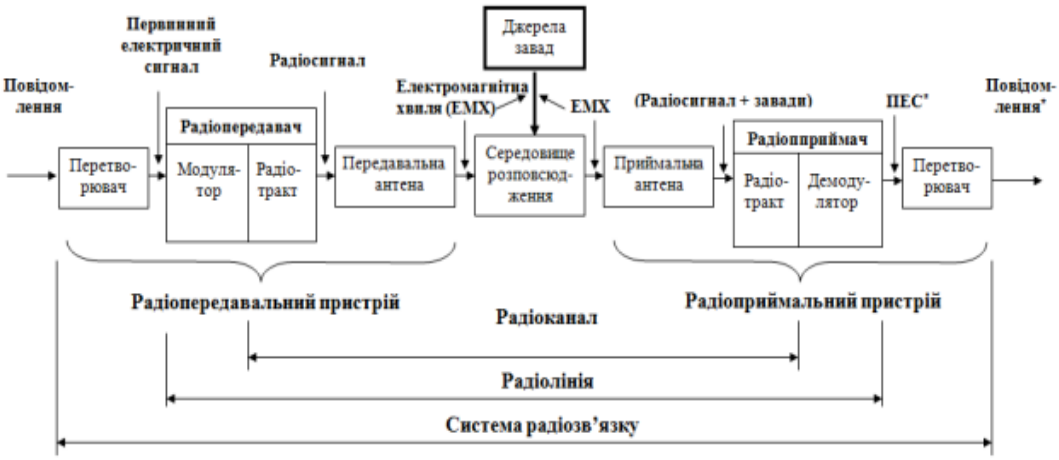


Рисунок 2.1 - Система радіозв'язку

1. Адитивні завади мають характер підсумовування. Фізичні явища, які зумовлюють заважаючий вплив, здатні спотворити сигнал. Атмосферні джерела завад: гроза, спалахи та збурення на сонці. В різних каналах зв'язку є завади, які є шумами, що породжуються електричними збуреннями в апаратурі.

Адитивні завади - це широкосмугові по спектру частот, безперервні, гладкі; створювані супротивником РЕБ.

2. Мультиплікативні завади є нелінійними ефектами та викликають нелінійні спотворення сигналу. Вони виникають в атмосфері з радіохвилями. Виникнення мультиплікативних завад, зумовлене змінами неоднорідностей в атмосфері,

які призводять до зміни параметрів амплітуди і фази радіосигналів, багатопроменевості. [12]

Завадостійкість системи зв'язку це здатність системи зв'язку нормально функціонувати під дією радіозавад. Вона забезпечується проведенням організаційних і технічних заходів.

Щоб досягти потрібної швидкості передачі у БСМ треба прикласти параметри потужності сигналу P_c і смуги пропускання каналу $F_к$. Щоб характеризувати ці параметри введено поняття енергетичної ($\beta = R_{кан}/(P_c / N_0)$) та частотної ефективності ($\gamma = R_{кан} / F_к$). Маємо відношення P_c / N_0 потужності сигналу до спектральної густини потужності шуму на вході демодулятора. Таким чином, критерії ефективності є слідуючі:

– інформаційна ефективність системи, що визначає ступінь використання пропускної здатності каналу

$$\eta = \frac{R_{кан}}{C_к}; \tag{2.1}$$

– енергетична ефективність

$$\beta = \frac{R_{кан}}{P_s / N_0}; \tag{2.2}$$

– частотна ефективність

$$\gamma = \frac{R_{кан}}{F_к}. \tag{2.3}$$

Показники β і γ мають сенс питомих швидкостей, а зворотні величини $\beta' = \beta^{-1}$ і $\gamma' = \gamma^{-1}$ визначають питомі витрати відповідних ресурсів на передачу інформації з одиничною швидкістю (1 біт/с).

Для гаусового каналу зі смугою пропускання $F_к$, відношенням потужностей сигналу та шуму $p = P_c / P_ш$ і пропускною здатністю $C_к = F_к \log(p+1)$ можна встановити, що ці показники ефективності пов'язані співвідношенням:

$$\eta = \frac{\gamma}{\log(1+\gamma/\beta)} \text{ і } \gamma = p\beta. \tag{2.4}$$

$$\beta = \frac{\gamma}{2^{\gamma} - 1}. \tag{2.5}$$

Формула (2.5) визначає залежність енергетичної від частотної ефективності в ідеальних умовах, що забезпечує рівність швидкості передачі інформації та пропускної здатності каналу.

Слід підкреслити, що частотна ефективність γ змінюється в межах від 0 до ∞, але енергетична ефективність обмежена величиною:

$$\beta_{\max} = \lim_{\gamma \to 0} \beta = \lim_{\gamma \to 0} \left(\frac{\gamma}{2^{\gamma} - 1}\right) = \frac{1}{\ln 2} \approx 1{,}443. \tag{2.6}$$

Енергетична ефективність системи передачі інформації гаусовим каналом не може перевищувати величини:

$$\beta_{\max} = 1{,}443. \tag{2.7}$$

Інформаційна ефективність менше граничної ефективності $\eta_{\max}$, тому в WSN імовірність помилки p завжди має кінцеве значення. В таких випадках для фіксованої ймовірності помилки $p = const$ можна визначити коефіцієнти ефективності β, γ і побудувати криві $\beta = f(\gamma)$. У координатах (β, γ) кожному варіанту WSN буде відповідати точка на площині.

Все це свідчить про прямий взаємозв'язок завадостійкості з енергетичною та частотною ефективністю WSN. Їх одночасне підвищення впливає на надійність WSN в цілому, як системи.

В якості пріоритетних шляхів оптимізації WSN на рівні системи передачі даних слід вказати про використання завадостійкого кодування, сигнально-кодових конструкцій, багатопозиційних сигналів або їх комбінацій. Такий підхід достатньо обґрунтований в існуючій множині публікацій.

В свою чергу, заслуговують уваги напрямки, що спираються на впровадження інноваційних технологій, які отримали значне поширення в більш розвинутих мережах, наприклад: 802.11ac(ax), 5G, MU-MIMO, Massive MIMO та ін.

2.2. Аналіз методів модуляції сигналів у БСМ

В існуючих WSN, до яких слід віднести ZigBee і Thread, застосовуються прийомо-передатчики (Рисунок 2.2) з частотною маніпуляцією сигналів FSK (Frequency Shift Key) зі згладжуванням позитивних і негативних частотних цифрових сигналів на основі фільтра Гауса GFSK (Gaussian Frequency Shift Keying). Також, існують прийомо-передатчики з зсунутою квадратурною фазовою маніпуляцією OQPSK (Offset Quadrature Phase Shift Keying,) або двійковою фазовою маніпуляцією BPSK, забезпечуючи роботу інтерфейсних модулів зі швидкістю 2 Мбіт/с.

Швидкість 250 кбіт/с це максимальна пропускна здатність мережі для різних WSN, а корисна швидкість в межах сусідніх вузлів буде приблизно до 40 кбіт/с, а при застосуванні ретрансляції десь від 5 до 25 кбіт/с.

Узагальнена схема модулятора FSK наведена на рисунку 2.3. Прямокутний бітовий потік перетворений до рівнів +(-)1 надходить на модулятор (генератор керований напругою), де рівню +1 відповідає одна частота, рівню -1 – інша. У такий спосіб на виході модулятора одержуємо FSK.

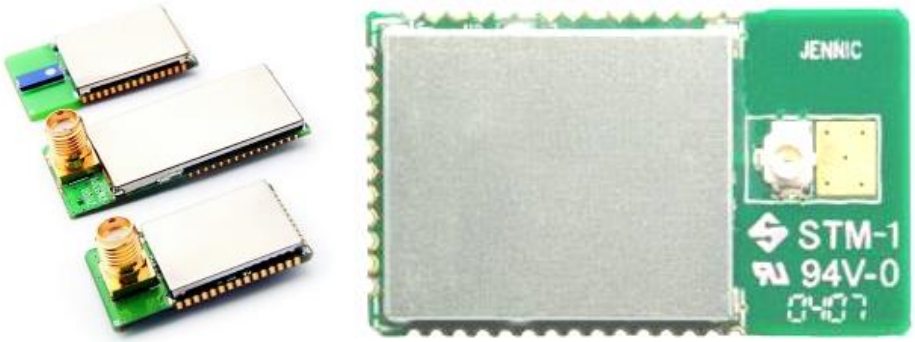


Рисунок 2.2 - Трансивери JN5148-001-M00/xx ZigBee PRO (к. NXP Semiconductors)

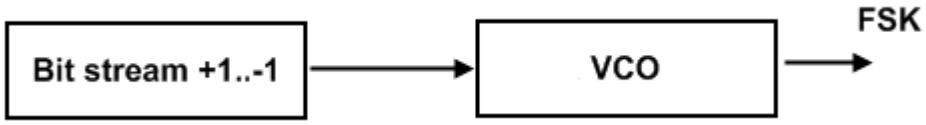


Рисунок 2.3 - Узагальнена схема модулятора FSK

Як видно, рознесення частот задається в модуляторі та може бути будь-яким, але не менше ніж швидкість маніпуляції (Baud Rate, Br). При меншому рознесенні коректна демодуляція такого сигналу неможлива. Слід відзначити, що генератор у модуляторі та бітовий потік, у цілому, ні як не пов’язані та не синхронізовані. Спектр такого сигналу містить множину гармонік через прямокутність імпульсів модуляції та різкого перемикання генератора в модуляторі в «невідповідні» моменти часу. Основна енергія зосереджена навколо частот маніпуляції та займає смугу рівну Br, що дає мінімально можливий спектр такого сигналу 2*Br при рознесенні рівному Br, або сумі Shift (рознесення частот маніпуляції) і Br, у більш загальному випадку. Гармоніки за межами даного спектра можуть бути ефективно подавлені без шкоди для успішної демодуляції, що й робиться на практиці (Рисунок 2.4). [14]

Слід звернути увагу, що спектр навколо частот маніпуляції при рознесенні рівному Br точно укладається в простір між частотами без перекриття. Якщо частоти зближати далі, то буде перекриття спектрів «чужих» посилок і взаємні сильні завади. Це наочне графічне зображення обмеження мінімального розносу при класичній FSK.

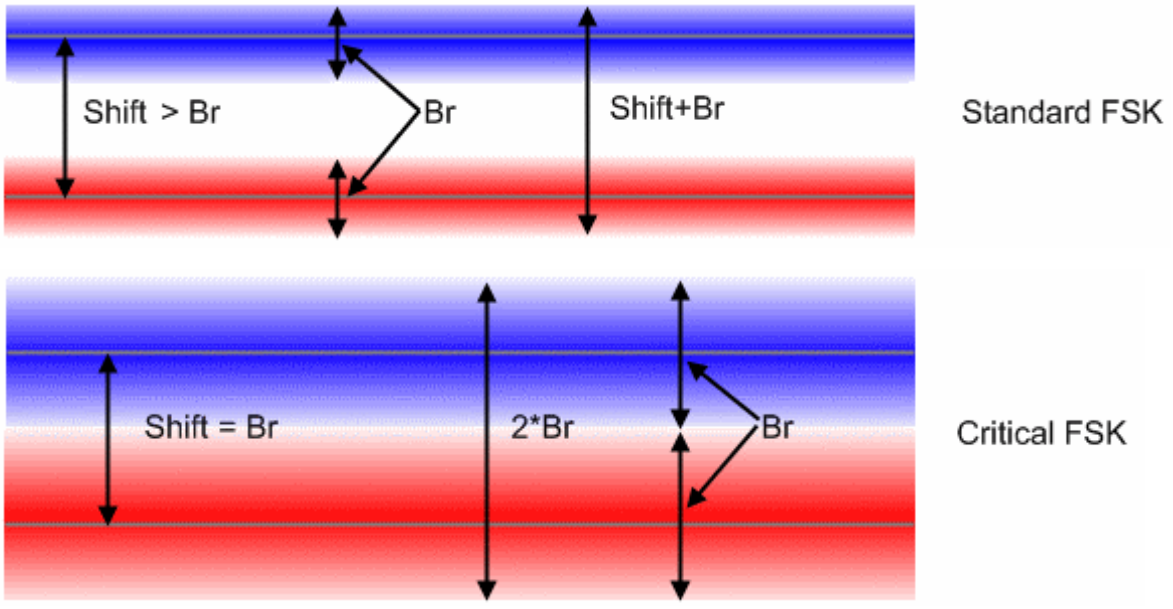


Рисунок 2.4 - Рознесення частот при FSK

Для зменшення розносу частот при тій же швидкості маніпуляції, треба

зменшити (звузити) область основної енергії бічних навколо частот маніпуляції, що дасть змогу зменшити рознесення. Ця ідея реалізується через попередню фільтрацію бітового потоку перед подачею на модулятор. Для FSK широке поширення одержали фільтри Гауса (GFSK), вони забезпечують досить ефективне звуження смуги за рахунок згладжування різких переходів напруги маніпуляції та гарну керованість параметрами. У принципі будь-який фільтр, що згладжує різкі переходи придатний для цієї мети. Однак, фільтри Гауса мають більш кращі характеристики, хоча вони не єдині звичайно. Загальна схема модулятора GFSK (Рисунок 2.5).

Це дозволяє відійти від обмеження мінімального зсуву FSK убік зменшення: Shift ≥ Br (Рисунок 2.6).

Від параметрів фільтра Гауса залежить наскільки сильно буде звужений основний спектр бічних і наскільки сильно можна зсунути частоти маніпуляції.

Рисунок 2.5 - Модулятор GFSK

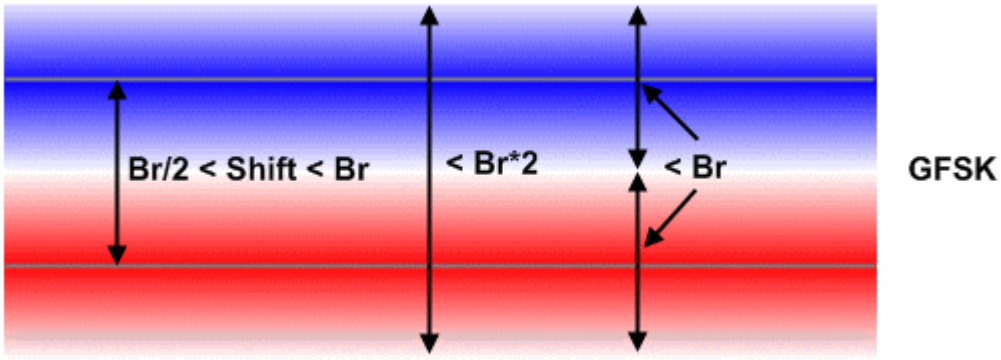


Рисунок 2.6 - Рознесення частот при GFSK

На практиці ця величина завжди більше чим Br/2. Це обумовлене тим, що зменшення бічних досягається сильною пологістю фронтів напруги маніпуляції, що призводить до накладання одного імпульсу на інший, і, як наслідок до неможливості демодуляції. Типове зменшення рознесення для GFSK становить на 30÷40 % від класичного Shift = Br, тобто Shift = (0,7÷0,6)*Br. В загальному випадку, досить складно при аналізі сказати, що використовується саме GFSK, тому що

такого ж або практично такого ж ефекту можна досягти й з іншими фільтрами.

2.3. Мультиплексування з ортогональним частотним розділенням каналів

Основна ідея мультиплексування з ортогональним частотним розділенням каналів OFDM (Orthogonal Frequency Division Multiplexing) в тому, що смуга пропускання каналу ділиться на вузькі смуги або субканали, які мають свою піднесучу. На всіх цих піднесучих сигнал передається одночасно, що забезпечує практично, як завгодно, велику загальну швидкість передачі інформації при невеликій швидкості передачі в кожному окремому субканалі. По суті, ортогональне частотне розділення каналів перетворює широкосмуговий частотно-вибірковий канал в кілька паралельних субканали. Це запобігає багатопроменевості міжсимвольної інтерференції.

Сигнал з ортогональним частотним розділенням каналів складається з ортогональних піднесучих *(N)*, модульовані з *N*-ю кількістю паралельних потоків даних. Кожен із субканалів відокремлений один від одного, що забезпечується взаємною ортогональністю піднесучих, що відповідає формулі (Рисунок 2.7):

$$\int_0^{T_S} (\sin 2\pi f_n t \cdot \sin 2\pi f_k t) dt = 0 \text{ , при } n \neq k \qquad (2.8)$$

де T_S – тривалість OFDM-символу, f_n і f_k – відповідно, несучі частоти n-го і k-го субканалів.

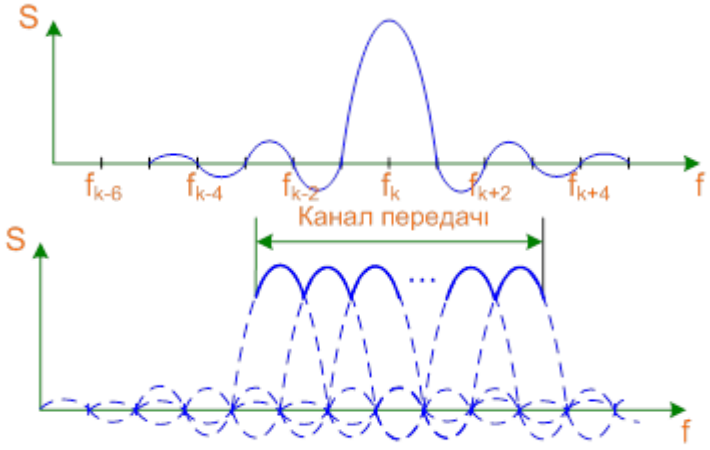


Рисунок 2.7 - Спектр сигналу OFDM з 6-ма ортогональними піднесучими

Спектр сигналу на k-ій піднесучій (в k-му субканалі) описується функцією вигляду:

$$\frac{\sin 2\pi(f - f_k)}{2\pi(f - f_k)}.$$

Формування субканалів з ортогональними піднесучими здійснюється за допомогою процедури ЗДПФ (зворотного дискретного перетворення Фур'є) потоку символів даних в передавачі. Зворотнє дискретне перетворення Фур'є вибирається так, щоб не відбувалося завмирання в субканалах.

Таким чином, функції OFDM-модулятора зводяться до створення сигналу, що містить N піднесучих, велика частина з яких модульовані інформаційними символами на проміжку T_s:

$$S(t) = \frac{1}{N}\sum_{k=0}^{N-1} a_k \times \cos(2\pi f_k t + \varphi_k) = \frac{1}{N}\sum_{k=0}^{N-1} \mathrm{Re}(a_k \times e^{j2\pi f_k t}), \qquad (2.9)$$

де $a_k = a_k \times e^{j\varphi_k}$ – комплексний модулюючий символ, T_s – тривалість символу, a_k – амплітуда символу, φ_k – фаза символу, $k = 1, 2...., (N-1)$.

В процесі передачі сигналу OFDM в радіоканалі із завмираннями виникають міжканальна інтерференція та міжсимвольна інтерференція.

Щоб запобігти взаємним завадам до корисного сигналу додається «активний» захисний інтервал. (Рисунок 2.8).

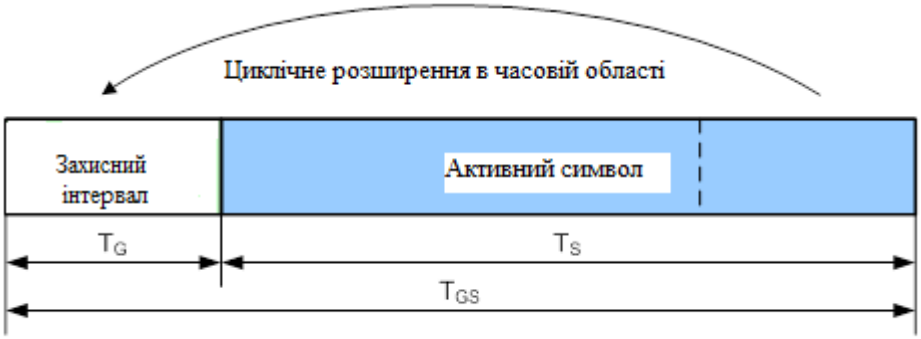


Рисунок 2.8 - Формування повного символу OFDM

Правильний вибір тривалості захисного інтервалу дозволяє в певних межах усунути завади, що викликані ехо-сигналами.

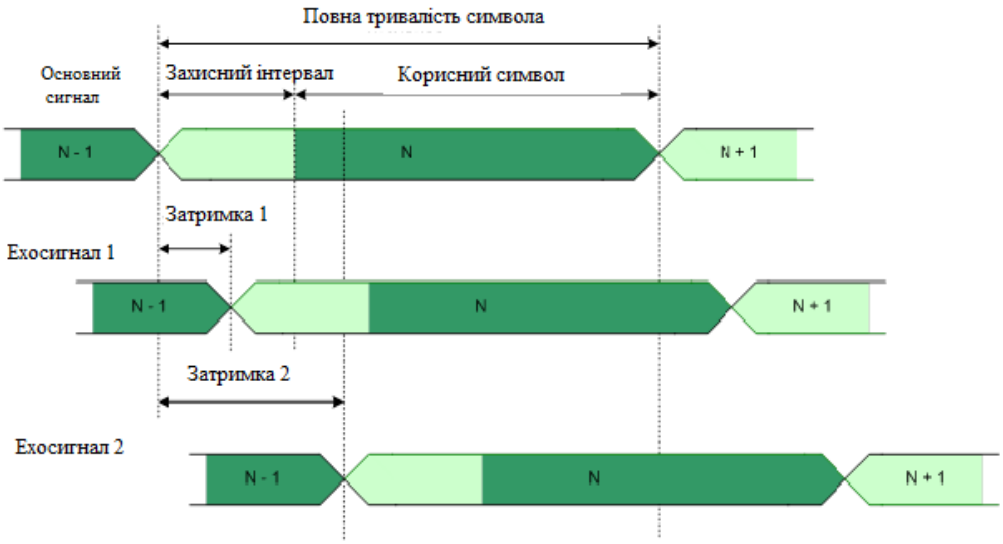


Рисунок 2.9 - Часові інтервали основного та двох ехо-сигналів

На рисунку 2.9 показані тимчасові інтервали для основного сигналу та двох його ехо-сигналів. Затримка першого ехо-сигналу перебуває в припустимих межах, і перехідні процеси через стик двох символів припадають на захисний інтервал основного сигналу, не спотворюючи його корисну частину. Напроти, якщо другий ехо-сигнал затриманий понад припустимі межі, то його перехідна зона припадає на корисну частину основного сигналу, тобто захист не забезпечується. Рисунок 2.10 ілюструє підсумовування декількох затриманих сигналів з утвором сигналу, що заважає, усувається за рахунок захисного інтервалу. [6]

Крім основного сигналу показані відбиті ехо-сигнали 1; 2 і сигнал сусіднього передавача одночастотної мережі (ехо-сигнал 3). На приймач надходить сума цих 4-ох сигналів. При виборі часу T_G більше часу імпульсної реакції каналу або часу затримки поширення, МСІ суттєво знижується, тому що всі перехідні процеси від небажаних сигналів завершуються в межах захисного інтервалу.

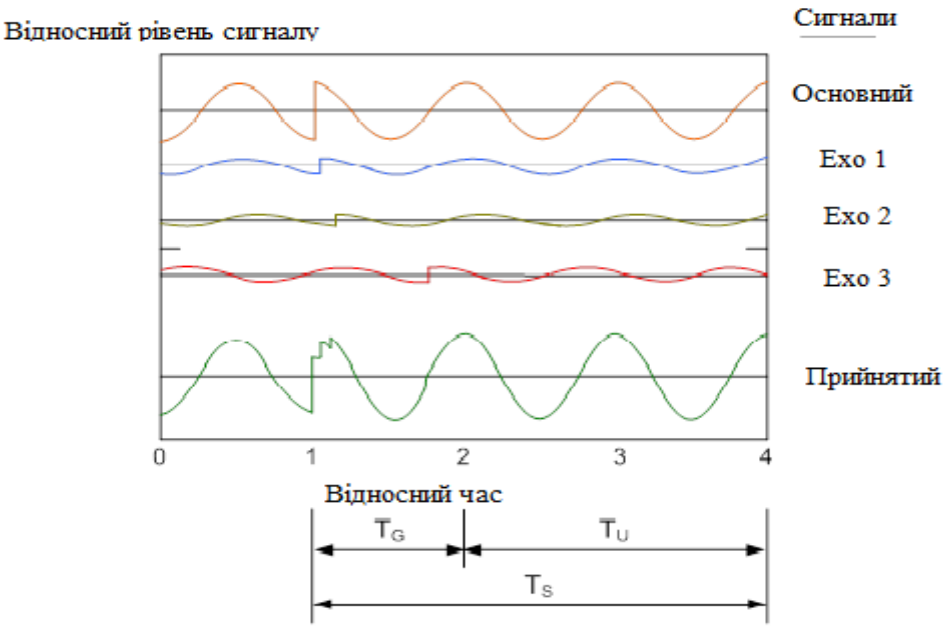


Рисунок 2.10 - Захисний інтервал у символі OFDM

Приклад формування сигналу OFDM за допомогою зворотного швидкого перетворення Фур'є (ЗШПФ по рос. ОБППФ), показаний на рисунку 2.11. Після ЗШПФ обидві частини обчисленого перетворення, переводяться в аналогову форму, проходячи ЦАП і ФНЧ для видалення ВЧ-продуктів, потім надходять у перетворювач частоти, де множаться відповідно на основний та квадратурний сигнали – гармонійне коливання частоти f_0. Це дозволяє після суматора одержати спектр сигналу OFDM, який зсунутий на частоту f_0. Така операція відповідає перетворенню частоти, необхідному при формуванні радіосигналу для обраного каналу.

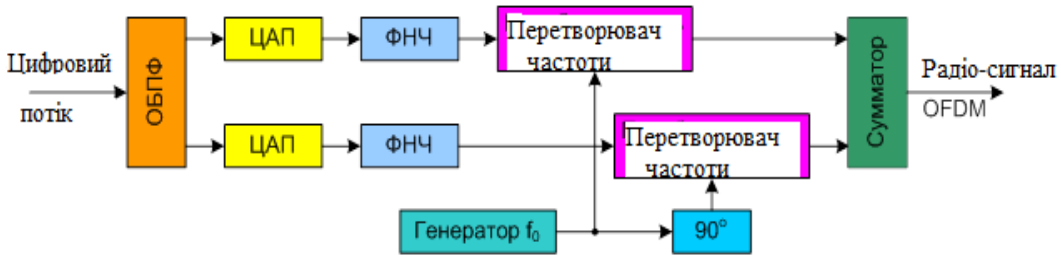


Рисунок 2.11 - Формування радіосигналу OFDM за допомогою зворотного швидкого перетворення Фур'є

Слід зазначити, що даний спосіб модуляції має ще один «резерв» підвищення завадостійкості. У процесі формування переданого сигналу, що містить кілька несучих, може виявитися так, що наступні один за одним послідовно в часі символи модулюють сусідні по частоті несучі. Ця обставина несприятливо впливає на стійкість такої системи передачі до завад, що вражають відразу певний діапазон частот (Рисунок 2.12).

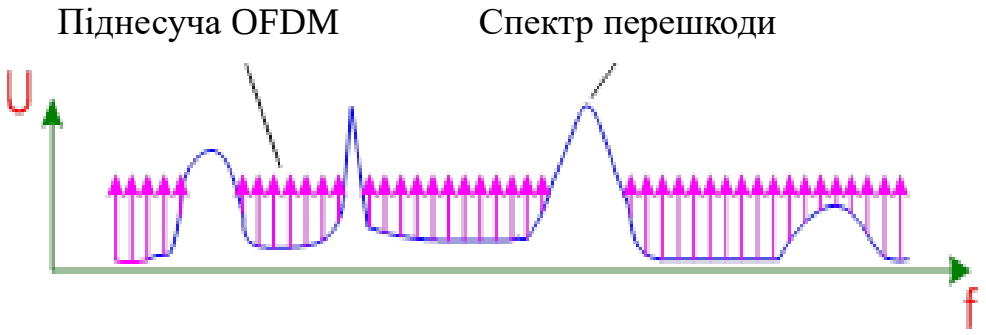


Рисунок 2.12 - Вплив завад при передачі сигналу OFDM

Один з варіантів способу модуляції OFDM, відомий за назвою COFDM, припускає «перемішування» переданих символів у часі таким чином, що наступні один за одним символи корисної інформації на передавальній стороні модулюють ті несучі, номера яких пропонуються спеціальною заздалегідь певною послідовністю. Ця послідовність точно витримується на передавальній стороні й, у зворотному порядку – у приймальному пристрої. Такий захід дозволяє зробити даний спосіб передачі інформації практично нечутливим до різного роду завмиранням, а також завадам, що виключають на короткий час можливість використання якої-небудь ділянки діапазону частот. [5]

Особливістю модуляції OFDM є підвищена нерівномірність рівня потужності групового модульованого сигналу. На рисунку 2.13 показаний результат підсумовування 5-ти немодульованих несучих різних частот. Їхній сумарний сигнал має сильну нерівномірність амплітуди. Відношення пікової до середньої потужності в кожному субканалі OFDM також як і для систем з одиночно несучою залежить тільки від виду сигнального сузір’я та коефіцієнта округлення спектра α. Те-

оретично, відмінність у значеннях відносин пікової потужності до середньої для повного спектра системи COFDM і системи з одиночною несучою становить:

$$\Delta(\frac{P_{OFDM}}{P_O}) = 10\lg N\,. \tag{2.10}$$

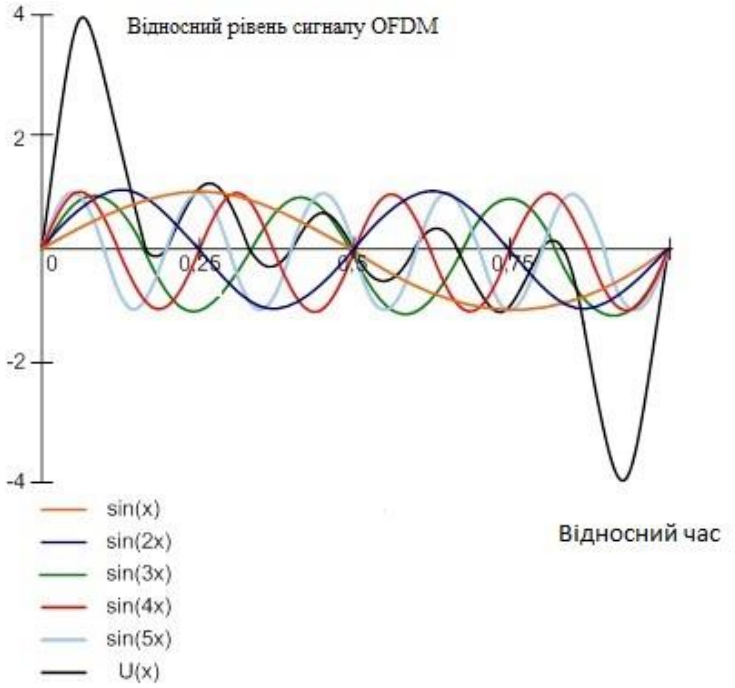


Рисунок 2.13 - Сума несучих OFDM

Однак, практично за рахунок рандомізації даних, скремблювання та інших перетворень структури потоку, теоретичне значення може бути досягнуто в дуже рідкісних випадках, зокрема, при великих розмірах сигнального сузір'я. Оскільки скремблірований сигнал OFDM може розглядатися як послідовність незалежних однаково розподілених несучих, то згідно центральної граничній теоремі теорії ймовірностей при великому числі несучих ($N \geq 20$) їх розподіл наближається до гаусовського. При цьому, ймовірність того, що перевищення пікової потужності над середньою потужністю складе 9,6 дБ, дорівнює 0,1%, а перевищення складе 12 дБ – менше 0,01%. Як наслідок, при OFDM необхідно прагнути формувати сигнал з кількістю субканалів не менше 20.

Ще один підхід полягає у нормуванні амплітуд сигналів субканалів.

До переваг OFDM відносяться наступні властивості:

1. Висока ефективність використання радіочастотного спктру, який має прямокутну форму огинаючої спектру.

2. Протидія міжканальній та міжсимвольній інтерференції.

3. Застосування схем модуляції для кожного субканалу, що дозволяє адаптивну варіацію між завадостійкістю та швидкістю передачі інформації.

До недоліків OFDM відносяться:

1. Необхідна висока синхронізація за частотою та часом.

2. Чутливість до ефекту Доплера.

3. Неідеальність сучасних трансміттерів має фазовий шум.

4. Захисний інтервал, який використаний в OFDM для боротьби з багатопроменевим поширенням, зменшує спектральну ефективність сигналу.

Однак, незважаючи на всі недоліки, OFDM є відмінним рішенням для архітектури WSN, що працюють в умовах міської агломерації.

На даний час, відомо кілька різних модифікацій технології OFDM, які можна зустріти.

1. N-OFDM – несучі розташовуються неортогонально та компактніше, що усуває частотні обмеження класичного OFDM на базі ШПФ. Як наслідок, такий підхід дозволяє значно підвищити пропускну здатність системи, навіть в умовах впливу ефекту Доплера. Його варіації, що мають інші назви та незначні відмінності були розроблені пізніше, згадуються в якості основи для систем мобільного зв’язку 5G.

2. COFDM (Coded OFDM). Даний вид OFDM відрізняється лише тим, що дані попередньо кодуються коригувальними кодами. В DVB-T (C, S), (C2, S2) до речі, використовується саме цей вид OFDM.

3. Flash OFDM (Fast Low-Latency Access With Seamless Handoff OFDM). Ця модифікація була розроблена компанією Flarion Technologies в інтересах функціонування мобільних пристроїв. Усі особливості модифікації полягають в алгоритмах роботи з комутацією пакетів даних.

4. OFDMA – багатокористувацький варіант OFDM (всі субканали розподіляються за кількома користувачами.

5. VOFDM (Vector OFDM). Дану модифікацію курирує компанія Cisco Systems. В основі лежить концепція технології MIMO. Сюди ж можна віднести MIMO-OFDM.

6. WOFDM (Wideband OFDM). Широкосмугова модифікація OFDM розроблена Wi-LAN Inc. У модифікації досягається підвищення пропускної здатності та завадостійкості. Основна відмінність у більшому частотному рознесенні між піднесучими.

2.4. Вибір методів формування модуляційних символів OFDM

Зазвичай, у системах з OFDM використовується квадратурна амплітудна модуляція (Quadrature Amplitude Modulation, QAM). Найменшу спектральну ефективність (відповідно високу завадостійкість) має QAM-4, синонімом якої є квадратурна фазова маніпуляція (Quadrature Phase Shift Keying, QPSK). Співвідношення між зсувами фази модульованого коливання з множини $\{45^0, -45^0, 135^0, -135^0\}$ та множиною символів (дібітів) цифрового повідомлення $\{00, 01, 10, 11\}$ встановлюється в кожному конкретному випадку стандартом на радіоканал і відображається сигнальним сузір'ям (Рисунок 2.14). Стрілками показані можливі переходи з одного фазового стану в інший.

$$S(t) = \sqrt{\frac{2E_s}{T_s}}\left(\frac{a_n^I}{2}\cos 2\pi f_0 t - \frac{a_n^Q}{2}\sin 2\pi f_0 t\right), \text{ при } nT_s < t \le (n+1)T_s, \quad (2.11)$$

де a_n^I і a_n^Q – двійкові інформаційні символи у квадратурних каналах, $E_s = 2E_B$ – енергія канального символу, E_B – енергія інформаційного біта, T_s – тривалість субканального символу, f_0 – несуча частота субканалу.

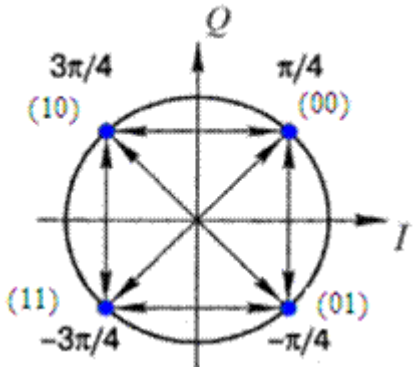


Рисунок 2.14 - Сигнальне сузірря QPSK

Огинаюча кожної посилки сигналу має прямокутну форму, а на стиках посилок можливі стрибки фази на 0^0, $+90^0$ і 180^0. Спектр QPSK є необмеженим. Однак, на практиці його обмежують. В свою чергу, це може призвести до появи паразитної амплітудної модуляції, що обумовлена перехідними процесами (в основному, при стрибками на 180^0).

Для усунення цього недоліку, застосовують модифікацію – зсунуту QPSK (Offset QPSK, OQPSK). В сигналі OQPSK стрибки фази на 180^0 відсутні, оскільки формування виконується з використанням двох квадратурних каналів, зсунутих за часом на половину тривалості символу $0{,}5T_S$. При цьому, стрибки фази на 90^0 залишаються.

При такій реалізації спектр сигналу на виході модулятора є нічим не обмеженим (Рисунок 2.15). Природно, цей сигнал можна обмежити по спектру за допомогою смугового фільтра, включеного на виході модулятора, проте так ніколи не роблять.

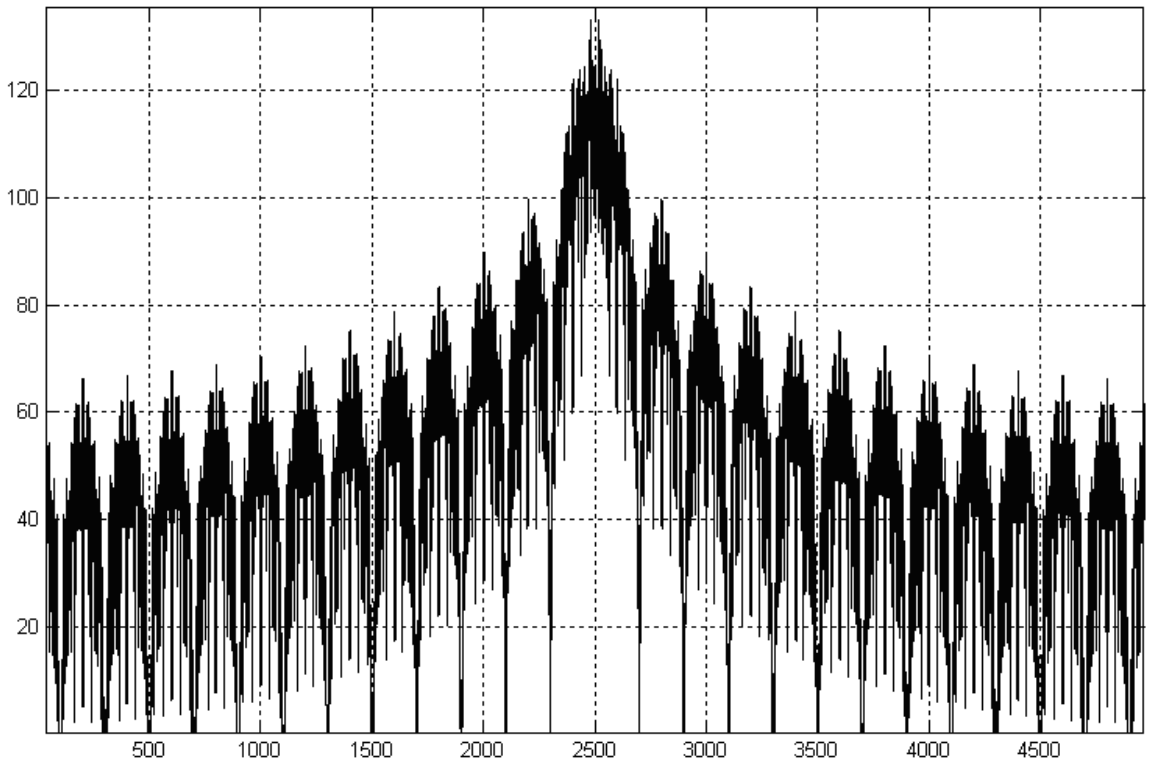


Рисунок 2.15 - Спектр сигналу QPSK, що модульований сигналом NRZ

Як наслідок, згідно п. 2.2, для звуження спектру сигналу доцільно використовувати округлення форми огинаючої. Наприклад, для QPSK прямокутна огинаюча округлюється до форми функції $h(t)$:

$$S(t) = \sqrt{\frac{2E_S}{T_S}} \cdot \sum_{i=1}^{n} \left(\frac{T_S a_n^I}{2} h(t - iT_S) \cos 2\pi f_0 t - \frac{T_S a_n^Q}{2} h(t - iT_S) \sin 2\pi f_0 t \right). \quad (2.12)$$

Така операція має назву округлення за Найквістом (Nyquist QPSK, NQPSK). Функція $h(t)$ вибирається таким чином, щоб забезпечувалася форма спектра у вигляді косо-симетричного зрізу з коефіцієнтом округлення спектра α, а сигнал (2.14) задовольняв умовам відліковості. Найбільш часто використовується cos-округлення зі спектром:

$$G(f) = \begin{cases} 1, & \text{при } 0 < |f| < (1-\alpha)/2T_S \\ \cos^2\left(\frac{nT_S}{2\alpha} \left(f - \frac{1-\alpha}{2T_S} \right) \right) & \text{при } \frac{1-\alpha}{2T_S} < |f| < \frac{1+\alpha}{2T_S} \\ 0, & \text{за межами} \end{cases}. \quad (2.13)$$

Таким же чином можливо сформувати NOQPSK. Структурна схема квадра-

турного модулятора сигналу QPSK, побудована з використанням фільтра Найквіста приведена на рисунку 2.16.

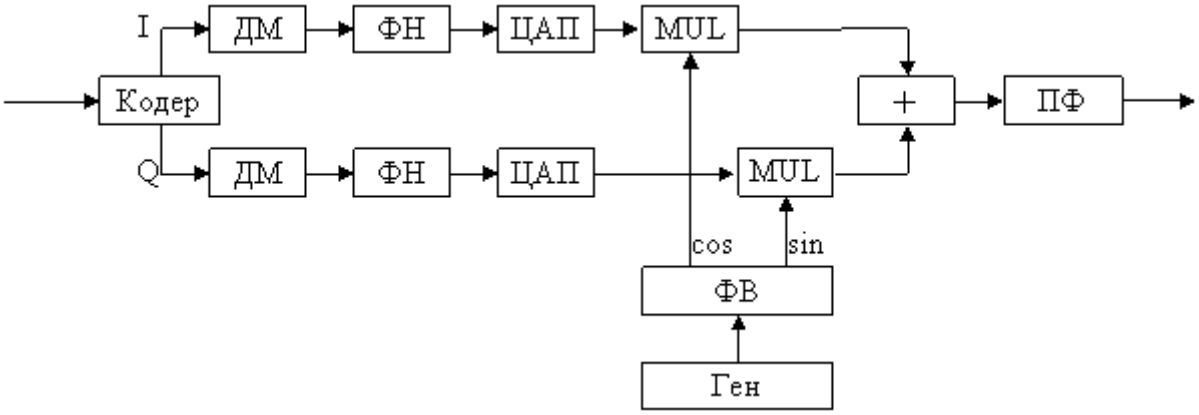


Рисунок 2.16 - Структурна схема модулятора QPSKз використанням фільтра Найквіста (ФН)

Крім звуження спектру сигналу, застосування фільтра Найквіста призводить до зміни амплітуди формованого сигналу. У проміжках між відліковими точками сигналу амплітуда може, як зростати по відношенню до номінального значення, так і зменшуватися майже до нульового значення.

Ще однією модифікацією є диференційна QPSK (Differential Quadrature Phase Shift Keying, DQPSK). Всі імпульси вхідної інформаційної послідовності розбиваються на пари (2-бітові символи). При переході від одного 2-бітового символу до іншого 2-битового символу початкова фаза сигналу змінюється на величину $\Delta\varphi$, яка визначається відповідно до табл. 1. Діаграма переходів станів сигналів, що відповідає цьому методу, представлена на рисунку 2.17. Кружечками позначені дискретні значення, які може приймати фаза несучої, яка відрізняється від деякого початкового значення. Стрілочками показано переходи між дозволеними значеннями фази. Осі координат відповідають синфазній (Inphase) і квадратурній (Quadrature) складовим сигналу. Ця фазова діаграма складається, з двох діаграм: звичайної квадратурної фазової маніпуляції: фазові стани однієї з них позначені як «+», а іншої значком «×», і діаграми зсуву одна відносно іншої на кут $\pi/4$. При переході від одного символу до іншого відбувається зміна фази від одного зі ста-

нів першої діаграми до одного зі станів другої, а при переході до наступного символу – повернення до попередньої діаграми, не до колишнього фазового стану.

Таблиця 1 - Закон зміни фази DQPSK

Біти вхідної послідовності		$\Delta\varphi_k(x_k y_k)$
Непарні (перші біти)	Парні (другі біти)	
1	1	$-\frac{3}{4}\pi$
0	1	$\frac{3}{4}\pi$
0	0	$-\frac{\pi}{4}$
1	0	$\frac{\pi}{4}$

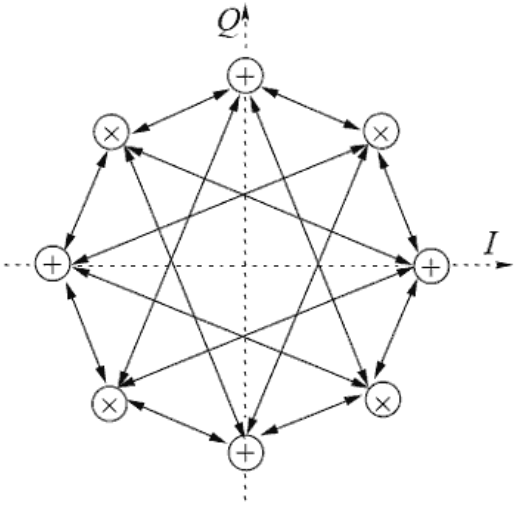


Рисунок 2.17 - Фазова діаграма DQPSK

Взагалі, якщо прийняти $a_n^Q = 0$, то відбувається трансформація до двійкової фазової маніпуляції або BPSK (Binary PSK). Підвидом сімейства BPSK є диференціальна (відносна) BPSK (DBPSK). Необхідність відносної модуляції обумовлена тим, що більшість схем відновлення несучої частоти призводять до фазової неоднозначності відновленої несучої. В результаті відновлення може утворитися постійний фазовий зсув, кратний 180^0. Порівняння сигналу з відновленою несучою призведе в даному випадку до інвертування (зміни значень всіх бітів на протилежні). Цього можна уникнути, якщо кодувати неабсолютним зсувом фази, а йо-

го зміною щодо значення на попередньому бітовому інтервалі. Наприклад, якщо на поточному бітовому інтервалі значення біта змінилося в порівнянні з попереднім, то змінюється й значення фази модульованого сигналу на 180^0, якщо не змінився, то фаза також не змінюється. Тобто, інформація визначається різницею фаз сусідніх посилок. [8]

Застосування відносного кодування призводить до розмноження помилок на прийомі та знижує стійкість. Однак, диференціальне кодування є раціональним способом вирішення неоднозначності фази в демодуляторі, що виникає при відновленні несучої для когерентного прийому, а також забезпечує можливість застосування фазової модуляції при некогерентному прийомі.

$$S(t) = \sqrt{\frac{2E_s}{T_s}} a_n \cos 2\pi f_0 t, \qquad (2.14)$$

де $a_n = 1$ при $(a_{n-1}, a_n) = \begin{Bmatrix} +1 & +1 \\ -1 & -1 \end{Bmatrix}$ або $a_n = -1$ при $(a_{n-1}, a_n) = \begin{Bmatrix} +1 & -1 \\ -1 & +1 \end{Bmatrix}$.

Розглянемо ще деякі модифікації FSK (GFSK). Маніпуляція з мінімальним частотним зсувом (Minimal Shift Keying, MSK). Теоретично було обґрунтовано при яких умовах можлива маніпуляція з розносом частот Br/2. В даному випадку, відбулася відмова від генератора керованого напругою, і для формування MSK використовуються I/Q-модулятори. MSK являє собою одну частоту, що має на різних посилках різну фазу, причому фаза ніколи не залишається на місці, а має постійний різний набіг, що й дають дві частоти з мінімальним рознесенням (Рисунок 2.18). Введення фільтра Гауса в схему MSK-модулятора (Рисунок 2.19) дозволяє зменшити ще більше загальний спектр сигналу, але платою за це буде деяке зниження завадостійкості – GMSK. Стандартно, GMSK маніпуляція може мати спектр приблизно всього на 12÷15% більше від Br, менші значення є сильною втратою завадостійкості (Рисунок 2.20).

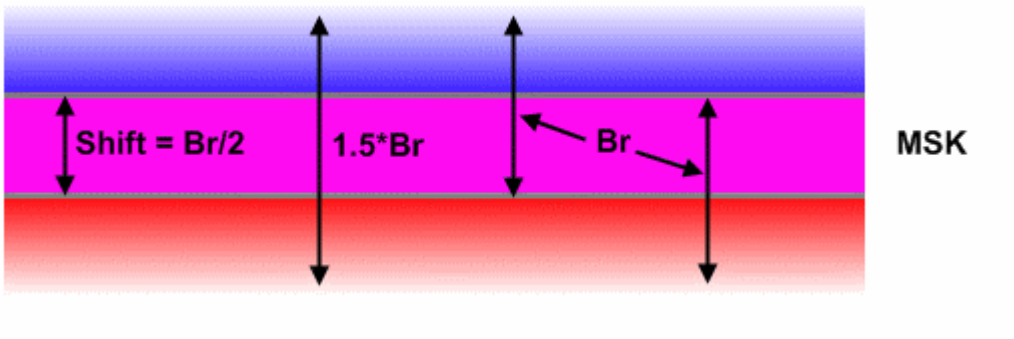


Рисунок 2.18 - Рознесення частот при MSK

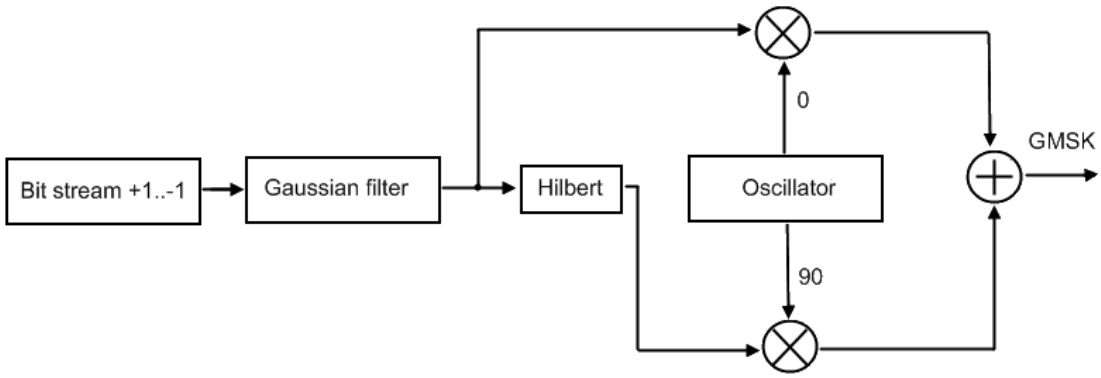


Рисунок 2.19 - Модулятор GMSK

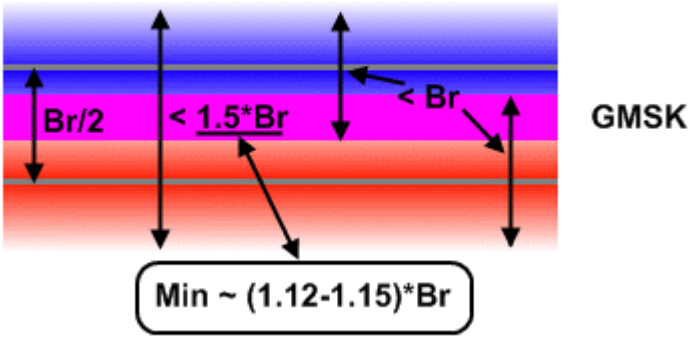


Рисунок 2.20 - Рознесення частот при GMSK

Найбільшу завадостійкість має звичайно MSK при когерентному демодуляторі. Звуження смуги при FSK дозволяє демодулювати режими MSK і GMSK звичайними частотними детекторами.

Маємо характеристики цих модуляцій. FSK – простота реалізації та відносно широкий спектр. GFSK – простота реалізації менший спектр, але й трохи гірша завадостійкість стосовно FSK. MSK – дуже висока завадостійкість при віднос-

но невеликому спектрі, але ускладнена схема модулятора-демодулятора. GMSK – ширина спектра практично близька до теоретичної межі Br, трохи гірша завадостійкість у порівнянні з MSK, ускладнена схема модулятора-демодулятора така ж як в MSK. [11]

MSK і GMSK мають назву «напівмоди», ця не загальноприйнята назва, просто треба було якось виділити цей клас сигналів із загального сімейства PSK, тому що володіючи й ознаками PSK і ознаками FSK вони й насправді займають особливе проміжне положення. Друга гармоніка цих напівмодів, має дві яскраві спектральні лінії, рознос між якими рівний Br, що є одним з ознак цих режимів. Це необхідна умова їх визначення при аналізі, але не достатнє. Дві лінії в другому ступені так само дають і SDPSK і OQPSK режими. SDPSK у загальному випадку не вимагає синхронності переходів в екстремумах несучої й за рахунок цього має більшу ширину спектра чому MSK, яку так само можна зменшити фільтруючи бітовий потік перед подачею на модулятор, що й роблять використовуючи звичайно RRC-фільтри. SDPSK (PSK-2 з обертанням фази) у сутності має такий же результуючий сигнал як і MSK, тільки з більш широким спектром, і так само може демодулюватися FSK-демодулятором, потрапляючи під визначення напівмод. Сучасні методи формування різних сигналів найчастіше стирають межу між різними режимами, з тієї причини, що розробники майже завжди (це сильно спрощує розробку) прагнуть вибрати кратне співвідношення між тактовою частотою маніпуляції та частотою несучої.

2.5. Рекомендації щодо використання багатопозиційних сигналів у бездротових сенсорних мережах

Вході досліджень запропоновано використати варіанти формування багатопозиційних сигналів для радіоканалів WSN:

1. OFDM з формуванням модуляційних символів субканалів на основі одного з методів: QAM, варіацій QPSK, DPSK та ін.) або BPSK (NBPSK, DSPSK та ін.), які розглянуті в п. 2.4.

2. COFDM з формуванням модуляційних символів субканалів на основі одного з методів: QAM, варіацій QPSK, DPSK та ін.) або BPSK (NBPSK, DSPSK та ін.).

3. N-OFDM з формуванням модуляційних символів субканалів на основі одного з методів: QAM, варіацій QPSK, DPSK та ін.) або BPSK (NBPSK, DSPSK та ін.).

4. Таким же чином, що і за пп. 1-3, відрізняється тим, що застосовується варіація QPSK, в який квадратурні канали продубльовано, тобто для їх формування використовується один єдиний інформаційний потік замість двох незалежних.

5. Таким же чином, що і за п. 4, тільки замість QPSK запропонована використання QAM з більш високою спектральною ефективністю.

6. Використання N-OFDM (в т. ч. з блоковою варіацією компоновки групового сигналу) з формуванням модуляційних символів субканалів на основі одного з методів FSK (GFSK, MSK або GMSK) – Рисунок 2.21.

7. Таким же чином що і за п. 6, але без врахування тривалості кадру N-OFDM.

8. Теж саме, що і за пп. 7 і 8, відрізняється тим, що використані додатково процедури додаткового стробування відліків АЦП.

9. Використання сигналів квазі-OFDM (COFDM), в яких субканали попарно згруповані для передачі сигналів +Br і -BR сигналів за методом FSK – Рисунок 2.22.

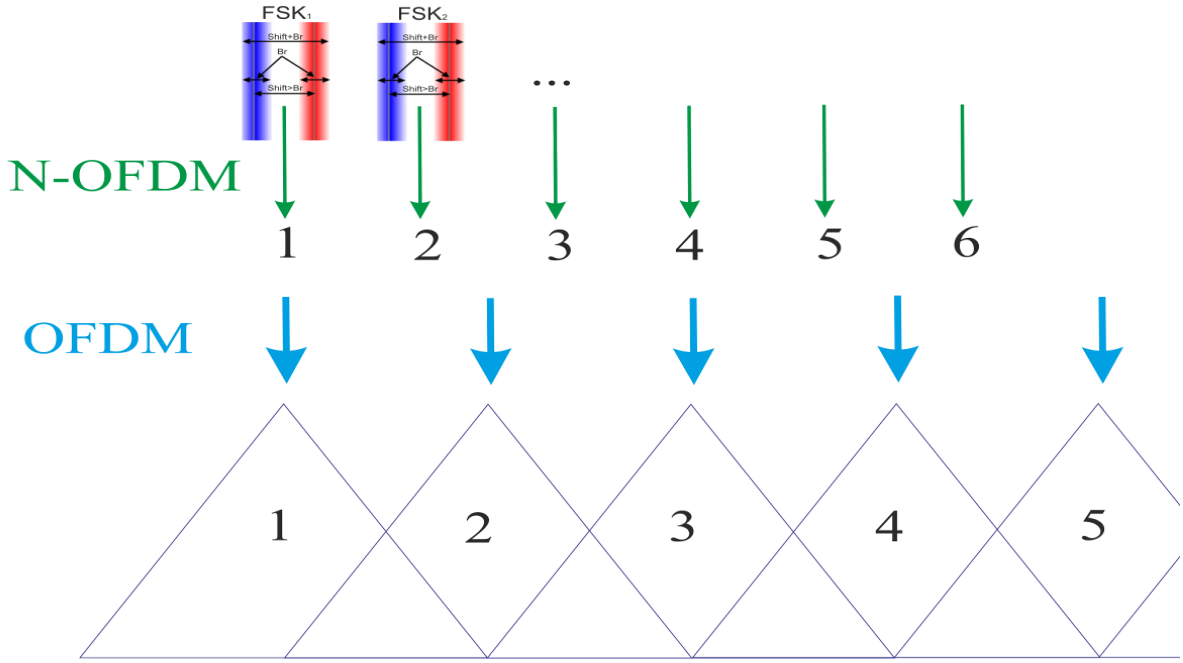


Рисунок 2.21 - Використання N-OFDM спільно з FSK (GFSK, MSK або GMSK)

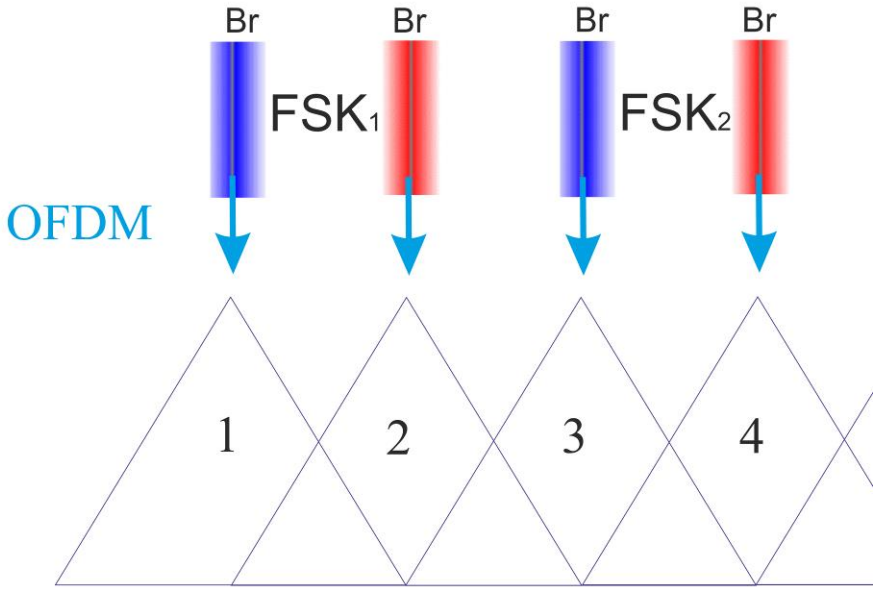


Рисунок 2.22 - Попарне групування субканалів квазі-OFDM

10. Таким же чином, що і за п. 9, відрізняється використанням сигналів GFSK, MSK або GMSK, в т. ч. з врахуванням сигнально-завадової обстановки (тобто використання різних методів для різних окремих пар субканалів).

11. Таким же чином, що і за пп. 9 і 10, відрізняється тим, що всі субканали поділяються на дві групи для передачі відповідних бічних сигналів FSK, GFSK, MSK або GMSK, в т. ч. враховуючи блочну компоновку (Рисунок 2.23).

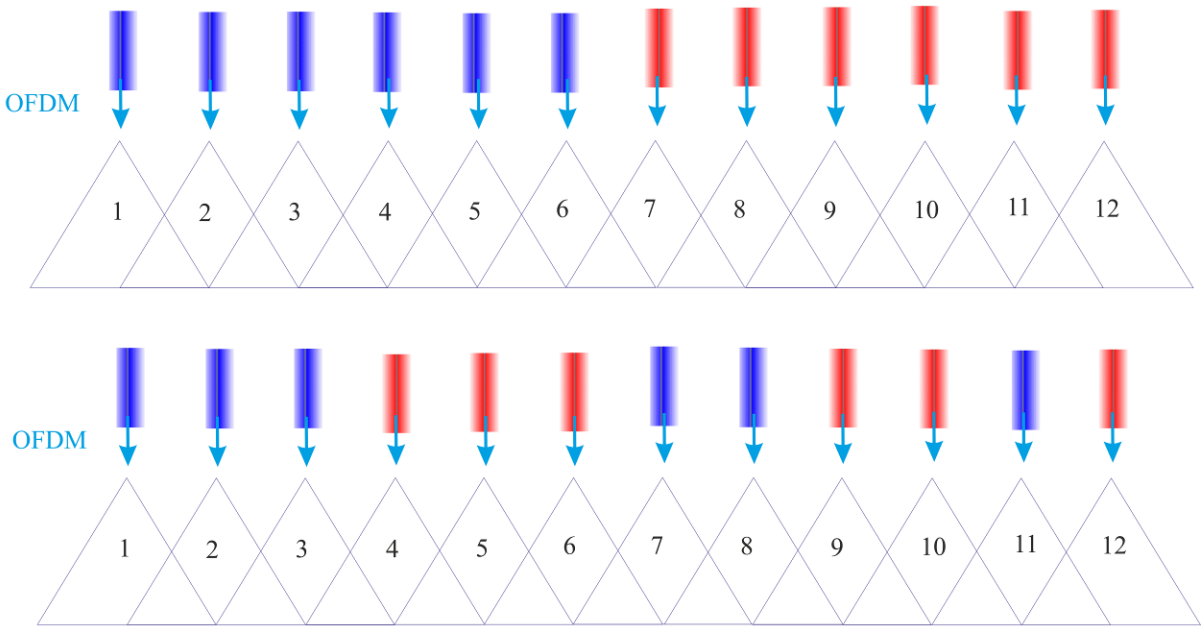


Рисунок 2.23 - Групування субканалів квазі-OFDM

12. Теж саме, що і за пп. 11, відрізняється тим, що для врахування алфавіту кодування групи містить не однакову кількість субканалів.

13. Теж саме, що і за пп. 9÷12, відрізняється застосуванням N-OFDM.

14. Теж саме, що і за пп. 1÷13, відрізняється додаванням технології MIMO в т.ч. за аналогією з п. 4.

15. Теж саме, що і за пп. 1÷14, відрізняється забезпеченням доступу на основі OFDMA. Це дозволяє деякою мірою усунути недоліки методу доступу CSM-A/CA.

Таким чином, замість одиничного сигналу FSK (GFSK) застосовується OFDM-подібний сигнал зі швидкістю передачі даних, яка дорівнює швидкості одного субканалу, що менше в N раз (де N – кількість субканалів, що відведені під передачу корисної інформації) у порівнянні з сигналом класичним для WSN на основі FSK (GFSK). Як видно, підвищення енергетики може відбуватись за рахунок введення надмірності (дубльовані канали) та переваг обробки на приймальній стороні сигналів OFDM. При цьому, з’явилась можливість варіації вибору між завадостійкістю та спектральною ефективністю радіоканалу WSN.

Підвищити завадостійкість БСМ можливо удосконаленням процедур детектування сигналів.

2.6. Сутність методу спектрального детектування

Для підвищення спектральної ефективності (або за її рахунок завадостійкості) каналів зв'язку в сучасних технічних рішеннях застосовується багаторівневе кодування, у т. ч., з OFDM. Як наслідок, використання зазначеного критерію про наявність сигналу в умовах впливу шумів, чи перешкод слабкого рівня прийому є не завжди доцільним. У такому випадку, доводиться орієнтуватися на специфічні методи адаптації рівня чи порога зниження спектральної ефективності телекомунікаційної системи в цілому.

Збільшення числа параметрів сигналу, що враховуються в процесі обробки, веде до росту імовірності ухвалення правильного рішення. У розглянутому контексті, одним з варіантів підвищення вірогідності декодування інформації є аналіз спектральних складових оброблюваного сигналу.

Сутність розглянутого методу обробки полягає в наступному. Спочатку формується спектр прийнятого сигналу з видаленням складових, амплітуди які знаходяться нижче визначеного граничного значення (шуми та одиночні імпульсні завади, як правило, характеризуються великою кількістю частотних складових з малими амплітудами). Далі, проводиться його порівняння з еталонними масками всіх можливих варіантів пакетів імпульсів. При цьому, кількість еталонних варіантів спектрів пакетів визначається довжиною пакету по відомій формулі. Той еталонний пакет, зі спектром якого найбільше корелює спектр прийнятого пакета імпульсів, буде вважатися правильно прийнятим сигналом.

Виходячи з вище викладеного, дана задача може бути віднесена, до задачі розпізнавання образу сигналу. Тобто знімається невизначеність у питанні про те, до якого із сигналів з числа еталонних відноситься прийнятий сигнал. У результаті розпізнавання ця невизначеність зменшується, причому можливо і до нуля (коли сигнал ідентифікується однозначно).

Як відомо, в основі систем розпізнавання сигналів лежать статистичні методи. При аналізі прийнятого сигналу на тлі перешкод, можливо, розглядати два можливих випадки:

– завада є гаусовським випадковим процесом (шум), при цьому математичне очікування даної перешкоди дорівнює нулю, а дисперсія – приймає визначене значення;

– завада описується наближеним ланцюгом Маркова, тоді дана перешкода характеризується значеннями математичного очікування і дисперсії не рівними нулю.

Для аналізу спектрів прийнятих сигналів пропонується використовувати процедуру - швидке перетворення Фур'є (ШПФ). По своїй суті, вона зводиться до формування лінійки ортогональних фільтрів (Рисунок 2.24) кількість яких прямо пропорційна кількості крапок операції ШПФ. Відповідно, чим більше цих крапок, тим з більшою імовірністю зі спектра прийнятого сигналу будуть вилучені складові шуму, а також можливо підвищити імовірність правильного прийому сигналу при тих самих характеристиках точності АЦП.

Аналіз пропонується проводити по методу ковзаючого вікна пакета імпульсів, довжина якого може бути оптимізована під обчислювальні можливості конкретної апаратури.

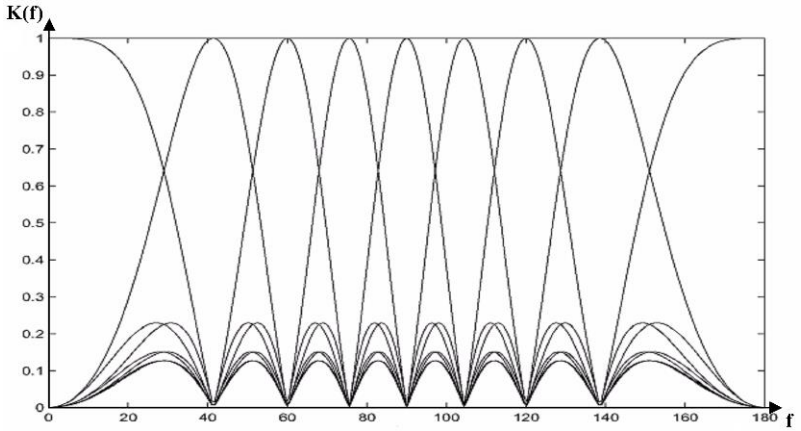


Рисунок 2.24 - Лінійка фільтрів ШПФ

У результаті проведення даної процедури вхідний сигнал буде представлений співвідношенням:

$$e(t) = B_0 + \sum_{n=1}^{\infty} (A_n \sin n\omega t + B_n \cos n\omega t) \ , \qquad (2.15)$$

де $\omega = 2\pi / T$, $e(t)$ – періодична функція часу, B_0 – постійна складова сигналу,

$$B_0 = \frac{1}{T}\int_{-T/2}^{T/2} e(t)dt,\ B_n = \frac{2}{T}\int_{-T/2}^{T/2} e(t)\cos n\omega t dt,\ A_n = \frac{2}{T}\int_{-T/2}^{T/2} e(t)\sin n\omega t dt.$$

Передбачається, що в WSN існує «генератор еталонних сигналів», під яким у даній роботі розуміється пристрій збереження значень амплітуди для кожної крапки ШПФ для всього набору можливих прийнятих сигналів. Інформація «генератора еталонних сигналів» має вид:

$$A = A_i(a_{i.j}),\qquad (2.16)$$

де $a_{i.j}$ – еталонне значення амплітуди для і-го сигналу в j-ом вікні при проведенні ШПФ.

Виходячи з вище зазначених вихідних даних, можливо, запропонувати процедуру проведення розпізнавання прийнятого сигналу. У даній процедурі передбачається два етапи реалізації.

На першому етапі пропонується виділити з усієї безлічі сигналів «генератора еталонних сигналів» підмножина сигналів, що найбільше «схожі» на прийнятий.

На другому етапі з вищевказаної підмножини виділяється сигнал, що із установленим рівнем якості відповідає прийнятому сигналу.

Для реалізації першого етапу процедури розпізнавання сигналу пропонується використовувати як критерій вибору «схожих» сигналів наступне правило: до «схожого» сигналу відносяться всі сигнали, що входять до складу «генератора еталонних сигналів», якщо їхній спектральний склад збігається з прийнятим із заданим рівнем імовірності розпізнавання, тобто:

$$P_p \le P_n,\qquad (2.17)$$

де P_p – заданий рівень імовірності розпізнавання прийнятого сигналу, P_n – розрахункове значення імовірності «подібності» сигналу.

Значення імовірності P_n можливо визначити на основі проведення статистичної обробки з використанням співвідношення:

$$P_n = \frac{n}{N}, \tag{2.18}$$

де N – кількість спектральних складових при проведенні ШПФ, n – кількість складових, котрі збіглися для еталонного і прийнятого сигналів.

Другий етап полягає в досягненні мінімального значення розбіжності квадратичної міри між прийнятим і еталонним сигналами. Незміщеною оцінкою міри наближення є дисперсія розбіжності між амплітудними значеннями еталонних і прийнятого сигналами.

Розрахунок результатів між амплітудними значеннями залишків еталонних і прийнятого сигналами може проводитися з використанням методу послідовного перебору, у наступній послідовності, увівши припущення про рівну точність проведення їхнього визначення.

1. У випадку, якщо відомі значення перешкод (значення і знаки), з результатів амплітудних значень для даної спектральний складової прийнятого сигналу $\tilde{\mathrm{X}}_q$ віддаляється систематична перешкода Δ_c шляхом уведення виправлення, використовуючи формулу $\tilde{X}_q = X - \Delta_c$, і виходить виправлений результат для кожної зі спектральних складових X_q, $q=\overline{1,n}$.

Систематичні перешкоди (чи їхні залишки), що неможливо виключити в процесі прийому сигналу відносимо до таких, котрі не виключені, і надалі при обробці сигналу розглядаються як випадкові перешкоди.

2. По виправленому результаті для кожної зі спектральних складових X_q прийнятого сигналу і значенням спектральних складових і-го еталонного сигналу $X_q^{эі}$, $i=\overline{1,k}$ визначають значення відхилення $\Delta_q = X_q - X_q^{эі}$. За відомим значенням Δ_q визначається оцінка математичного чекання відхилення для кожного і-го еталонного сигналу. Як таку оцінку, виходячи з вимог, що пред'являються до неї, є середньоарифметичне значення, що визначається виразом:

$$\overline{\Delta}_i = \frac{\sum_{q=1}^{n} \Delta_q}{n} \ . \qquad (2.19)$$

3. По відомим $\overline{\Delta}_i$ і Δ_q визначається незміщена оцінка значення середньоквадратичного відхилення з використанням співвідношення:

$$\hat{\sigma}_\Delta = \sqrt{\frac{1}{n-1} \sum_{q=1}^{n} \left(\Delta_q - \overline{\Delta}_i\right)^2} . \qquad (2.20)$$

4. Визначаються помилки відхилення значень амплітуд для прийнятого й еталонного сигналів. Для більшості законів розподілу границі цензурування приблизно визначаються з використанням співвідношення:

$$t_{гр} = 1{,}55 + 0{,}8\sqrt{\varepsilon_i - 1} \cdot \lg(N/10) \ , \qquad (2.21)$$

де $\varepsilon_i = \mu_4 / \sigma_\Delta{}^4$ – оцінка ексцесу для отриманої вибірки, $\mu_4 = \frac{\sum_{i=1}^{n} (X_i - \overline{X})^4}{n}$ – 4-ий центральний момент, отриманий за результатами вибірки.

З подальшої обробки віддаляються всі відліки, що не задовольняють співвідношенню $\left|\Delta_q\right| \geq t_{гр} \cdot \sigma_\Delta$.

5. Після виключення Δ_q (еквівалентно виключенню значень X_q) для забезпечення необхідного рівня імовірності прийому сигналу необхідно провести операцію по відновленню втраченого інформативного параметра, для чого можна скористатися різницевими операторами. Вони мають одну особливість – оператор порядку $q+1$ анулює поліном ступеня q.

6. Після завершення даної операції, як прийнятий сигнал, приймається такий еталонний сигнал (пакет), для якого виконується вимога:

$$\sum_{q=1}^{n} \Delta_q^i \to \min \ . \qquad (2.25)$$

Вихідними даними для проведення даної операції є крапкові характеристики фільтрів і АЦП, кількість крапок ШПФ.

Таким чином, запропонований спосіб обробки сигналів, на відміну від ві-

домих методів спектральної фільтрації не приводить до збільшення загальної кількості переданих символів, а виконується проведенням аналізу спектрального складу прийнятого сигналу. Даний спосіб, можливо, використовувати як самостійно так і з методом безперервного кодування з виправленням помилок.

2.7. Застосування технології MIMO в БСМ

Технологія MIMO *(англ. Multiple Input Multiple Output)* — це найсучасніша форма сигналу, яка вирішує багато проблем, з якими стикаються сучасні бездротові системи це системи зв'язку з приймальними і передавальними рознесеними антенами. Їхнє використання дозволяє проводити просторову і часову обробку сигналів, ефективніше використовувати випромінювану передавачем потужність і знижувати негативний вплив завад. Пропускна спроможність збільшується пропорційно числу антен у порівнянні з одноелементними антенами.

Прикладом застосування технології MIMO є радіостанції SiLVUS (Рисунок 2.25)

Рисунок 2.25 - Радіостанції SILVUS

Кілька антен для передавачів і приймачів значно покращують продуктивність зв’язку. У багатьох сучасних телекомунікаційних стандартах, особливо в споживчому просторі, використовується технологія кількох антен (MIMO) через

значні переваги, які вона надає перед аналогічною системою, що використовує трансивери з однією антеною (SISO).

MIMO розшифровується як *Multiple-In Multiple-Out* , посилаючись на той факт, що коли пакет передається в канал, він передається більш ніж на одну антену, а коли він виходить з каналу, він приймається на кілька антен. [16]

Кілька антен у передавача та приймача вводять сигнальні ступені свободи, які були відсутні в системах SISO. Це називається просторовим ступенем свободи. Просторові ступені свободи можуть бути використані для «різноманітності», «мультиплексування» або їх комбінації. Простими словами, різноманітність означає надмірність.

Простим прикладом рознесення є кілька антен, які намагаються прийняти той самий сигнал. Сигнал, отриманий двома антенами, спотворюється шумом, який не корельований між антенами, тому, об’єднавши два сигнали, можна відтворити сигнал кращої якості. Аналогія тут полягає в тому, що, дивлячись на той самий об’єкт з двох різних точок зору, можна отримати повнішу інформацію про об’єкт. Рознесення також можна досягти за допомогою кількох передавальних антен за допомогою методів просторово-часового кодування (STC).

Другою основною технікою MIMO є просторове мультиплексування. Бездротовий канал — це матриця, яка є функцією геометрії приймально-передавальної антенної решітки та розсіювання/відбивачів, присутніх у середовищі.

Коли пара передавач/приймач MIMO працює в середовищі, багатому на розсіювання, матриця каналу стає оборотною, таким чином дозволяючи приймачу декодувати всі різні сигнали, що передаються через різні апертури передавальної антени, що призводить до посилення мультиплексування. Існує компроміс між кількістю різноманітності та посиленням мультиплексування, яке може забезпечити система MIMO (Рисунок 2.26). Типова пара передавач/приймач MIMO автоматично знаходить робочу точку на кривій компромісу рознесеного мультиплексування на основі миттєвих умов бездротового каналу.

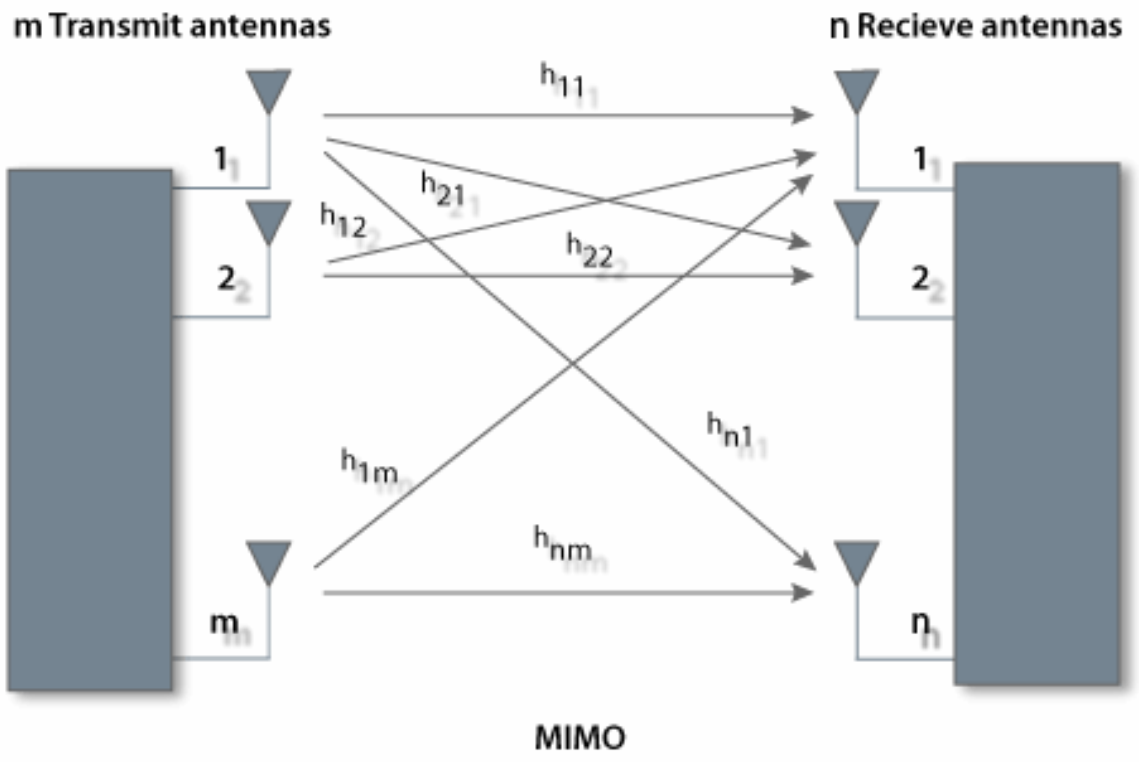


Рисунок 2.26 - Технологія MIMO

Мультиплексування з кодованим ортогональним частотним поділом каналів (COFDM) є альтернативою сигналу з однією несучою, яка часто використовується через обмеження систем з однією несучою для широкосмугових програм, де присутня багатопроменевість. Ці обмеження зумовлені частотно-вибірковим завмиранням, яке спричиняє значну різницю потужності сигналу прийому в широкосмуговому каналі, а також міжсимвольними перешкодами, які можуть виникати в середовищах із великим розповсюдженням затримки. COFDM розбиває широкосмуговий канал на багато окремих вузьких підканалів або піднесучих, як показано нижче на (Рисунок 2.27).

Рисунок 2.27 - Сигнали COFDM

Термін «ортогональна» означає той факт, що кожна з піднесучих створюється таким чином, що за своєю суттю не заважає іншим піднесучим без необхідності фільтрації кожної з них у частотній області, як це традиційно робиться для ізоляції каналів один від одного.

Проблема частотного вибіркового завмирання вирішується шляхом поєднання використання піднесучих із використанням кодування з прямим виправленням помилок, яким є C у COFDM. Кодування FEC перетворює задану кількість бітів у більшу кількість бітів, які містять надлишковість інформації. Грубо кажучи, якщо x бітів перетворити на 2x біти, половина з них може бути втрачена, але вихідні дані все одно відновляться. Цей сценарій називається кодом швидкості ½. Перетворення кожні 5 біт даних на 6 біт буде кодом швидкості 5/6. Код 5/6 дозволяє пропускати більше даних користувача, але більш сприйнятливий до втрати або пошкодження бітів. Це кодування FEC використовується для розподілу даних між піднесучими системи COFDM. Таким чином, навіть якщо певна піднесуча страждає від частотно-селективного завмирання до такої міри, що вона повністю втрачена, дані можна відновити, оскільки вони були надлишково закодовані на інших піднесучих.

Бездротовий зв'язок COFDM також забезпечує практичне вирішення проблеми міжсимвольної інтерференції (ISI). Цю проблему можна продемонструвати за допомогою наступної ілюстрації (Рисунок 2.28):

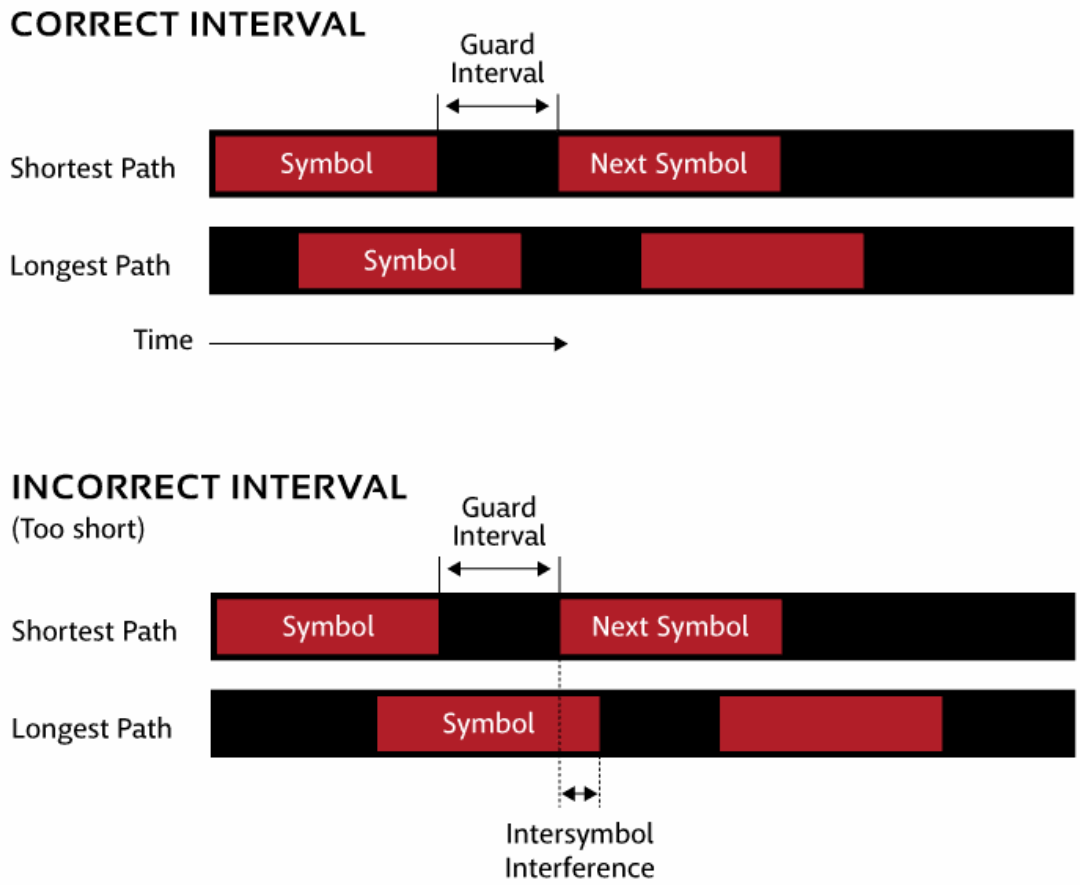


Рисунок 2.28 - Міжсимвольна інтерференція (ISI)

Між кожним переданим символом залишається безшумний захисний інтервал, щоб у приймача був час для отримання копії символу, що надходить на довшому відбитому шляху, без перекриття з наступним символом. Наведена вище ілюстрація (Рисунок 2.28) показує, що відбувається в приймачі, коли захисний інтервал достатньо довгий, а коли він занадто короткий, що призводить до ISI.

Проблема широкосмугової системи з однією несучою полягає в тому, що довжина символу стає дуже малою для даної швидкості передачі даних. У практичних сценаріях захисний інтервал, необхідний для врахування відмінностей у довжині шляху, може стати таким же чи довшим, ніж символ. Це значно зменшує кількість даних, які можна надіслати, оскільки період мовчання починає домінувати.

Символи бездротової системи COFDM стають довшими прямо пропорційно кількості використаних піднесучих. Таким чином, захисний інтервал заданої довжини матиме набагато менший вплив на кількість даних, які можуть бути передані, оскільки символ перенесення даних домінує над тихим захисним інтервалом.

Прийоми MIMO:

1. Формування власного променя.

2. Просторово-часове кодування STC.

3. Просторове мультиплексування.

Усі ці методи, використовуються чі окремо чі комбіновано, забезпечують канал зв’язку з меншою потужністю передачі, з більшою завадостійкістю, дальністю, або більшою пропускною здатністю.

Висновок

На даний час, в якості пріоритетних шляхів оптимізації БСМ на рівні системи передачі даних слід вказати про використання завадостійкого кодування, сигнально-кодових конструкцій, багатопозиційних сигналів та їх комбінацій.

В свою чергу, заслуговують уваги напрямки, що спираються на впровадження інноваційних технологій, які отримали значне поширення в більше розвинутих мережах, наприклад: 8021.11ac(ax), 5G, MU-MIMO, Massive MIMO та ін.

В ході досліджень запропоновані варіанти формування багатопозиційних сигналів для радіоканалів БСМ. Замість одиничного сигналу FSK (GFSK) застосовується OFDM-подібний сигнал зі швидкістю передачі даних, яка дорівнює швидкості одного субканалу, що менше в N раз (де N – кількість субканалів, що відведені під передачу корисної інформації) у порівнянні з сигналом класичним для БСМ на основі FSK (GFSK). При цьому, з’явилась можливість варіацій вибору між завадостійкістю та спектральною ефективністю радіоканалу БСМ.

Підвищити завадостійкість БСМ можливо також за рахунок удосконалення процедур детектування сигналів.

Запропонований метод обробки сигналів, на відміну від відомих методів спектральної фільтрації не призводить до збільшення загальної кількості переданих символів, а виконується проведенням аналізу спектрального складу прийнятого сигналу. Даний метод, можливо використовувати, як самостійно так і з методами безперервного кодування з виправленням помилок.

РОЗДІЛ 3.
ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ПРИЙНЯТИХ РІШЕНЬ

3.1. Експериментальне підтвердження працездатності методу спектрального детектування сигналу в умовах впливу вузькосмугової завади

Для реалізації експерименту був використаний пакет Mathcad. Дослідження були проведені для 2-ох варіантів вузькосмугової завади:

– синусоїдальна немодульована завада;

– вузькосмуговий фазоманіпульований сигнал зі швидкістю маніпуляції в 4 рази меншої швидкості детектованого сигналу. [13]

На початку моделювання в пакеті Mathcad формувався вектор *W*, що містить комбінацію 4-ох відеоімпульсів з 64-ох відліків із загальною довжиною вибірки рівної 256-ти відліків і амплітудою імпульсів, що дорівнює 1. Приклад комбінації (послідовність 1011) представлений на рисунку 3.1.

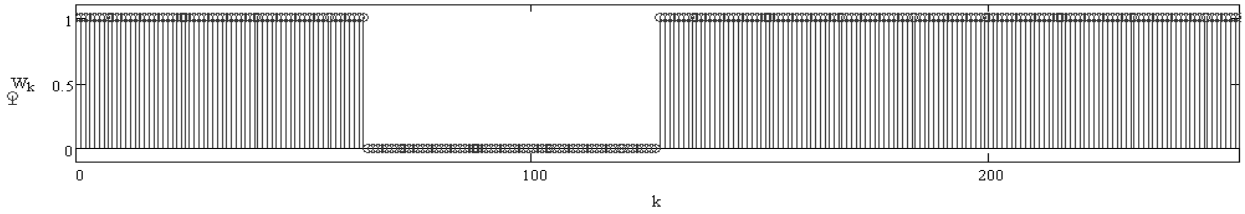


Рисунок 3.1 - Послідовність відеоімпульсів, що підлягає передачі

Розрахунки значень вектору вузькосмугової завади визначався виразом:

$$N_S = A_S \cdot \left(\frac{2\pi \cdot k}{k_{krat}} \right), \tag{3.1}$$

де A_S – амплітуда завади, k_{krat} – коефіцієнт кратності, що визначає частоту завади, $k = 0 \ldots 255$ – номер відліку у вибірці.

Далі, за допомогою додавання вектору адитивного шуму *N* і вектору вузькосмугової завади N_S, імітувався процес передачі сигналу через середовище по-

ширення в умовах впливу зазначених видів завад:

$$U = W + N + N_S. \tag{3.2}$$

Спочатку розглянемо процес і результати імітаційного моделювання при впливі синусоїдальної немодульованої завади. Для виконання цих умов коефіцієнт кратності k_{krat} вибирався рівним $2n$, а в конкретному випадку – дорівнював 16-ти.

Формування адитивного шуму виконувалося з використанням вбудованої функції Mathcad. Сума векторів послідовності відеоімпульсів (Рисунок 3.1), адитивного шуму зі середньоквадратичним відхиленням (СКВ) рівним 0,1 і періодичної завади з амплітудою рівною 5-ти показана на рисунку 3.2.

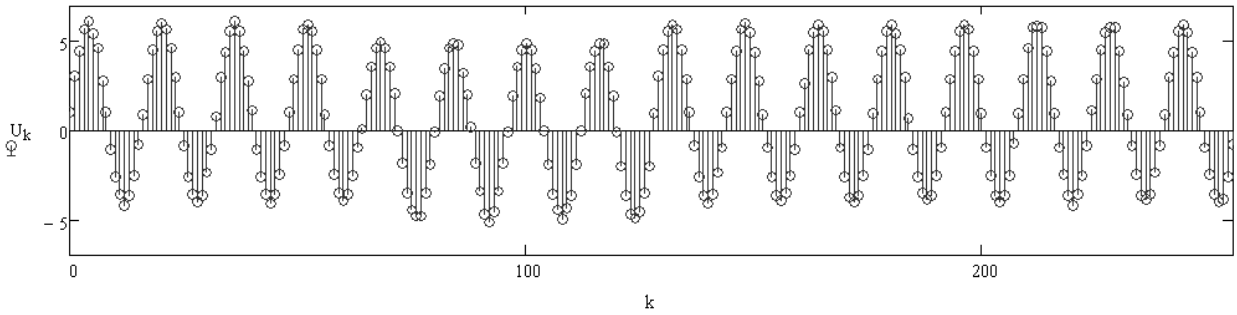


Рисунок 3.2 - Суміш інформаційного сигналу, адитивного шуму та періодичної завади

Після перетворення з часової в частотну область вектору U за допомогою процедури ДПФ, проводилося його порівняння з еталонними спектрами ДПФ усіх можливих 16-ти комбінацій послідовностей із 4-ох відеоімпульсів. Еталони ДПФ комбінацій були обчислені заздалегідь і при проведенні розрахунків зчитувалися за допомогою стандартних функцій Mathcad з файлів «*.prn» на жорсткому диску. Так, на рис. 3.3 представлений спектр суміші сигналу та адитивного шуму, отриманий за допомогою процедури дискретного перетворення Фур'є (ДПФ). На рисунку 3.4 показане ДПФ суміші сигналу адитивного шуму та періодичної завади.

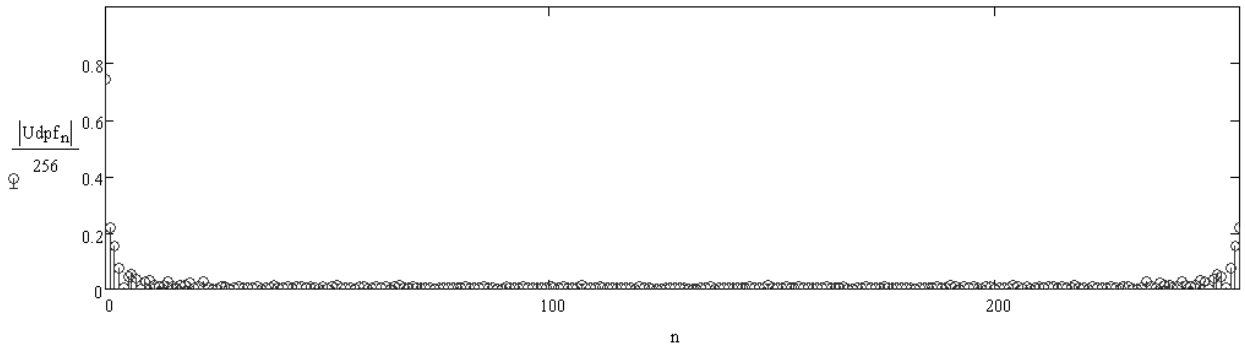


Рисунок 3.3 - Спектр інформаційного сигналу й адитивного шуму

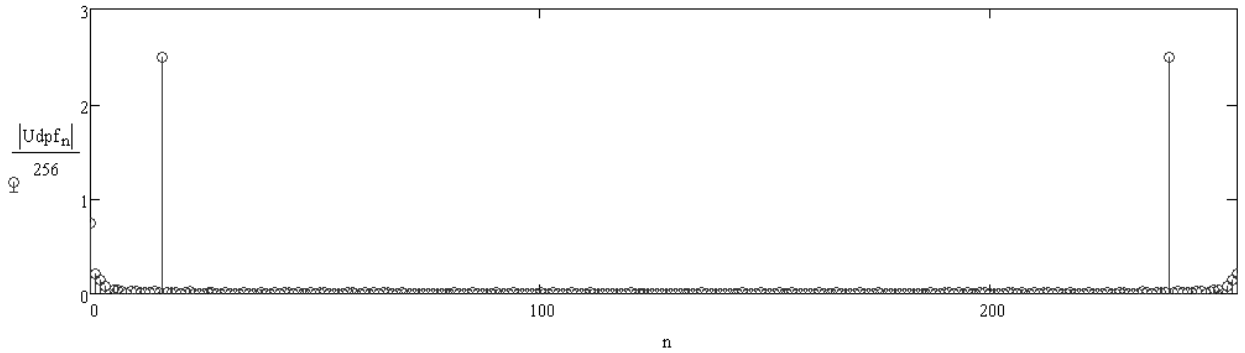


Рисунок 3.4 - Спектр інформаційного сигналу, адитивного шуму та періодичної завади

Відновлення вихідної комбінації послідовності W проводилося порівнянням складової ДПФ прийнятого вектору змішаного сигналу, шуму та вузькосмугової завади за методом найменших квадратів (МНК). Лістинг алгоритму обчислення функціонала МНК представлений в ДОДАТКУ Б.

Отриманий результат алгоритму по МНК для 16-ти комбінацій представлений на рис. 3.5.а. Як видне нього, мінімальне значення функціонала МНК відповідає комбінації № 11, що відповідає прийнятому сигналу 1011 у двійковій послідовності. Результат виконання додаткового алгоритму по визначенню номера з мінімальним значенням функціонала у векторі Sravre_1 і виводом його значення показаний на рис. 3.5.б.

З аналізу результатів моделювання (Рисунок 3.5) видно, що сигнал упевнено розпізнається на тлі вузькосмугової завади, амплітуда якої в 5 раз перевищує амплітуду інформаційного сигналу. В ході експерименту імітувалася завада з амп-

літудою більшою в десятки та навіть сотні раз. При цьому сигнал був упевнено розпізнаний.

Таким чином, при застосуванні МНК одиночний спектральний викид незалежно від його амплітуди, практично не впливав на кінцевий результат.

round(SravRe_1, 1) =

	0
0	$4.013 \cdot 10^4$
1	$1.621 \cdot 10^4$
2	$3.214 \cdot 10^4$
3	$8.23 \cdot 10^3$
4	$3.226 \cdot 10^4$
5	$8.598 \cdot 10^3$
6	$4.04 \cdot 10^4$
7	$1.674 \cdot 10^4$
8	$1.609 \cdot 10^4$
9	$8.307 \cdot 10^3$
10	$8.109 \cdot 10^3$
11	323.7
12	$8.221 \cdot 10^3$
13	691.7
14	$1.637 \cdot 10^4$
15	$8.836 \cdot 10^3$

а)

$$SravNomRe\_1 = \begin{pmatrix} 323.744 \\ 11 \end{pmatrix}$$

б)

Рисунок 3.5 - Результати виконання алгоритму по МНК

Тепер розглянемо процес і результати імітаційного моделювання при впливі синусоїдальної модульованої завади. Для того щоб одержати імітацію модульованої завади була використана властивість ДПФ, що обумовлена початковими умовами та обмеженнями цієї процедури, а саме:

– спостереження за сигналом проводиться в обмеженому інтервалі часу;
– за межами цього інтервалу часу сигнал нескінченно повторюється.

Враховуючи зазначені властивості, для того щоб одержати модульовану заваду коефіцієнт кратності k_{krat} був узятий нерівним $2n$, а саме $k_{krat} = 15{,}5$. Внаслідок цього, функція Ns на інтервалі спостереження уклалася в нецілe число періодів, що ілюструється рис. 3.6. Завдяки другій із зазначених властивостей ДПФ, у результаті періодичного повторення цієї функції за межами інтервалу спостереження була отримана фазоманіпульована завада із частотою фазових стрибків в 4 рази меншою чим частота проходження інформаційних імпульсів. Спектр сигналу

та завади показаний на рис. 3.7. Порівнюючи рисунки 3.3 і 3.7 можна помітити, що завада на рисунку 3.7 придбала додаткові складові, які спотворили частину спектра корисного сигналу.

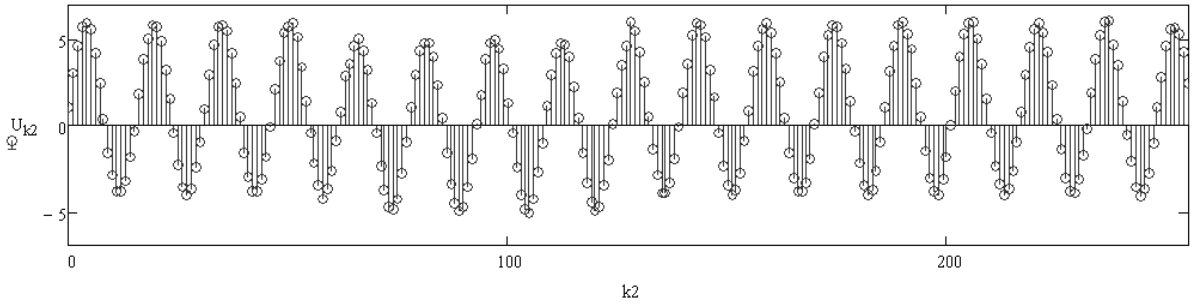


Рисунок 3.6 - Суміш інформаційного сигналу, адитивного шуму та періодичної завади при $k_{krat} = 15{,}5$

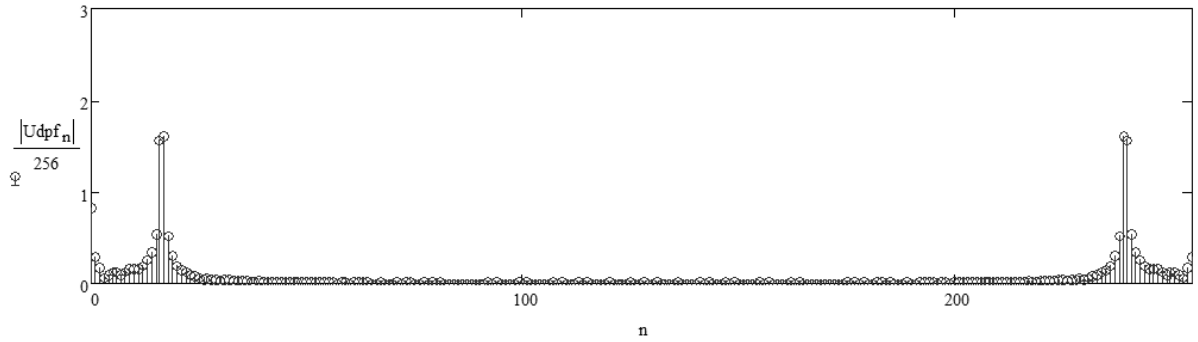


Рисунок 3.7 - Спектр інформаційного сигналу, адитивного шуму та фазоманіпульованої завади

На рисунку 3.8 представлені результати виконання алгоритму по МНК у випадкові впливу фазоманіпульованої завади. З аналізу результатів випливає:

– сигнал розпізнаний правильно при тому, що амплітуда завади 5-кратно перевищувала амплітуду сигналу;

– мінімум, що визначає детектируючий сигнал (рядок 11 рисунку 3.8.а) значно більше мінімуму в тому ж рядку рисунку 3.5.а, що свідчить про меншу завадостійкість методу в умовах впливу фазоманіпульованої завади.

Враховуючи, що в реальних умовах немодульована синусоїдальна завада зустрічається досить не часто, а її частота та кількість цілих періодів у вибірці будуть випадковими, то на практиці більш затребуване буде вирішення завдання виділення сигналу на тлі модульованої завади. Однак у тих випадках, коли в ролі за-

вади будуть виступати наведення електромережі, то, використовуючи методи адаптації, можна розраховувати на результати такі як при впливі немодульованої завади.

round(SravRe_1, 1) =

	0
0	$8.642 \cdot 10^5$
1	$8.378 \cdot 10^5$
2	$8.51 \cdot 10^5$
3	$8.246 \cdot 10^5$
4	$8.519 \cdot 10^5$
5	$8.258 \cdot 10^5$
6	$8.549 \cdot 10^5$
7	$8.287 \cdot 10^5$
8	$8.394 \cdot 10^5$
9	$8.291 \cdot 10^5$
10	$8.262 \cdot 10^5$
11	$8.159 \cdot 10^5$
12	$8.271 \cdot 10^5$
13	$8.171 \cdot 10^5$
14	$8.3 \cdot 10^5$
15	$8.2 \cdot 10^5$

а)

$$SravNomRe\_1 = \begin{pmatrix} 8.159 \times 10^5 \\ 11 \end{pmatrix}$$

б)

Рисунок 3.8 - Результати виконання алгоритму по МНК у випадкові впливу фазоманіпульованої завади

Таким чином, у роботі проведене імітаційне моделювання методу спектрального детектування сигналу в умовах впливу вузькосмугової завади, а також при впливі білого гаусовського шуму із порівняно невеликим значенням СКВ. Результати моделювання свідчать про працездатність запропонованого методу. Слід помітити, що при моделюванні не використовувалися додаткові методи обробки сигналів.

3.2. Технічні аспекти практичного застосування WSN Zigbee

Типова структура мережі Zigbee представлена на рисунку 3.9. При цьому, можна виділити найбільше часто підтримувані топології мережі: зірка, кластерна та коміркова (Рисунок 3.10). На даний час, існують 3 різні типи пристроїв Zigbee.

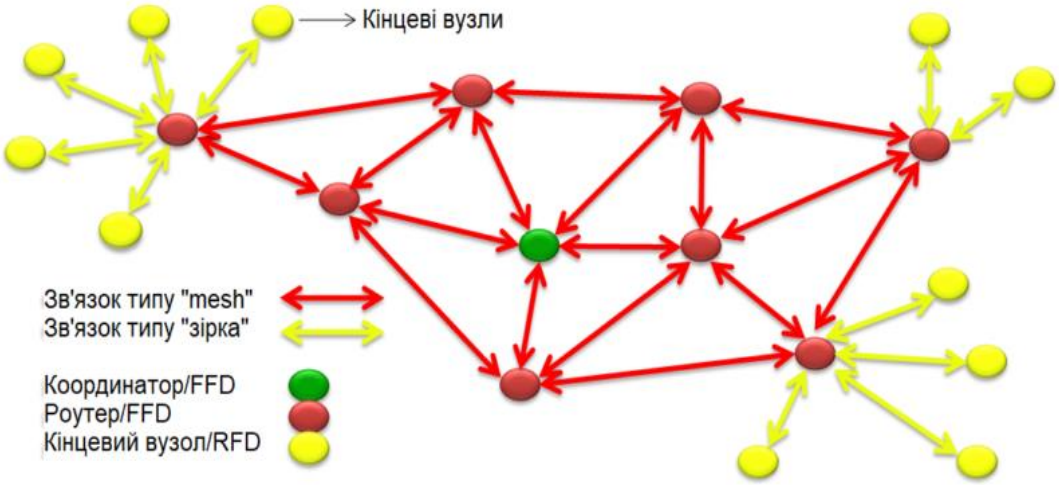


Рисунок 3.9 - Типова структура мережі Zigbee

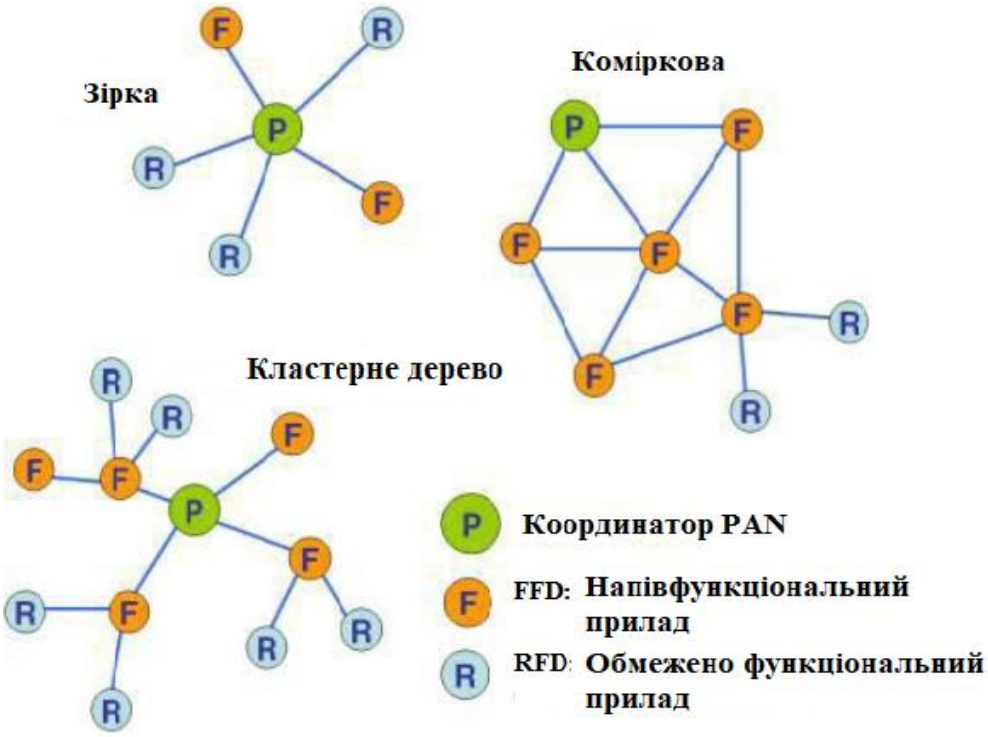


Рисунок 3.10 - Топології Zigbee

1. Координатор Zigbee (ZC) – формує шляхи древа мережі та зв’язується з іншими мережами. У кожній мережі є тільки один координатор. Координатор запускає мережу від початку. Він зберігає інформацію про мережу, зберігає ключі безпеки і являється довіреним центром. Координатор відповідає за безпеку мере-

жі, дає дозвіл чи забороняє підключатися новим пристроям до мережі. При появі перешкод в ефірі перестроює процес перекладу пристроїв в мережі на інший.

2. Маршрутизатор Zigbee (ZR) – маршрутизатор може бути проміжним маршрутизатором, передаючи дані з інших пристроїв. ZR може запускати функцію додатка. Він постійно в роботі мережі. ZC також є маршрутизатором. ZR постійно підтримують таблиці маршрутизації для прокладки раціонального маршруту і пошуку нового, якщо пристрій вийшов з ладу. Приклад, ZR-ом в мережі ZigBee може бути розумна розетка, блоки управління освітлювальними приладами або інший пристрій, який під'єднаний до електроживлення.

3. Кінцевий пристрій Zigbee (ZED) – обмінюється інформацією з материнським вузлом або координатором ZC, або з маршрутизатором ZR він не передає дані з інших пристроїв. Тому вузол ZED більшість часу перебуває в «сплячому стані», цим він збільшує термін енергоживлення. Для ZED потрібно мінімум пам'яті чим здешавшується його виробництво.[17]

У топології зірка, де ZC Zigbee відповідає за ініціювання та підтримку пристроїв у мережі, інші пристрої безпосередньо спілкуються з координатором. Ця топологія підходить для мереж із централізованим пристроєм і додатків критичних до часу.

У кластерному дереві ZC як і раніше відповідає за мережу та технічне обслуговування; однак, ZR можуть бути використані для розширення мережі. ZR управляють потоками даних за допомогою ієрархічної стратегії маршрутизації в мережі.

У комірковій мережі ZC відповідальні за запуск мережі та при виборі певних ключових параметрів мережі, однак мережа може бути розширена за рахунок використання ZR. ZR можуть бути використані для розширення мережі.

Коміркова мережа дозволяє створити повністю однорангови зв'язки. Якщо вузол не доступний, тоді інший маршрут використовується для доставки даних.

Вільна концепція Zigbee і оптимізація його роботи залучає все нових розробників. Це значить, що розумний будинок під цей стандарт варто розглядати й у якості власного проекту. Серед них такі проекти як: Xiaomismarthome, Wulian,

Legrand. Так само, набори модулів Xbee Zigbee Mesh, дозволяють створювати власні смарт-пристрої, узгоджуючи з Zigbee мікроконтролери та плати. Тільки в 2016 р., про співробітництво з Альянсом оголосили такі компанії як Phillips, Digi International, Enerbee, Greenpeak Technologies, Jiuzhou Greeble: MMB Networks, Murata і Ubisys.

Модулі ZCL використовують профілі, які зв'язують бездротові пристрої різних компаній і екосистем. Ці спеціалізовані елементи мережі об'єднані в «публічні профілі» (наприклад, «Homeautomation»), але ще доступні профілі для організації мережі в лікарнях, на будівництві або заводах. Оскільки вихідний код у системи відкритий: доступний через проект ZBOSS, у сторонніх розробників спостерігається зустрічний процес стандартизації. Так, наприклад, модулі компанії Atmel сумісні з Zigbee за замовчуванням.

3.3. Приклад реалізації розумного дому на основі Zigbee

Надалі доцільно розглянути деякі елементи розумного дому з Zigbee.

Хаб – головний пристрій, центр керування та контролю. Ухвалює команди людини, а потім пересилає їхнім пристроям з підходящої до запиту спеціалізацією. Спосіб спілкування розумного будинку й людину залежить від форм-фактора хаба. У його стандартних реалізаціях ви використовуєте тільки додатки на ПК і смартфоне, а от розумні колонки Google Home або Amazon Echosовмещают хаб із вбудованим мікрофоном і динаміком для голосового керування.

У розумних колонках, Google, Amazon або Cubic використовують власних голосових помічників. Оскільки розроблювач хаба обмежує вибір сумісних пристроїв рамками умовної «екосистемы», вам доведеться завести обновлюваний чек-аркуш компаній, чиї пристрої сертифіковані з вашим хабом.

Екосистема розумного будинку – модель сумісності, в основі якої лежать не стільки технологічні стандарти, скільки домовленості між творцями хаба й пристроїв розумного будинку. Це значить, що смарт-чайник Xiaomi Kettle не підключиться до екосистеме Google Home, хоча, напевно, міг би.

Великі гравці як Google або Xiaomi здатні одночасно випускати й хаб і сумісну з ним лінійку розумних побутових приладів. Так відбувається тому, що поки технологія нова й ринок не встоявся, кожний прагне зробити свою екосистему загальноприйнятим стандартом.

Втім, майданчик Google Home відкритий для більшості розроблювачів і вже підтримує такі комплексні продукти, як смарт-система опалення Honeywell. Навіть закрите середовище Applehome Kit сертифікована з лампочками Phillips Hue.

Планувальники екосистем залучають продукти розроблювачів з боку, тому що завдання того ж домашнього опалення або висвітлення перебувають в обастях, далеких від спеціалізації компанії. Коротко – котельні від Google коштували б занадто дорого.

Датчики – пристрої для прямого, автоматичного й вилученого контролю над станом будинку: температура, вологість повітря, висвітлення, задимленість і незаконне проникнення перебувають у віданні датчиків. Коли потрібне участь людини, вони розсилають повідомлення через Wi-Fi або GSM-мережа, але в штатному режимі автоматично підтримують установлені користувачем параметри. Наприклад, смарт-системи опалення (термостати) регулюють температуру в будинку за графіком. Коли мешканці йдуть на роботу, температура в будинку знижується для економії тепла, а до закінчення робочого дня опалення знову заробить інтенсивніше. Якщо ви збираєтеся додому раніше, те віддалено запускаєте підігрів будинку зі смартфона. З Honeywell, ви взагалі можете просто попросити асистента Google підняти температуру.

Iot – у рамках розумного будинку, це мережа побутових приладів, гаджетов і подібних пристроїв, які зв’язуються з хабом по Wi-Fi через хмарний сервер. Ви управляєте всією цією мережею з одного додатка на смартфоне, ПК або голосом через розумного помічника. Пристрій, несумісний з хабом, зможе управлятися тільки через окремий додаток. Для прикладу, надалі наведений список сумісних датчиків і пристроїв екосистеми Xiaomi Smart Home (Таблиця 3.1).

1. Smart-освітлення: Smart-лампи Xiaomi Yeelight Blue і Xiaomi Yeelight

LED; Smart-світильник Xiaomi Yeelight Lamp; Світильник Rui Chi Philips Lamp; Настільна лампа Xiaomi Philips Eyecare Smart Lamp 2; Smart-стрічка з LED-світлодіодами Xiaomi Yeelight LED strip.

Таблиця 3.1 - Елементи екосистеми розумного будинку Xiaomi Smart Home

 Контролер Xiaomi Magic Cube White – 499 грн.	 Mi Smart socket 2 ZigBee Version – 499 грн.	 Універсальний пульт Mi Smart Home Universal Remote Controller – 649 грн.
 Розумний монітор сну Lunar Smart Sleep Sensor – 499 грн.	 Контролер Xiaomi Magic Cube Blue – 444 грн.	 Бездротовий комутатор Mi Smart Home Wireless Switch – 349 грн.
 Фумігатор Xiaomi Mi Portable Electronic Mosquito Repeller Gray – 349 грн.	 Розумна розетка Mi Smart socket – 444 грн.	 Розумна розетка Xiaomi Innolinks Smart socket – 799 грн.
 Комплект вимикачів світла Aqara smart light control set – 1298 грн.		 Набір Mi Smart Home Set – 2399 грн.

2. Кліматичне обладнання: очисники повітря Mi Air Purifier (2); зволожувач повітря Xiaomi Air Humidifier; водяні Smart-фільтри Mi Water (2); Smart-кондиціонер Mi-youth Smart Air Conditioner; Smart-вентилятор Xiaomi Mi Smart Fan.

3. Smart-ТВ: телевізори Xiaomi Mitv; Android Smart-ТВ приставки Mi Box TV (Mi Box 3 Pro, Mi Box TV mini); універсальний пульт ДК IR Remote Controller.

4. Електрика: Smart-розетка Mi Smart Power Plug; Smart-подовжувач електричний Xiaomi SMART Power Strip; автомобільне зарядне із вбудованим Bluetooth і FM-трансмитером Xiaomi Roidmi.

5. Відеокамери: домашня камера Xiaomi YI Home Camera; Smart-камери Xiaomi Mi White Smart Camera і Xiaofang Smart Camera; Smart-годинник Xiaomi Mi Alarm Clock.

6. Wi-Fi: роутеры Xiaomi Miwi-fi; підсилювач сигналу Wi-Fi Xiaomi Wi-Fi Amplifier

7. Решта: квадрокоптер Xiaomi Mi Drone; скутер Xiaomi Ninebot Mini; Smart-чайник Xiaomi Kettle; Хаб Xiaomi Mi Cube; Smart-машина пральна Kokichi Smart Mini; робот-Пилосос Xiaomi Mi Robot Vacuum; домашні ваги Xiaomi Smartscale; дитячий Smart-годинник із трекером Xiaomi Mimi Rabit Watch. [23]

Подальший розвиток концепції розумного будинку орієнтований на впровадження хмарного голосового помічника, який налаштовується під конкретного користувача та конфігурується з ростом можливостей штучного інтелекту.

В інтересах промисловості продукцію Zigbee пропонують компанії: NXP Semiconductors, Panasonic, ST Microelectronics, Uniband Electronic Corporation (UBEC).

Висновок

З метою підтвердження працездатності методу спектрального детектування сигналу в умовах впливу вузькосмугової завади було проведено його математичне моделювання в пакеті Mathcad. Дослідження були проведені для 2-ох варіантів ву-

зькосмугової завади: синусоїдальна немодульована завада; вузькосмуговий фазоманіпульований сигнал зі швидкістю маніпуляції в 4 рази меншої швидкості детектованого сигналу. Результати свідчать про працездатність запропонованого методу.

Вільна концепція Zigbee і оптимізація його роботи залучає всі нових розробників. Це значить, що розумний будинок під цей стандарт варто розглядати й у якості власного проекту. Серед них такі проекти як: Xiaomismarthome, Wulian, Legrand. Так само, набори модулів Xbee Zigbee Mesh, дозволяють створювати власні смарт-пристрої, узгоджуючи з Zigbee мікроконтролери та плати. Тільки в 2016 р., про співробітництво з Альянсом оголосили такі компанії як Phillips, Digi International, Enerbee, Greenpeak Technologies, Jiuzhou Greeble: MMB Networks, Murata і Ubisys.

В якості прикладу реалізації розумного дому на основі Zigbee розглянуто екосистему Xiaomi Smart Home, яка дозволяє задіяти понад 45-ть типів різновидів пристроїв.

ВИСНОВКИ

Актуальність досліджень WSN очевидна. Уже зараз у багатьох галузях їх використовують. Це й моніторинг екології, автотрафіка, погоди та ін. З удосконалюванням технологій та різних виробництв, потреба в WSN зростатиме. Основними завданнями WSN є: періодично вимір показника (і обчислення); детектування події; вимірювання показника за запитом.

До найбільш поширених варіантів схемо-технічних рішень WSN слід віднести: DASH7, Z-Wave, Insteon, Enocean, ISA100.11a, Wirelesshart, Miwi, 6Lowpan, One-Net, Wavenis, Rubee, Zigbee (Pro).

На жаль, використання CSMA/CA як базовим режимом доступу не гарантує втрат багатьох пакетів в результаті колізії. Експерименти з вузлами сенсорної мережі стандарту 802.15.4 показали, що значна кількість колізій відбувається коли губляться пакети тільки від вузлів з більш слабким сигналом. Вузли з більш сильним сигналом немають таких колізій.

В свою чергу, в радіодіапазоні 2,4 ГГц втрачатися пакети можуть до 90%, в залежності від якості трафіка. Це спонукає до застосування спеціальних алгоритмів виявлення завад від мереж стандарту Wi-Fi.

Вході досліджень встановлено, що для каналів зв’язку WSN властиві наступні ефекти та явища: нестабільність каналів, несиметричність каналів, варіації рівня потужності сигналу, непередбачуваність.

Вони мають сильний вплив на роботу всієї мережі в цілому (втрата зв’язку, зниження зв’язності мережі, помилки в локалізації та ін.), а саме головне – впливають на протоколи верхніх рівнів.

Таким чином, можливо сформувати наступні вимоги до WSN.

1. Стійкість до активних радіозавад.

2. Виявлення підміни вузлів.

3. Наявність резервних маршрутів передачі даних.

4. Виявлення та запобігання спробам реконфігурації мережі, підміни адресної інформації, несанкціонованої «перепрошивки» пристроїв,

5. Стійкість до викривлення та фільтрації кадрів.

На даний час, в якості пріоритетних шляхів оптимізації WSN на рівні системи передачі даних слід вказати про використання завадостійкого кодування, сигнально-кодових конструкцій, багатопозиційних сигналів або їх комбінацій. Такий підхід достатньо обґрунтований в існуючій множині публікацій.

В досить перспективних WSN, до яких слід віднести ZigBee і Thread, використовуються трансивери з FSK або GFSK.

В свою чергу, заслуговують уваги напрямки, що спираються на впровадження інноваційних технологій, які отримали значне поширення в більше розвинутих мережах, наприклад: 8021.11ac(ax), 5G, MU-MIMO, Massive MIMO та ін.

В ході досліджень запропоновано використання кількох варіантів формування багатопозиційних сигналів для радіоканалів WSN. Замість одиничного сигналу FSK (GFSK) застосовується OFDM сигнал. Швидкість передачі даних сигналу, рівна швидкості субканалу, що менше в кілька раз від сигналу для WSN на основі FSK (GFSK). Збільшення енергетики може відбуватись за рахунок введення надмірності (дубльовані канали) та переваг обробки на приймальній стороні сигналів OFDM.

При цьому, з’явилась можливість вибору між завадостійкістю та спектральною ефективністю радіоканалу WSN. Варто мати на увазі, що до наведених пропозицій не включена існуюча номенклатура модифікацій N-OFDM.

Підвищити завадостійкість WSN можливо також за рахунок удосконалення процедур детектування сигналів.

Запропонований метод обробки сигналів, на відміну від відомих методів спектральної фільтрації не призводить до збільшення загальної кількості переданих символів, а виконується проведенням аналізу спектрального складу прийнятого сигналу. Даний метод, можливо, використовувати як самостійно так і з методами безперервного кодування з виправленням помилок.

З метою підтвердження працездатності методу спектрального детектування сигналу в умовах впливу вузькосмугової завади було проведено його імітаційне моделювання в пакеті Mathcad. Дослідження були проведені для 2-ох варіантів ву-

зькосмугової завади: синусоїдальна немодульована завада; вузькосмуговий фазоманіпульований сигнал зі швидкістю маніпуляції в 4 рази меншої швидкості детектованого сигналу. Результати свідчать про працездатність запропонованого методу.

Таким чином, результатами дипломної роботи є: пропозиції щодо використання багатопозиційних сигналів у сенсорних мережах; результати імітаційного моделювання методу спектрального детектування сигналу в умовах впливу вузькосмугової завади. Все це може бути використане для подальших досліджень та при побудові перспективних сенсорних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Razaque, A., Elleithy, K., & Al-Maadeed, S. (2019). Бездротові сенсорні мережі: Еволюційні алгоритми та методи оптимізації для ефективної розробки протоколів. Журнал мережевих та комп'ютерних додатків, с. 53-71, 126

2. Ель-Хадж, М., & Артайл, Х. (2019). Комплексне дослідження технології ZigBee: Застосування, виклики та рішення. Журнал мережевих та комп'ютерних додатків, с. 1-23, 126.

3. "Бездротові сенсорні мережі: Огляд останніх розробок та потенційної синергії". IEEE Communications Surveys & Tutorials. 2019.

4. Khan, M. A., & Madani, S. A. (2019). Комплексний огляд бездротових сенсорних мереж та їх застосування в галузі охорони здоров'я. Журнал мережевих та комп'ютерних додатків, с. 24-52, 126.

5. Слюсар В.І. Метод неортогональної дискретної частотної модуляції сигналів для вузкосмугових каналів зв’язку. / Слюсар В.І., Смоляр В.Г. // Радіоелектроніка.–2004.–Том 47, №4. с. 53-59.

6. Слюсар Д. Бездротові мережі на кристалі – перспективні ідеї та методи реалізації. / Слюсар Д., Слюсар В. //Електроніка: наука, технологія, бізнес. – 2011. – № 6. – с. 74-83.

7. Слюсар В.І. Неортогональне частотне мультиплексування (N-OFDM) сигналів. Частина 1. / Слюсар В.І. // Технології та засоби зв’язку. – 2013. – № 5. – с. 61-65.

8. Слюсар В.І. Неортогональне частотне мультиплексування (N-OFDM) сигналів. Частина 2. / Слюсар В.І. // Технології та засоби зв’язку. – 2013. – № 6. – с. 60-65.

9. Чунг-Чі Лі. Бездротова мережа датчиків та управління ZigBee. 2020.

10. Калачов А. 6LOWPAN VS. ZIGBEE [Електронний ресурс] / Калачов А. – Режим доступу: https://r-iot.org/2016/05/15/6lowpan-vs-zigbee/.

11. Смоляр В.Г. Спектральна фільтрація з кореляційною демодуляцією сигналу. / Смоляр В.Г., Тишко С.А., Слюсар І.І. // Системи управління, навігації та зв’язку. – Центральний науково-дослідний інститут навігації та управління, 2011. – с. 268-271.

12. Мулярчик К.С. Захист каналів комунікації в безпроводових сенсорних мережах

і системах телеметрії. [Електронний ресурс]/ Мулярчик К.С. // IM&CTCPA-2016. – Режим доступу: http://comsec.spb.ru/imctcpa16/02. 03.MulyarchikKS.pdf.

13. Офіційний сайт MathCad [Електронний ресурс]. – Режим доступу: http://www.mathcad.com.

14. Жук О.В. Аналіз методів управління топологією безпроводових сенсорних мереж. ВІТІ. 2017.

15. Горбенко Р. А. Дослідження залежності ефективної пропускної спроможності дискретного каналу зв'язку бездротової сенсорної мережі від ймовірності бітової помилки та довжини кадру даних /Системи обробки інформації. - 2015. - № 8. - с. 114-118.

16. Офіційний сайт SILVUS [Електронний ресурс]. – Режим доступу: http://www.Silvus Technologies.com.

17. Переваги застосування сенсорних мереж [Електронний ресурс]/ITMiBT. – Режим доступу: www.ipmce.ru/img/release/is_sensor.pdf.

18. Петріго В. Безпроводові мережі ZigBee. Частина 1. [Електронний ресурс] / Петріго В. – Режим доступу: https://habrahabr.ru/company/efo/blog/ 281048/.

19. Садков А. Лекція 2. Бездротові канали зв'язку: Моделі, Поведінка, Ефекти. [Електронний ресурс]/ Садков А. Режим доступу: https://alterozoom.com/documents/11099.html.

20. Дрю Гісласон,"Бездротові мережі ZigBee", 2020.

21. Liu, Y., & Wu, J. Огляд протоколів маршрутизації для бездротових сенсорних мереж. Sensors, 2019, 1342.

22. Фінк Л.М. Сигнали. Перешкоди. Помилки... Нотатки про деякі несподіванки, парадокси та помилки в теорії зв'язку / Фінк Л.М. - 2 е вид., Перероб. та дод. - М.: Радіо і зв'язок, 1984. – с. 256.

23. Zigbee [Electronic resource] / Zigbee Alliance. – Last access: www.zigbee.org/.

ДОДАТКИ

ДОДАТОК А

Розділ 1 (Англійська версія)

CHAPTER 1.

CHARACTERISTICS OF WIRELESS SENSOR NETWORKS

1.1. Purpose of sensor networks

The latest wireless communication technologies and progress in the field of microelectronics production have allowed in recent decades to move to the practical development and implementation of a new class of distributed communication systems - sensor networks.

A wireless sensor network (WSN) is a type of wireless network that includes a large number of self-controlled, miniature low-power devices called sensor nodes or motes (from the English motes - dust) (Figure 1.1).

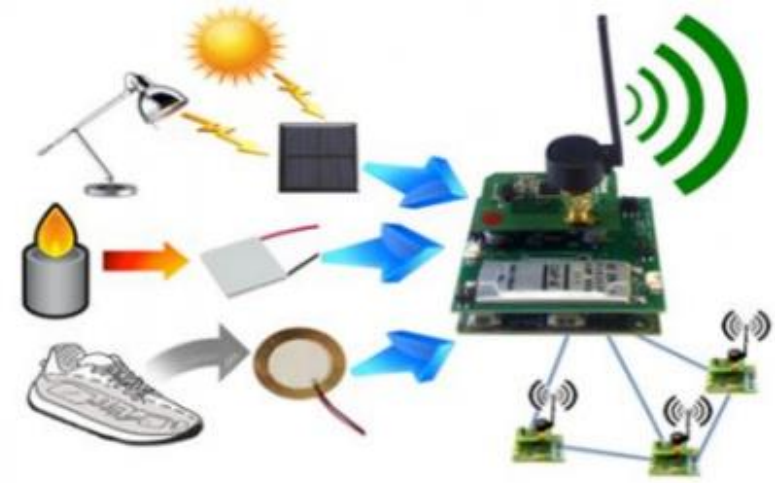


Figure 1.1 - Wireless sensor network

Sensor networks, of course, encompass a huge number of spatially distributed miniature embedded devices operating on battery power, which are combined into a network to collect, process and transmit data to operators, and they control the computing and processing capabilities. Nodes are microcomputers that together form networks. The range of wireless communication depends on the power of the transmitted signal level, and with increasing distance between sensors, the bandwidth of the com-

munication line drops sharply. Since a sensor network involves the use of small autonomous sensors, the signal power level is severely limited, and increasing power leads to a decrease in the autonomous operation time of the sensors and the use of more energy.

Typically, a mote is a board no larger than one cubic inch in size (Figure 1.2). The board contains a processor, memory (RAM and flash), digital-to-analog and analog-to-digital converters (DAC and ADC, respectively), a radio-frequency transceiver, a power supply, and sensors.

Of the rather large number of examples of WSN use, we will highlight two. The most famous is probably the deployment of the network on board an oil tanker by British Petroleum. Using a network built on Intel equipment, the vessel's condition was monitored in order to organize its preventive maintenance.

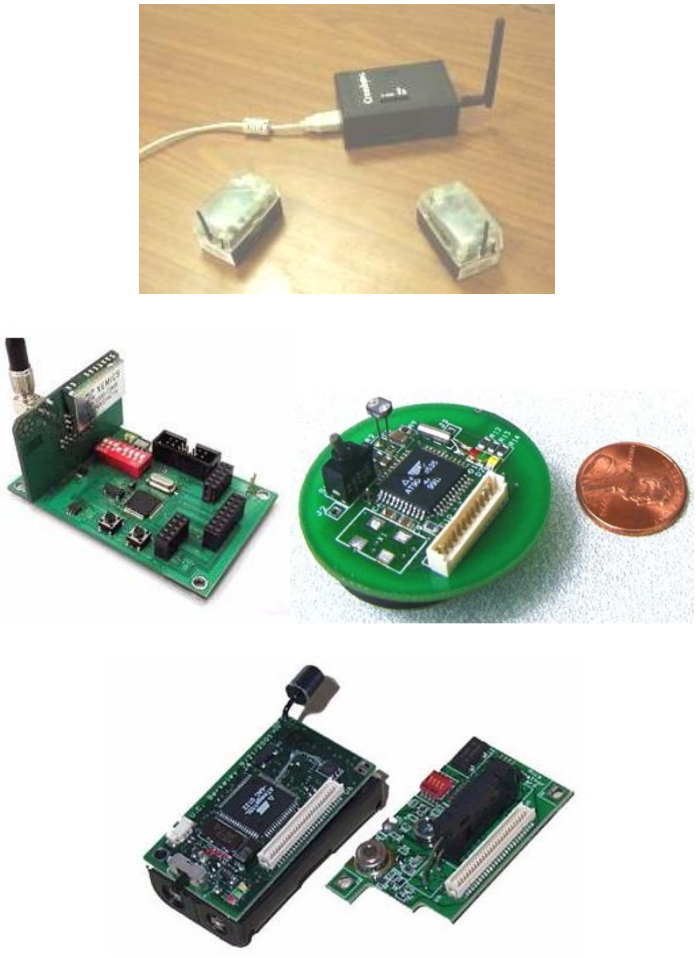


Figure 1.2 - Appearance of the motes

British Petroleum analyzed whether the sensor network could operate on board the vessel in conditions of extreme temperatures, high vibration, and a significant level of radio frequency interference present in some of the vessel's rooms. The experiment was successful, with the network automatically reconfiguring and restoring its operability several times.

Another example of a pilot project implemented is the deployment of a sensor network at the US Air Force (Air Force) base in Florida. The system demonstrated good capabilities for recognizing various metal objects, including moving ones. The use of the sensor network made it possible to detect the penetration of people and cars into the controlled area and track their movements. To solve these problems, motes equipped with magnetoelectric and temperature sensors were used. The corresponding application software (SW) is being developed by several American universities.

Delta is a national military situational awareness system used by the Security and Defense Forces of Ukraine; built according to NATO standards. Delta is an online system that provides real-time information about the tactical and operational situation on the battlefield. Thanks to Delta, soldiers see the battlefield with the location of enemy forces online. Data from aerial reconnaissance, satellites, drones, stationary cameras, radars, chats, etc. is pulled up to the platform. Delta is an important component when planning military operations.

WSNs are used in many industries. However, before implementing networks, they must be thoroughly tested, which is why research in this area is needed.

At present, the main advantages of WSNs include:

- complete absence of cables;

- the possibility of compact placement or even integration of motes into environmental objects;

- reliability of both individual elements and, more importantly, the entire system as a whole; in some cases, the network can function with only 10÷20% of sensors (motes) in working order;

- no need for personnel for installation and maintenance.

In general, it is possible to distinguish the following main areas of application of this technology:

- security and safety systems;
- environmental control;
- industrial equipment monitoring;
- security systems;
- monitoring of the condition of agricultural land;
- energy supply management;
- control of ventilation, air conditioning and lighting systems;
- fire alarm;
- warehouse accounting;
- enemy observation on the battlefield;
- cargo transportation observation;
- monitoring of the physiological state of a person;
- personnel control.

Each network node includes: a mote, which is equipped with a radio transceiver or other wireless communication device, a small microcontroller and a power source. It is possible to use solar lighting batteries or other alternative energy sources.

Data from remote elements is transmitted over the network between the nearest nodes via a radio channel. As a result, a data packet is transmitted from the nearest moto to the gateway. The gateway is usually connected to the server by a USB cable. The collected data is processed, stored on the server and can be accessed via a WEB interface to a wide range of users.

The hardware of the wireless node and the network interaction protocols between the nodes are optimized for energy consumption to ensure a long service life of the system with autonomous power sources. Depending on the operating mode, the node life can reach several years. A typical structural diagram of a moto with

autonomous power supply is shown in Figure 1.3. Typically, piezo-resistive and tensor-resistive sensors are used.

1.2. Architecture and working principle of WSN

Nodes are usually randomly located throughout the observation area (Figure 1.4). Each of them can use the data collection and knows the route of data transmission back to the central node or the end-user device via the shortest route. Data is transmitted using a multipath network architecture.

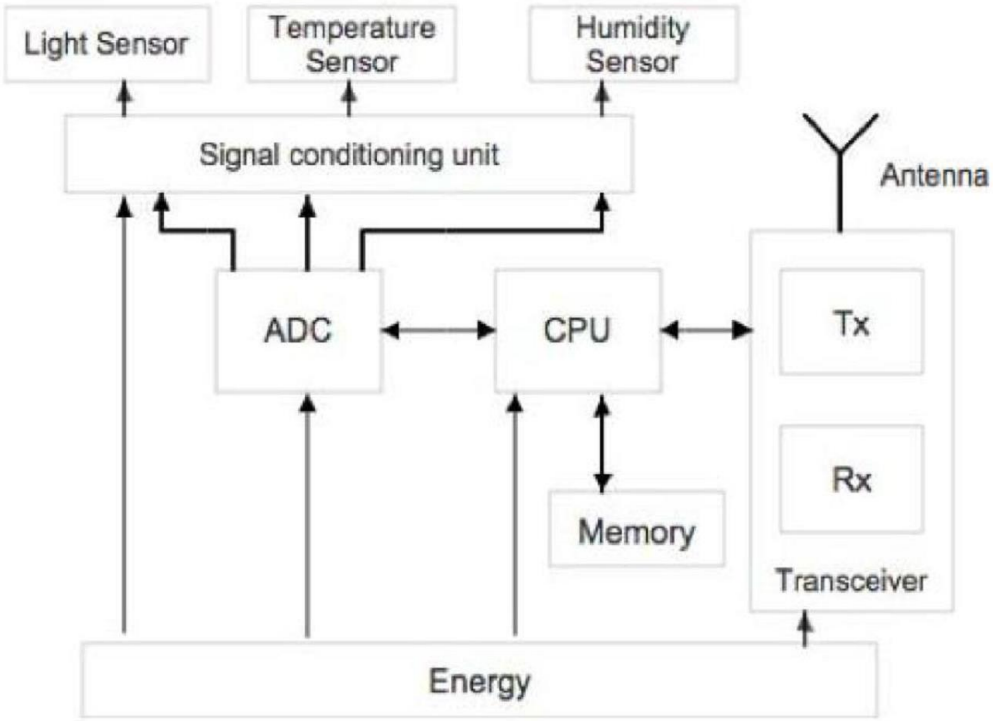


Figure 1.3 - Composition of a WSN node

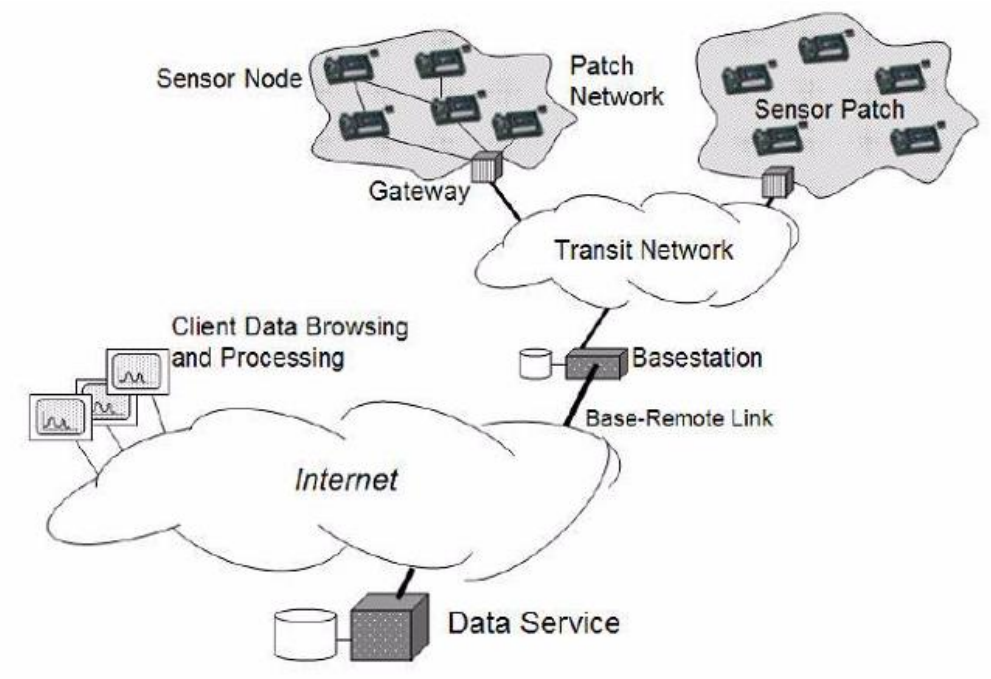


Figure 1.4 - WSN architecture

The protocol stack contains information about power and routes, data about network protocols and communicate effectively using the wireless medium, and thanks to the cooperation of nodes. The protocol stack consists of: application layer, transport layer, network layer, link layer, physical layer, power management area, mobility management and task scheduling (Figure 1.5).

Depending on the data collection tasks, other types of software can be built on the application layers.

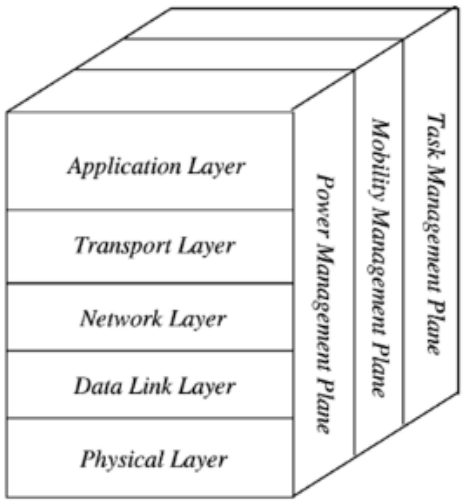


Figure 1.5 - Protocol Stack

The transport layer provides the means for data transmission over a network.

The network layer provides the routing of traffic provided by the transport layer. If the medium is noisy and nodes may move, the medium access control (MAC) protocol must minimize the occurrence of collisions between neighboring nodes.

The physical layer carries physical signals from the source to the receiver. These protocols help nodes perform tasks while saving power.

The three cross-layers include the following:

1. Power management plane.
2. Mobility management plane.
3. Task management plane.

The power management plane decides how a node should use power. For example, a node can turn off its receiver after receiving a message from one of its neighbors. This helps avoid message duplication. Additionally, when a node has a low battery, it tells its neighbors that it cannot participate in message routing. All the remaining energy will be used for data collection. The mobility control area (MAC) creates and registers the movement of nodes. As a result, there is always a route for data transmission to the central node, and nodes can determine their neighbors. Knowing their neighbors, a node can balance the energy consumption, working together with them. The task management area plans and sets the schedules for collecting information for each region separately.

It is worth considering that not all nodes in one region are needed to perform sensing tasks at the same time. Accordingly, some nodes provide more tasks than others. This depends on their power. All these areas and modules ensure that nodes work together and strive for maximum energy efficiency, optimize the data transmission route in the network, and also share resources with each other. Without them, each node will work individually. From the point of view of a sensor network, the most effective case is when nodes work together with each other, which contributes to the extension of the lifetime of the network itself.

Summarizing information about WSN, for the OSI model, the following protocols can be distinguished.

1. Application layer – Modbus TCP, IEC 60870-5, MQTT.

2. Network layer (NWK) – Directed Diffusion, Rumor, LEACH, TEEN, APTEEN, SPEED, 6LoWPAN.

3. Channel layer (MAC) – S-MAC, T-MAC, SS-TDMA, ZigBeeMAC, etc.

4. Physical layer (PHY) – ISM Band (433, 868 MHz – Europe, 902÷928 MHz – America, 2.4÷2.4835 GHz – worldwide).

Thus, the main tasks of WSN include:

- cyclic measurement of the indicator;

- event detection;

- measurement of the indicator on request.

1.3. Analysis of the WSN nomenclature

The most advanced variants of WSN circuit solutions:

DASH7 is a WSN standard that uses a 433 MHz signal frequency in the unlicensed frequency range. When transmitting data over a distance of up to 2 km, a speed of 200 kbit/s is provided. DASH7 technology is open and represents serious competition to patented WSN technologies such as Zigbee or Z-Wave.

Z-Wave is a wireless radio communication technology used to organize sensor networks. The main purpose of the Z-Wave network is remote control of household appliances and free home devices that provide control of lighting, heating and other devices for the automation of management of residential buildings and office premises. Z-Wave technology provides data transmission over a distance of up to 30 m in line-of-sight conditions at a speed of 9.6 or 40 kbit/s, at frequencies of 908.42 MHz in the USA, 868.42 MHz in Europe, etc. Due to the fact that in home and office conditions it is impossible to ensure that all sensors in the network are in line-of-sight to each other, in the Z-Wave standard each node or device can relay a given other node. Thus, if it is necessary to transmit data from a node that is out of sight, this can be done through a chain of nodes. At the same time, Z-Wave networks have elements of self-organization

depending on external factors. For example, when requests arise between the two nearest network nodes, the signal will be automatically transmitted through a chain of other network nodes.

Insteon is a combined (partially wired and wireless) sensor network. To transmit information, a radio signal at a frequency of 902÷924 MHz is used, which provides data transmission over a distance of up to 45 m in line of sight conditions with an average speed of 180 bit/s. To transmit information over wires, the electrical wiring of a house or office is used. The use of a combined network ensures its reliability and allows you to avoid problems associated with tasks or overlapping visibility zones when transmitting data over a radio channel. The Insteon sensor network is traditionally used for home or office automation. It originated in the USA, where it was created to replace the X10 sensor network and from where it moved to Europe.

Enocean is a WSN organization technology that uses ultra-miniature sensors with electricity generators, microcontrollers and transceivers. The use of electricity generators and elements with ultra-low power consumption allows the elements of the Enocean network to operate autonomously, practically without power supplies, for a long time. The Enocean network is mainly used for home and office automation. Enocean technology allows data transmission at a frequency of 868 MHz (for Europe, in other countries the frequency may differ due to the fact that it is a licensed frequency) at a speed of 120 kbit/s at a distance of up to 300 m within direct visibility. In rooms this figure is much lower and depends on the materials of the walls and the layout of the house. Each element of the network has its own 32-bit identification number and an exchange protocol that protects neighboring sensors from mutual requests, which allows you to install up to 4 billion devices in close proximity to each other (according to the developers) without mutual interference.

ISA100.11a is a standard for organizing industrial sensor networks, sensors and actuators. For transmission, low-speed wireless communication is used using elements that have low power consumption. Distinctive features of ISA100.11a from other sensor networks are:

- orientation towards industrial use and, accordingly, special requirements for robustness, noise immunity, reliability and security,

- possibility of emulation using ISA100.11a technology of protocols of already existing and proven wired sensor networks and WSN.

Data exchange is created at a frequency in the region of 2.4 GHz and a speed of about 250 kbit/s.

Wirelesshart is a data transfer protocol over a wireless communication line, developed by the HART Communication Foundation for data transfer in the form of HART messages in a wireless environment. HART is a data exchange protocol for interaction with field sensors based on an extended set of simple "request-response" commands transmitted digitally over a 2-wire line. Wirelesshart provides data transfer at a speed of up to 250 kbit/s at a distance of up to 200 m (within direct visibility) at a data transfer frequency in the 2.4 GHz range.

Miwi is a protocol for organizing sensor and personal networks with low data transfer rates over short distances, which is based on the IEEE802.15.4 specification for wireless personal networks. A Miwi-based network can publish up to 1024 nodes, controlled by up to 8 coordinators. Each coordinator can provide interaction with up to 127 nodes. Data transmission is carried out in the 2.4 GHz frequency range (operation in the 868 and 915 MHz frequency ranges with lower speeds is planned) at speeds up to 250 kbit/s.

6Lowpan is a standard that provides interaction of small wireless networks (parts of a network or network sensors) with an IP network using the IPv6 protocol. It is mainly used for organizing network sensors and automation of residential and office premises with the ability to control them via the Internet. However, it can also be used autonomously, as simple wireless network sensors. Data transmission in the 6Lowpan standard implies the use of gigahertz mode and provides a transmission speed of 50 to 200 kbit/s over a distance of up to 800 m. Currently, 6Lowpan is most suitable for the IEEE 802.15.4 standard.

One-Net is an open protocol for organizing WSNs and home automation networks and distributed objects. It allows you to organize networks that include up to

4096 nodes with multiple coordinators and repeaters, which increases the data transmission range. Data transmission is provided at a distance of up to 100 m indoors and up to 500 m outdoors at a data transfer rate of 28.4÷230 kbit/s.

Wavenis is a wireless data transmission technology that uses 433/868/915 MHz frequencies, providing transmission at a distance of up to 1 km outdoors and up to 200 m at a speed of up to 100 kbit/s. Wavenis technology is the choice for organizing personal networks and network sensors. As a result, the ultra-low consumption of transceivers allows them to operate autonomously for up to 15 years from a single battery.

Rubee is a local wireless network, which is mainly used as a sensor network. Magnetic waves are used for data transmission in Rubee, and the transmission is created at a frequency of 131 kHz, which provides a speed of only 1200 bit/s at distances from 1 to 30 m. However, it allows to significantly reduce power consumption and allows network nodes to operate autonomously for several years from a single battery.

The network is used mainly for specific purposes that do not require high speed, but require long-term autonomous operation and reliable, secure communication. The use of LF allows to avoid problems associated with data transmission indoors due to the fact that the signal is not reflected and is not blocked by walls and other objects. The Rubee network in the USA is certified by the Departments of Defense and Energy, and is also recommended for use in high-risk facilities. Next, it is advisable to note Zigbee more, as the most advanced WSN technology.

1.4. Zigbee-based WSN

Zigbee is a standard for a set of high-level communication protocols that selects small, low-power digital transceivers, based on the IEEE 802.15.4-2006 standard for wireless personal area networks. The Zigbee supplementary specification technology, designed with the intention of being simpler and cheaper than other personal area

networks (such as Bluetooth). Zigbee is intended for radio frequency devices where long battery life and secure data transmission in the network are required.

The main feature of Zigbee technology is that it supports not only simple network topologies ("point-to-point", "tree" and "star") with low power consumption, but also a self-organizing and self-healing cellular (mesh) topology with message relaying and routing. . In addition, the ZigBee specification includes the ability to select a routing algorithm according to software requirements and network conditions, a mechanism for standardizing applications - application profiles, a library of standard clusters, endpoints, bindings, a security protection mechanism, and also provides ease of deployment, maintenance and modernization.

The Zigbee Alliance is the body that ensures the publication of Zigbee standards and application profiles, which allows end-user manufacturers to create compatible products. The exact list of application profiles published or in the works:

- home automation;
- energy efficiency (Zigbee Smart Energy 1.0/2.0);
- commercial building automation;
- telecommunications add-ons;
- personal, home and hospital monitoring;
- toys.

The cooperation between IEEE 802.15.4 and Zigbee is similar to that between IEEE 802.11 and the Wi-Fi Alliance. The Zigbee 1.0 specification was ratified on December 14, 2004, and is available to Zigbee Alliance members. The Zigbee 2007 specification was posted on October 30, 2007. The first Zigbee profile application, Home Automation, was announced on November 2, 2007. Zigbee operates in the Industrial, Scientific, and Medical (ISM) radio bands: 868 MHz in Europe, 915 MHz in the United States and Australia, and 2.4 GHz in the rest of the world. Typically, commercially available Zigbee chips are radio and microcontroller combinations with 60K to 128K Flash memory from manufacturers such as Jennic JN5148, Freescale MC13213, Ember EM250, Texas Instruments CC2430, Samsung Electro-Mechanics. ZBS240, and Atmel Atmega128RFA1. The radio can also be used separately with any

processor and microcontroller. Typically, radio manufacturers also offer a Zigbee software stack, although other independent stacks are available.

Because Zigbee can wake up (i.e., go from sleep to wake) in 15 ms or less, device response times can be very low, especially compared to Bluetooth, which typically wakes up in 3 s. In turn, because Zigbee spends most of its time in sleep, power consumption can be very low, allowing for long battery life.

The first release of the stack is now known as Zigbee 2004. The second release of the stack is called Zigbee 2006, and basically replaces the MSG/KVP framework used in Zigbee 2004 along with a "cluster library". The 2004 stack is now more or less obsolete. The Zigbee 2007 implementation is currently the current one, and it contains 2 stack profiles:

- Stack Profile #1 (called simply Zigbee) for home and light commercial use,
- Stack Profile #2 (called Zigbee Pro).

Zigbee Pro offers more features such as broadcasting, multipoint-to-point routing, and high security using symmetric key encryption (SKKE), while Zigbee (Stack Profile #1) takes up less RAM and Flash memory. . Both profiles should deploy a full-scale network with a cellular topology and work with all Zigbee application profiles.

Zigbee 2007 is fully compatible with Zigbee 2006 devices. A Zigbee 2007 device can connect to and work with a Zigbee 2006 network and vice versa. Due to differences in routing options, a Zigbee Pro device can only be an end device (Zeds) of a Zigbee 2006 network, and vice versa, Zigbee 2006 and Zigbee 2007 devices can only be end devices in a Zigbee Pro network. However, the add-ons that run on the devices work the same, regardless of the implementation of the stack profile.

Zigbee protocols are designed for use in embedded applications that require low data rates and low power consumption.

Thus, the purpose of Zigbee is to create low-cost, self-organizing networks with a cellular topology designed to solve a wide range of tasks. The network can be used in industrial control, embedded sensors, medical data collection, intrusion or smoke alarm, building and home automation, etc. The resulting network consumes very little energy -

individual devices according to this Zigbee certification allow energy batteries to work for 2 years. Typical examples of Zigbee implementation are:

- home entertainment and control - smart lighting, advanced temperature control, security and safety, movies and music;

- home security - water and energy sensors, energy monitoring, smoke and fire sensors, smart access and negotiation sensors;

- mobile services - mobile payment, monitoring and control, security and access control, healthcare and telecare;

- commercial building – energy monitoring, HVAC, lighting, access control;

- industrial equipment – process control, industrial devices, energy and property management.

The protocols are built on the AODV (dynamic routing protocol for mobile ad-hoc networks (MANET) and other wireless networks) and Neurfon algorithms, which are designed to create ad-hoc (decentralized wireless network formed by random subscribers) or nodes. In some cases, the network is a cluster of clusters. It can also take the form of a network or a single cluster. Current profiles are derived from Zigbee protocols and support networks with or without beacons.

In networks with beacons disabled (where the order of the beacons is 15), a channel access mechanism is used. In this type of Zigbee network routers, your receivers are usually supported by long-term activations, which requires powerful power support. However, this allows heterogeneous networks, in which some devices receive while others only transmit, when external signals appear. A typical example of a heterogeneous network is a wireless lamp switch. The Zigbee node in the lamp can be used continuously, since it is connected to the common power supply, while the switch that appears in the lamp with the battery remains in sleep mode, as long as the switch is turned off. The switch then goes into active mode, sends commands to the lamp, waits for confirmation, and returns to sleep. In such networks, the lamp node must be at least a Zigbee router, if it is not a coordinator, the switch node is of course this Zigbee end device.

In networks with ad hoc network nodes, Zigbee routers transmit periodic messages to confirm their presence to other nodes in the network. Nodes can be in sleep mode between beacons, which reduces their switching frequency and increases battery life. Beacon intervals can vary from 15.36 ms to 15.36 * 214 = 251.65824 s for 250 kbps, from 24 ms to 24 * 214 = 393.216 s for 40 kbps, and from 48 ms to 48 * 214 = 786.432 s for 20 kbps. However, the low duty cycle of operations (signals) together with the long beacon intervals require precise timing, which can be part of the requirement for low product cost.

In general, Zigbee protocols reduce the time it takes for radios to turn on and reduce power consumption. In beacon networks, nodes must be active only when the beacon is transmitting. In beaconless networks, power consumption is significantly asymmetric, with some devices always active while others spend most of their time in sleep mode. Zigbee devices must be compatible with the IEEE 802.15.4-2003 wireless personal area network standard (except for the "power-efficient" profile 2.0). The standard defines the lower layers of the protocol - the physical layer (PHY), and the access control (MAC) as part of the data link layer (DLL). This standard specifies operation at 2.4 GHz (worldwide, unlicensed frequency), 915 MHz (USA) and 868 MHz (Europe) ISM bands. There are 16 Zigbee channels at 2.4 GHz. Each channel requires a bandwidth of 5 MHz. The fundamental frequency for each channel can be calculated as:

$$f_c = (2405 + 5 \cdot (CH - 11)) \text{ [МГц]},$$

де $CH = 11, 12, \ldots, 26$.

The radio segments use wideband direct spread spectrum modulation which is controlled by the digital stream in the modulator. Dual phase shift keying is used on the 868 and 915 MHz bands, and offset quadrature phase shift keying, which transmits 2 bits per symbol, is used on the 2.4 GHz band. In its pure form, when transmitted over the air, the data rate is 250 kbps for each channel in the 2.4 GHz band, 40 kbps for each channel in the 915 MHz band, and 20 kbps for each channel in the 868 MHz band. The transmission distance is from 10 to 75 m and over 1.5 km for Zigbee Pro, although it

depends heavily on the individual equipment. The maximum output power of the radio is generally 0 dBm (1 mW).

The basic channel access mode is "carrier sense multiple access/frame collision avoidance" (CSMA/CA - probabilistic channel MAC layer network protocol). That is, before nodes start transmitting on the information exchange path, they briefly check that none of them is transmitting before starting the general operation. There are three exceptions to the operation of CSMA. Beacons are sent for a predetermined time interval and CSMA is not used. Message acknowledgements also do not use CSMA. Finally, devices in beacon-oriented networks that have low secrecy in real-time requirements can also use guaranteed time slots, which by definition do not use CSMA.

Zigbee RF4CE specification. On March 3, 2009, the RF4CE (Radio Frequency for Consumer Electronics) concern agreed to work with the Zigbee Alliance to jointly distribute a standardized specification intended for radio frequency remote control. Zigbee RF4CE was designed for widespread use in remote-controlled audio-video products such as TVs and set-top boxes. It promises a number of advantages over existing remote control solutions, including expanded connectivity, increased reliability, enhanced capabilities and flexibility, compatibility, and removal of the line-of-sight barrier, etc.

The software is designed to simplify the process of building small, low-cost microprocessors. The radio designs used in Zigbee are optimized to achieve a low price point among the large number of products in this line. There are several analog cascades where it is possible to use digital circuits.

Although the radios themselves are inexpensive, the Zigbee qualification process includes a complete verification of the requirements at the physical layer. This reporting of the physical layer has numerous advantages, because all radios derived from this semiconductor equipment will have the same RF characteristics. On the other hand, if the physical layer is not certified, incorrect operation can reduce the battery life of other devices connected to the Zigbee network. Where other protocols can hide poor sensitivity or other hidden problems that manifest themselves in the distorted reduced response of Zigbee, radio circuits have hard engineering constraints related to power

supply and function width. There are solutions that integrate a microcontroller and a radio in a single package, such as the STM32W series microcontrollers from Stmicroelectronics.

The Zigbee specification is available to the general public for non-commercial use. An entry-level membership in the Zigbee Alliance, called Adopter, provides access to unpublished specifications and allows you to create products for the specification for commercial use. Registration to use the Zigbee specification requires a commercial developer to join the Zigbee Alliance. Since the GPL does not distinguish between commercial and non-commercial use, it is not possible to make a licensed Zigbee stack compliant with the GPL or to make a Zigbee implementation compliant with GPL-licensed code. Helping a developer join the Zigbee Alliance also conflicts with other free software licenses.

1.5. Analysis of WSN operation features

Using CSMA/CA as the basic access mode does not guarantee the elimination of even a significant number of packets due to collisions. Experiments have shown that such collisions occur due to the peculiarities of the CCA algorithm implementation. Due to the peculiarities of information traffic in sensor networks, competitive transmission often occurs. There is a general opinion that collisions in sensor networks built using the CSMA/CA algorithm can occur only in the case of a “hidden terminal”. However, experiments with 802.15.4 standard sensor network nodes have shown that a significant number of collisions occur even in the absence of a receiving terminal.

As a packet, with this type of collisions, it is lost only from nodes with a weaker signal. Nodes with a stronger signal are more resistant to such collisions. In general, lowering the sensitivity threshold (CCA Threshold) closer to the noise level allows you to significantly reduce the number of collisions.

In turn, when using the 2.4 GHz function, lost packets can reach up to 90%, regardless of traffic. This encourages the use of a special network loading algorithm

from the 802.11x (Wi-Fi) standard and the implementation of dynamic channel switching in WSN (Figure 1.6).

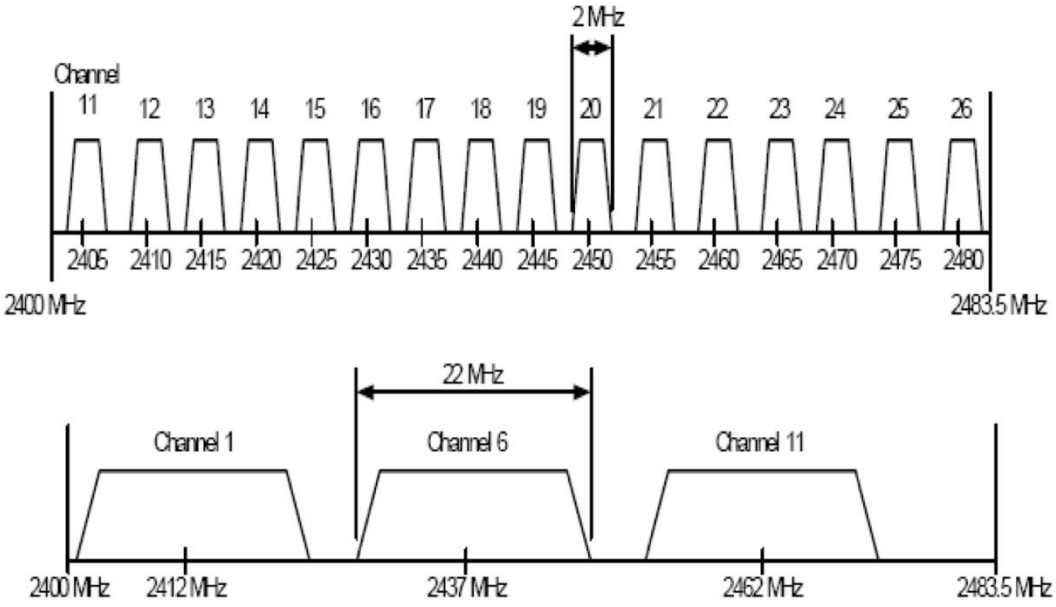


Figure 1.6 - Joint operation of Wi-Fi and WSN networks in the 2.4 GHz region

Input studies have established that WSN communication channels have effects and phenomena:

- channel asymmetry;
- channel instability;
- change in the signal power level over long periods of time;
- the indicator of the dependence of the received signal level (Received Signal Strength Indicator, RSSI) on temperature (changes of the order of 2 dB for every 10 degrees, and at elevated temperatures the level of transmitter output power and receiver sensitivity also decrease);
- unpredictability.

They have a strong impact on the operation of the entire network as a whole (loss of communication, reduced network connectivity, localization errors, etc.). The presence of a power amplifier (PA) and a low-noise amplifier (LNA) requires thermal compensation.

In their case, these effects affect the protocols of the upper layers. Thus, the packet reception rate (PRR) depends not only on the distance and environmental conditions, but also on the error correction scheme used. Small packets are less prone to errors (fewer bits in a packet - less probability of a packet error). If we take short packets, it is impossible to precisely adjust the PRR when using longer packets. As a result of using short packets to increase the transmission range. For example, control packets are short and have a high probability of correct reception.

To ensure the proper level of WSN protection, it is necessary to develop encryption algorithms focused on use in nodes with limited computing capabilities, implement variable block duration, incl. taking into account the energy consumption of the node. In addition, it is necessary to develop algorithms for authenticating network nodes, taking into account their limited computing capabilities and traffic authentication (ensuring data integrity).

As a result, to protect WSNs, it is necessary to use:

- mechanisms for redundancy of the transport environment;

- interference-resistant data transmission technologies at the physical level;

- implementation of ultra-wideband communication systems (range 3.1÷10.6 GHz with a bandwidth > 500 MHz).

Thus, it is possible to formulate the following requirements for WSNs.

1. Resistance to active radio interference.

2. Detection of node substitution.

3. Availability of backup data transmission routes.

4. Detection and prevention of attempts to reconfigure the network, substitution of address information, unauthorized "flashing" of devices,

5. Resistance to frame distortion and filtering.

Further research should be directed towards increasing the noise immunity of WSN communication channels.

1.6. General statement of the problem

Analysis of ways to increase the efficiency of WSN operation by using communication channels with increased noise immunity, defining research tasks that arose in the development of proposals for the implementation of digital processing of positional signals based on many N-OFDM (OFDM).

As a result, the following research tasks are necessary in the work:

1. Substantiation of directions for increasing the noise immunity of WSN.

2. Analysis of signal modulation methods in WSN.

3. Development of proposals for the use of multi-position signals in WSN.

4. Feasibility study of the decisions made.

Mathematical formalization of the main research tasks will be carried out in the sections in which they will be solved.

Conclusion

The relevance of WSN research is obvious. They are used in many industries: this is monitoring the situational situation of troops, weather, ecology, etc. With the improvement of technologies and various industries, the need for WSN will only grow. The main tasks of WSN are: periodic measurement of the indicator; event detection; measurement of the indicator on request.

The most advanced options for WSN circuit solutions include: DASH7, Z-Wave, Insteon, Enocean, ISA100.11a, Wirelesshart, Miwi, 6Lowpan, One-Net, Wavenis, Rubee, Zigbee (Pro).

The main feature of ZigBee is that with low power consumption, not only a simple network topology (“point-to-point”, “tree” and “star”) is supported, but also a mesh topology with message relay and routing. In addition, the ZigBee specification (based on IEEE 802.15.4) contains the ability to choose a routing algorithm, in accordance with the requirements of the software and the network state, an application standardization mechanism - application profiles, a library of standard clusters, endpoints, bindings, a security mechanism, and also provides ease of deployment, maintenance and modernization.

Unfortunately, the use of CSMA/CA as the basic access mode does not guarantee the elimination of significant packet losses due to collisions. Experiments with 802.15.4 sensor network nodes have shown that a significant number of collisions occur even if there is no accepted terminal; with this type of collision, packets are lost only from nodes with a lower signal level. Nodes with a stronger signal are more resistant to such collisions.

In turn, when using the 2.4 GHz function, lost packets can reach up to 90%, regardless of traffic. This applies to the use of special algorithms for starting from the 802.11ax network (Wi-Fi) and the implementation of dynamic channel switching in WSNs.

Initial studies have established that the following effects and phenomena are inherent in WSN communication channels: channel asymmetry; channel instability; signal power level variations over long periods of time; RSSI dependence on temperature; unpredictability.

They have a strong impact on the operation of the entire network as a whole (loss of communication, reduced network connectivity, localization errors, etc.), and most importantly, they affect the protocols of the upper layers.

As a result, to protect WSNs, it is advisable to use: transport environment redundancy mechanisms; interference-protected data transmission technologies at the physical level; implementation of ultra-wideband communication systems (range 3.1÷10.6 GHz with a bandwidth > 500 MHz).

Thus, it is possible to formulate the following requirements for WSNs.

1. Resistance to active radio interference.

2. Detection of node substitution.

3. Availability of backup data transmission routes.

4. Detection and prevention of attempts to reconfigure the network, substitution of address information, unauthorized "flashing" of devices,

5. Resistance to frame distortion and filtering.

Further research should be directed towards increasing the noise immunity of WSN communication channels.

ДОДАТОК Б.

ЛІСТИНГ ПРОГРАМИ ОБЧИСЛЕННЯ ФУНКЦІОНАЛА МНК ДЛЯ МЕТОДУ СПЕКТРАЛЬНОГО ДЕТЕКТУВАННЯ СИГНАЛУ В УМОВАХ ВПЛИВУ ВУЗЬКОСМУГОВОЇ ЗАВАДИ

Функции преобразования чисел из десятичной в двоичную и наоборот

Перевод числа из десятичной ф. в двоичную

```
ChDesToDv(chDes, bt) := | tmpCh ← chDes
                        | for i ∈ 0 .. bt − 1
                        |   | TmpV_i ← 0
                        |   | sr ← tmpCh − 2^(bt−1−i)
                        |   | TmpV_i ← 1  if sr ≥ 0
                        |   | tmpCh ← sr  if sr ≥ 0
                        | TmpV
```

Перевод числа из двоичной ф. в десятичную

```
ChDvToDes(VchDv) := | bt ← rows(VchDv)
                    | ChDes ← 0
                    | for i ∈ 0 .. bt − 1
                    |   | tmp ← VchDv_i · 2^(bt−1−i)
                    |   | ChDes ← ChDes + tmp
                    | ChDes
```

$Ntmp := rnorm(100, 0, 1)$

$T := 64 \qquad M := 4 \qquad TT := T \cdot M$

$k := 0 .. T - 1 \qquad s := 0 .. M - 1$

	0
0	-0.439
1	-0.679
2	-0.473
3	-0.951
4	...

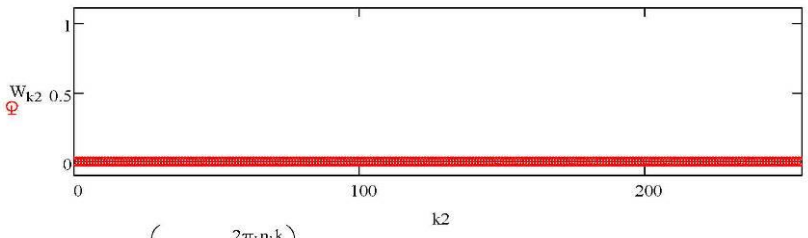
Ntmp =

```
W := | for s ∈ 0 .. M − 1
     |   for k ∈ 0 .. T − 1
     |     Tmw_(T·s+k) ← | 1  if Ntmp_s > 0
     |                   | 0  otherwise
     | Tmw
```

```
Wsokr := | for s ∈ 0 .. M − 1
         |   Tmws_s ← W_(T·s)
         | Tmws
```

$$Wsokr = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$k2 := 0 .. TT - 1$



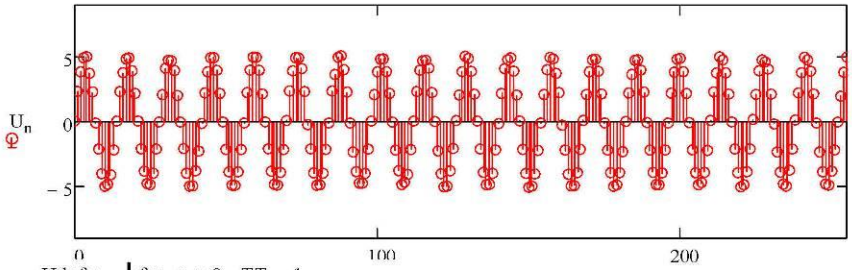
$$dpf(n) := \sum_{k=0}^{TT-1} \left(W_k \cdot e^{-i \cdot \frac{2\pi \cdot n \cdot k}{TT}} \right)$$

$n := 0 .. TT - 1 \qquad Nois := rnorm(TT, 0, 1)$

формирование синусоидальной помехи

$$Wsin := \left| \begin{array}{l} \text{for } n \in 0..TT-1 \\ \quad Tmws_n \leftarrow Rsin \cdot \sin\left(2 \cdot \pi \cdot \frac{1}{krat} \cdot n\right) \\ Tmws \end{array} \right.$$

$$U := \left| \begin{array}{l} \text{for } n \in 0..TT-1 \\ \quad Tmwn_n \leftarrow W_n + Rnois \cdot Nois_n + Wsin_n \\ Tmwn \end{array} \right.$$



$$Udpf := \left| \begin{array}{l} \text{for } n \in 0..TT-1 \\ \quad Wtmp_n \leftarrow \sum_{k=0}^{TT-1} \left(U_k \cdot e^{-i \cdot \frac{2\pi \cdot n \cdot k}{TT}} \right) \\ Wtmp \end{array} \right.$$

$Udpf =$

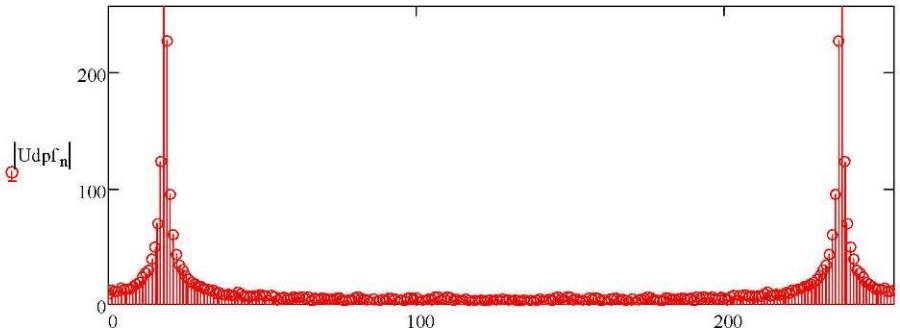
	0
0	8.91204
1	11.23836-3.94936i
2	10.87442+0.62963i
3	10.74074-1.71113i
4	13.10073-3.53611i
5	11.95285-3.98228i
6	12.08742-4.07773i
7	...

$$Udpf2 := \left| \begin{array}{l} \text{for } s \in 0..M-1 \\ \quad \text{for } n \in 0..T-1 \\ \quad\quad Wtmp_{n,s} \leftarrow \sum_{k=0}^{T-1} \left(U_{k+s \cdot T} \cdot e^{-i \cdot \frac{2\pi \cdot n \cdot k}{T}} \right) \\ Wtmp \end{array} \right.$$

$Udpf2 =$

	0	1	2	3
0	22.09	-18.797	11.488	-5.869
1	23.552+1.152i	-20.393-3.532i	14.909+4.067i	-4.967-5.224i
2	26.923+3.704i	-23.735-7.825i	16.041+10.075i	-5.47-11.846i
3	38.961+5.391i	-32.594-17.064i	21.109+22.829i	-4.756-25.31i
4	91.296+18.058i	-75.353-50.336i	44.802+73.687i	-3.853-80.668i
5	-107.261-26.625i	83.821+75.686i	-43.401-109.484i	-6.023+120.084i
6	-29.104-9.048i	21.701+24.493i	-9.498-34.078i	-4.754+38.519i
7	-15.313-5.695i	9.847+15.803i	-2.554-21.998i	-4.546+23.986i
8	-9.712-3.569i	5.932+11.375i	-0.604-15.593i	-4.302+17.56i
9	-6.278-3.781i	2.144+8.891i	0.899-12.872i	...

$$Udpf := \left| \begin{array}{l} \text{for } n \in 0..TT-1 \\ \quad \left| \begin{array}{l} Wtmp_n \leftarrow \sum_{k=0}^{TT-1} \left(U_k \cdot e^{-i \cdot \frac{2\pi \cdot n \cdot k}{TT}} \right) \\ 0 \text{ if } \left| Re\left(Wtmp_n\right) \right| < 2 \\ Wtmp_n \text{ otherwise} \end{array} \right. \\ Wtmp \end{array} \right.$$



Формирование эталонной матрицы $Matrix\_Etalon^{n}$

$Matrix\_Etalon1 :=$

$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_0000.prn")$
for $k \in 0..TT-1$
$TmEt_{k,0} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_0001.prn")$
for $k \in 0..TT-1$
$TmEt_{k,1} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_0010.prn")$
for $k \in 0..TT-1$
$TmEt_{k,2} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_0011.prn")$
for $k \in 0..TT-1$
$TmEt_{k,3} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_0100.prn")$
for $k \in 0..TT-1$
$TmEt_{k,4} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_0101.prn")$
for $k \in 0..TT-1$
$TmEt_{k,5} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_0110.prn")$
for $k \in 0..TT-1$
$TmEt_{k,6} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_0111.prn")$
for $k \in 0..TT-1$
$TmEt_{k,7} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_1000.prn")$
for $k \in 0..TT-1$
$TmEt_{k,8} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_1001.prn")$
for $k \in 0..TT-1$
$TmEt_{k,9} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_1010.prn")$
for $k \in 0..TT-1$
$TmEt_{k,10} \leftarrow Et_k$
$Et \leftarrow READPRN("\backslash Etalon\_Dpf\backslash 256\_1011.prn")$

```
for k ∈ 0 .. TT − 1
  TmEt_{k,11} ← Et_k
Et ← READPRN("\Etalon_Dpf\256_1100.prn")
for k ∈ 0 .. TT − 1
  TmEt_{k,12} ← Et_k
Et ← READPRN("\Etalon_Dpf\256_1101.prn")
for k ∈ 0 .. TT − 1
  TmEt_{k,13} ← Et_k
Et ← READPRN("\Etalon_Dpf\256_1110.prn")
for k ∈ 0 .. TT − 1
  TmEt_{k,14} ← Et_k
Et ← READPRN("\Etalon_Dpf\256_1111.prn")
for k ∈ 0 .. TT − 1
  TmEt_{k,15} ← Et_k
TmEt
```

```
Matrix_Etalon2 := Et ← READPRN("\Etalon_Dpf\64_0.prn")
                  for k ∈ 0 .. T − 1
                    TmEt_{k,0} ← Et_k
                  Et ← READPRN("\Etalon_Dpf\64_1.prn")
                  for k ∈ 0 .. T − 1
                    TmEt_{k,1} ← Et_k
```

Matrix_Etalon1 =

	0	1
0	0	64
1	0	40.24+41.24i
2	0	-1+40.74i
3	0	-14.08+13.08i
4	0	$-8.549\cdot10^{-15}+1.915i\cdot10^{-15}$
5	0	7.639+8.639i
6	0	-1+13.56i
7	0	-6.306+5.306i
8	0	$1.998\cdot10^{-15}-5.274i\cdot10^{-15}$
9	0	4.009+5.009i
10	0	-1+8.108i
11	0	-4.181+3.181i
12	0	$-3.664\cdot10^{-15}+2.331i\cdot10^{-15}$
13	0	2.607+3.607i
14	0	-1+5.763i
15	0	...

Matrix_Etalon2 =

	0	1
0	0	64
1	0	$-2.331\cdot10^{-15}+3.594i\cdot10^{-15}$
2	0	$-1.221\cdot10^{-15}-2.665i\cdot10^{-15}$
3	0	$-4.108\cdot10^{-15}-2.498i\cdot10^{-15}$
4	0	$-7.327\cdot10^{-15}-4.607i\cdot10^{-15}$
5	0	$-1.443\cdot10^{-15}+4.885i\cdot10^{-15}$
6	0	$-4.663\cdot10^{-15}+1.11i\cdot10^{-15}$
7	0	$-2.887\cdot10^{-15}-1.665i\cdot10^{-15}$
8	0	$-6.883\cdot10^{-15}-3.775i\cdot10^{-15}$
9	0	$1.309\cdot10^{-14}-1.932i\cdot10^{-14}$

9	0	1.399·10^-14-1.952i·10^-14
10	0	-1.443·10^-15
11	0	-7.994·10^-15-4.441i·10^-15
12	0	-1.249·10^-14-1.499i·10^-14
13	0	...

Сравнение для **многоимпульсной** комбинации

$$SravRe\_1 := \left| \begin{array}{l} \text{for } i \in 0..15 \\ TmpSr_i \leftarrow \sum_{k=0}^{TT-1} \left(Re\left(Udpf_k\right) - Re\left(Matrix\_Etalon1_{k,i}\right) \right)^2 \\ TmpSr \end{array} \right.$$

$$SravIm\_1 := \left| \begin{array}{l} \text{for } i \in 0..15 \\ TmpSr_i \leftarrow \sum_{k=0}^{TT-1} \left(Im\left(Udpf_k\right) - Im\left(Matrix\_Etalon1_{k,i}\right) \right)^2 \\ TmpSr \end{array} \right.$$

$$SravMod\_1 := \left| \begin{array}{l} \text{for } i \in 0..15 \\ TmpSr_i \leftarrow \sum_{k=0}^{TT-1} \left(\left|Udpf_k\right| - \left|Matrix\_Etalon1_{k,i}\right| \right)^2 \\ TmpSr \end{array} \right.$$

$$SravNomRe\_1 := \left| \begin{array}{l} Tmpmin_0 \leftarrow SravRe\_1_0 \\ Tmpmin_1 \leftarrow 0 \\ \text{for } i \in 1..15 \\ \quad \text{if } SravRe\_1_i < Tmpmin_0 \\ \quad\quad Tmpmin_0 \leftarrow SravRe\_1_i \\ \quad\quad Tmpmin_1 \leftarrow i \\ Tmpmin \end{array} \right.$$

$$SravNomIm\_1 := \left| \begin{array}{l} Tmpmin_0 \leftarrow SravIm\_1_0 \\ Tmpmin_1 \leftarrow 0 \\ \text{for } i \in 1..15 \\ \quad \text{if } SravIm\_1_i < Tmpmin_0 \\ \quad\quad Tmpmin_0 \leftarrow SravIm\_1_i \\ \quad\quad Tmpmin_1 \leftarrow i \\ Tmpmin \end{array} \right.$$

$$SravNomMod\_1 := \left| \begin{array}{l} Tmpmin_0 \leftarrow SravMod\_1_0 \\ Tmpmin_1 \leftarrow 0 \\ \text{for } i \in 1..15 \\ \quad \text{if } SravMod\_1_i < Tmpmin_0 \\ \quad\quad Tmpmin_0 \leftarrow SravMod\_1_i \\ \quad\quad Tmpmin_1 \leftarrow i \\ Tmpmin \end{array} \right.$$

Сравнение для **одноимпульсной** комбинации

$$SravRe\_2 := \left| \begin{array}{l} \text{for } s \in 0..M-1 \\ \quad \text{for } i \in 0..1 \\ \quad\quad TmpSr_{i,s} \leftarrow \sum_{k=0}^{T-1} \left(Re\left(Udpf2_{k,s}\right) - Re\left(Matrix\_Etalon2_{k,i}\right) \right)^2 \\ TmpSr \end{array} \right.$$

SravIm_2 :=
for $s \in 0..M-1$
  for $i \in 0..1$
    $TmpSr_{i,s} \leftarrow \sum_{k=0}^{T-1} \left(Im\left(Udpf2_{k,s}\right) - Im\left(Matrix\_Etalon2_{k,i}\right)\right)^2$
TmpSr

SravMod_2 :=
for $s \in 0..M-1$
  for $i \in 0..1$
    $TmpSr_{i,s} \leftarrow \sum_{k=0}^{T-1} \left(\left|Udpf2_{k,s}\right| - \left|Matrix\_Etalon2_{k,i}\right|\right)^2$
TmpSr

DecOdnoimpRe :=
for $s \in 0..M-1$
  if $SravRe\_2_{0,s} < SravRe\_2_{1,s}$
    $Tmpmin_{0,s} \leftarrow SravRe\_2_{0,s}$
    $Tmpmin_{1,s} \leftarrow 0$
  if $SravRe\_2_{1,s} < SravRe\_2_{0,s}$
    $Tmpmin_{0,s} \leftarrow SravRe\_2_{1,s}$
    $Tmpmin_{1,s} \leftarrow 1$
Tmpmin

DecOdnoimpIm :=
for $s \in 0..M-1$
  if $SravIm\_2_{0,s} < SravIm\_2_{1,s}$
    $Tmpmin_{0,s} \leftarrow SravIm\_2_{0,s}$
    $Tmpmin_{1,s} \leftarrow 0$
  if $SravIm\_2_{1,s} < SravIm\_2_{0,s}$
    $Tmpmin_{0,s} \leftarrow SravIm\_2_{1,s}$
    $Tmpmin_{1,s} \leftarrow 1$
Tmpmin

DecOdnoimpMod :=
for $s \in 0..M-1$
  if $SravMod\_2_{0,s} < SravMod\_2_{1,s}$
    $Tmpmin_{0,s} \leftarrow SravMod\_2_{0,s}$
    $Tmpmin_{1,s} \leftarrow 0$
  if $SravMod\_2_{1,s} < SravMod\_2_{0,s}$
    $Tmpmin_{0,s} \leftarrow SravMod\_2_{1,s}$
    $Tmpmin_{1,s} \leftarrow 1$
Tmpmin

Сравнение для **многоимпульсной** комбинации

	0
0	$5.063 \cdot 10^5$
1	$5.108 \cdot 10^5$
2	$5.149 \cdot 10^5$
3	$5.195 \cdot 10^5$
4	$5.186 \cdot 10^5$

	0
0	$3.137 \cdot 10^5$
1	$3.285 \cdot 10^5$
2	$3.156 \cdot 10^5$
3	$3.304 \cdot 10^5$
4	$3.275 \cdot 10^5$

round(SravRe_1, 1) =

5	$5.234 \cdot 10^5$
6	$5.433 \cdot 10^5$
7	$5.482 \cdot 10^5$
8	$5.092 \cdot 10^5$
9	$5.299 \cdot 10^5$
10	$5.178 \cdot 10^5$
11	$5.385 \cdot 10^5$
12	$5.215 \cdot 10^5$
13	$5.424 \cdot 10^5$
14	$5.463 \cdot 10^5$
15	$5.672 \cdot 10^5$

round(SravIm_1, 1) =

5	$3.42 \cdot 10^5$
6	$3.132 \cdot 10^5$
7	$3.277 \cdot 10^5$
8	$3.159 \cdot 10^5$
9	$3.146 \cdot 10^5$
10	$3.177 \cdot 10^5$
11	$3.164 \cdot 10^5$
12	$3.296 \cdot 10^5$
13	$3.28 \cdot 10^5$
14	$3.153 \cdot 10^5$
15	$3.137 \cdot 10^5$

$Rnois \equiv 0.1 \qquad Rsin \equiv 5 \qquad krat \equiv 14$

Было передано $Wsokr^T = (0 \;\; 0 \;\; 0 \;\; 0)$

Принято $ChDesToDv(SravNomRe\_1_1, 4)^T = (0 \;\; 0 \;\; 0 \;\; 0)$

Сравнение для **одноимпульсной** комбинации (пошагово)

$$SravRe\_2 = \begin{pmatrix} 4.832 \times 10^4 & 3.12 \times 10^4 & 1.05 \times 10^4 & 1.533 \times 10^3 \\ 4.959 \times 10^4 & 3.77 \times 10^4 & 1.312 \times 10^4 & 6.38 \times 10^3 \end{pmatrix} \qquad SravIm\_2 = \begin{pmatrix} 2.528 \times 10^3 & 1.978 \times 10^4 & 4.129 \times 10^4 & 4.985 \times 10^4 \\ 2.528 \times 10^3 & 1.978 \times 10^4 & 4.129 \times 10^4 & 4.985 \times 10^4 \end{pmatrix}$$

$$SravMod\_2 = \begin{pmatrix} 5.085 \times 10^4 & 5.098 \times 10^4 & 5.179 \times 10^4 & 5.138 \times 10^4 \\ 5.211 \times 10^4 & 5.267 \times 10^4 & 5.441 \times 10^4 & 5.473 \times 10^4 \end{pmatrix}$$

$$S\_re := \sqrt{\frac{SravRe\_1}{TT^2}}$$

$S\_re^T =$

	0	1	2	3	4	5	6	7	8
0	2.779	2.792	2.803	2.816	2.813	2.826	2.879	2.892	...

Декодировано
по реальной по мнимой составляющей

$$SravNomRe\_1 = \begin{pmatrix} 5.063 \times 10^5 \\ 0 \end{pmatrix} \qquad SravNomIm\_1 = \begin{pmatrix} 3.132 \times 10^5 \\ 6 \end{pmatrix}$$

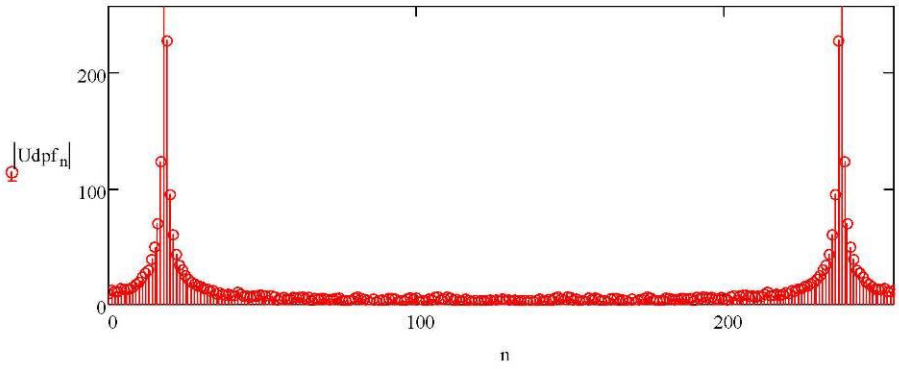
по модулю $SravNomMod\_1 = \begin{pmatrix} 8.054 \times 10^5 \\ 1 \end{pmatrix}$

Декодировано
по реальной по мнимой составляющей

$$DecOdnoimpRe = \begin{pmatrix} 4.832 \times 10^4 & 3.12 \times 10^4 & 1.05 \times 10^4 & 1.533 \times 10^3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$DecOdnoimpIm = \begin{pmatrix} 0 & 1.978 \times 10^4 & 0 & 4.985 \times 10^4 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

по модулю $DecOdnoimpMod = \begin{pmatrix} 5.085 \times 10^4 & 5.098 \times 10^4 & 5.179 \times 10^4 & 5.138 \times 10^4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$


200
100
0
|Udpf_n|
0
100
200
n

ДОДАТОК В

Тези статей науково-практичних конференцій

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Департамент економічного розвитку, торгівлі та залучення інвестицій
Полтавської обласної військової адміністрації
Полтавська торгово-промислова палата
Університет Флорида (США)
"1 DECEMBRIE 1918" University of Alba Iulia (Румунія)
Білостоцький технологічний університет (Польща)
Вільнюський університет прикладних наук (VIKO) (Литва)
London Metropolitan University (Велика Британія)
Словацький технологічний університет (Словаччина)
Рада молодих вчених Національної академії наук України
Рада молодих вчених Національного університету «Запорізька політехніка»
Рада молодих вчених Національного технічного університету «Дніпровська політехніка»
Рада молодих вчених Національного університету «Чернігівська політехніка»
Рада молодих вчених Національного університету «Одеська політехніка»
Рада молодих вчених Одеського національного університету імені І.І. Мечникова
Рада молодих вчених Ізмаїльського державного гуманітарного університету
Рада молодих вчених Глухівського національного педагогічного університету імені Олександра Довженка
Рада молодих вчених Сумського національного аграрного університету
Рада молодих вчених Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
Рада молодих вчених Харківського національного педагогічного університету імені Г.С. Сковороди
Рада молодих вчених Чернівецького національного університету імені Юрія Федьковича
Наукове товариство студентів та молодих вчених Хмельницького національного університету
Рада молодих вчених Київського національного університету будівництва та архітектури
Рада молодих вчених Херсонського державного аграрно-економічного університету

МОЛОДІЖНА НАУКА: ІННОВАЦІЇ ТА ГЛОБАЛЬНІ ВИКЛИКИ

ЗБІРНИК ТЕЗ

Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених

Полтава, 06 листопада 2024 року

УДК 621.396

Дюдюк Ігор Миколайович,
магістрант гр. 2дТТ,
Івко Сергій Олександрович,
к.т.н.,
Смоляр Віктор Григорович,
к.т.н., доцент,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

УДОСКОНАЛЕННЯ РОБОТИ СЕНСОРНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ КАНАЛІВ ЗВ'ЯЗКУ З ПІДВИЩЕНОЮ ЗАВАДОСТІЙКІСТЮ

Новітні технології бездротового зв'язку та прогрес в області виробництва мікроелектроніки дозволили протягом останніх десятиліть перейти до практичної розробки та впровадженню нового класу розподілених комунікаційних систем – сенсорних мереж.

Бездротові сенсорні мережі – це перспективна технологія. В процесі розробки сенсорних мереж, були виявлені недоліки каналів зв'язку бездротових сенсорних мереж такі як: асиметричність каналів, нестабільність каналів, непередбачуваність, зміна рівня потужності сигналу на тривалих проміжках часу. Всі ці явища вносять свій вплив на стабільність роботи мережі. Тому навіть використовуючи метод множинного доступу з виявленням несучої і уникнення колізій (CSMA/CA), не є гарантом компенсації втрат пакетів від колізій. При цьому губляться пакети тільки від вузлів з найбільш слабким рівнем сигналу, а вузли з більш сильним рівнем сигналу стабільні.

Щоб підвищити, ефективність використання радіочастотного спектру знайшла застосування технологія OFDM (мультиплексування з ортогональним частотним розділенням каналів).

Мультиплексування з кодованим ортогональним частотним поділом каналів (COFDM) є альтернативою сигналу з однією несучою, яка часто використовується через обмеження систем з однією несучою для широкосмугових програм, де використовується багатопроменевість. Ці обмеження зумовлені частотно-вибірковим завмиранням, яке спричиняє значну різницю потужності сигналу прийому в широкосмуговому каналі, а також міжсимвольними перешкодами, які можуть виникати в середовищах із великим розповсюдженням затримки.

COFDM також забезпечує бездротовий зв'язок вирішенням проблеми міжсимвольної інтерференції (ISI). Між кожним переданим символом залишається захисний інтервал, щоб у приймача був час для отримання копії символу, що надходить на довшому відбитому шляху, без перекриття з наступним символом. В приймачі відбувається перекриття символів, в момент коли захи-

сний інтервал достатньо довгий і коли він занадто короткий, що призводить до міжсимвольної інтерференції.

В широкосмуговій системі з однією несучою довжина символу стає дуже малою для даної швидкості передачі даних. Захисний інтервал, необхідний для врахування відмінностей у довжині шляху, може стати таким же або довшим, ніж символ. Це зменшить кількість даних, які можна надіслати, так як пауза буде збільшуватися.

Символи ставатимуть довшими прямо пропорційно кількості використаних піднесучих. Таким чином, захисний інтервал установленої довжини менше впливатиме на кількість даних, які можуть бути передані, так як символ перенесення даних переважатиме над захисним інтервалом.

Мультиплексування з кодованим ортогональним частотним поділом каналів практично нечутливе до завмирань та короткочасним завадам.

Також, треба врахувати технологію MIMO (множинного входу – множинного виходу).

Сигнал на вході двох приймальних антен, спотворюється шумом, який не корельований між антенами, таким чином об’єднавши два сигнали, можна отримати кращий сигнал. Рознесення також можна досягти за допомогою кількох передавальних антен методом просторово-часового кодування (STC).

Все це свідчить про прямий взаємозв’язок завадостійкості з енергетичною та частотною ефективністю бездротових сенсорних мереж. Їх одночасне підвищення впливає на надійність роботи в цілому, як системи. Завадостійкість приймання сигналів в системі MIMO суттєво залежить від вибору методу обробки сигналів на приймальному боці. Існуючі методи обробки сигналів, які забезпечують задану якість передачі інформації, мають високу обчислювальну складність, тому виникає необхідність удосконалення цих методів.

Література

1. Смоляр В.Г., Тишко С.А., Слюсарь І.І. // Системи управління, навігації та зв’язку. – К.: Центральний науково-дослідний інститут навігації та управління, 2011. – Вип. 1(21). – С. 268-271.

2. Вісник Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Комунікаційні та інформаційні системи. Випуск № 1. – Київ: ВІТІ, 2021. – 122 с.

3. https://silvustechnologies.com

4. https://uk.wikipedia.org/wiki/MIMO.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами X Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:

ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

20 грудня 2024 року

Полтава 2024

БМ встановлюються поблизу труби (5-10 м), на певній відстані (100 м) та з'єднуються між собою за допомогою бездротового радіозв'язку [2], утворюючи сенсорну мережу послідовно розташованих бездротових пристроїв, які за допомогою ретрансляції передають інформацію від точки до точки.

Вибір бездротового каналу зв'язку для передачі даних між БМ та ЕОМ пояснюється складністю прокладання кабелю у важкодоступних районах експлуатації газопроводів.

ЛІТЕРАТУРА:

1. Грудз В.Я., Грудз Я.В., Боднар В.М., Самсоненко В.В. Прогнозування ремонтних робіт магістральних газопроводів в умовах централізованої системи обслуговування. Розвідка та розробка нафтових і газових родовищ. 2018. №3(68). С. 31 – 38.

2. Електронний ресурс. Режим доступу: https://promsystem.com.ua/product/crowcon-smart-3g-c2-staczionarnyj-detektor-gazu/

3. Електронний ресурс. Режим доступу: https://atomic-shop.ua/products/zeronoise-6300036-komplekt-bezdrotovoho-radiozviazku-10-serii

DESIGN OF A SENSOR-BASED TELECOMMUNICATION SYSTEM FOR MONITORING GAS LEAKAGE FROM A PIPELINE

***O. Shefer**, Doctor of Science, Professor,*
***O. Romanenko**, Master's Student,*
National University "Yuri Kondratyuk Poltava Polytechnic"

УДК 621.396

***І.М. Дюдюк**, магістрант,*
***О.С. Фомін**, к.т.н., доцент*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

УДОСКОНАЛЕННЯ РОБОТИ СЕНСОРНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ КАНАЛІВ ЗВ'ЯЗКУ З ПІДВИЩЕНОЮ ЗАВАДОСТІЙКІСТЮ

Новітні технології бездротового зв'язку та прогрес в області виробництва мікроелектроніки дозволили протягом останніх десятиліть перейти до практичної розробки та впровадженню нового класу розподілених комунікаційних систем – сенсорних мереж.

Бездротові сенсорні мережі – це перспективна технологія. В процесі розробки сенсорних мереж, були виявлені недоліки каналів зв'язку бездротових сенсорних мереж такі як: асиметричність каналів, нестабільність каналів, непередбачуваність, зміна рівня потужності сигналу на тривалих проміжках часу. Всі ці явища вносять свій вплив на стабільність роботи мережі. Тому навіть використовуючи метод множинного доступу з виявленням несучої і уникнення

колізій (CSMA/CA), не є гарантом компенсації втрат пакетів від колізій. При цьому губляться пакети тільки від вузлів з найбільш слабким рівнем сигналу, а вузли з більш сильним рівнем сигналу стабільні.

Щоб підвищити, ефективність використання радіочастотного спектру знайшла застосування технологія OFDM (мультиплексування з ортогональним частотним розділенням каналів).

Мультиплексування з кодованим ортогональним частотним поділом каналів (COFDM) є альтернативою сигналу з однією несучою, яка часто використовується через обмеження систем з однією несучою для широкосмугових програм, де використовується багатопроменевість. Ці обмеження зумовлені частотно-вибірковим завмиранням, яке спричиняє значну різницю потужності сигналу прийому в широкосмуговому каналі, а також міжсимвольними перешкодами, які можуть виникати в середовищах із великим розповсюдженням затримки.

COFDM також забезпечує бездротовий зв'язок вирішенням проблеми міжсимвольної інтерференції (ISI). Між кожним переданим символом залишається захисний інтервал, щоб у приймача був час для отримання копії символу, що надходить на довшому відбитому шляху, без перекриття з наступним символом. В приймачі відбувається перекриття символів, в момент коли захисний інтервал достатньо довгий і коли він занадто короткий, що призводить до міжсимвольної інтерференції.

В широкосмуговій системі з однією несучою довжина символу стає дуже малою для даної швидкості передачі даних. Захисний інтервал, необхідний для врахування відмінностей у довжині шляху, може стати таким же або довшим, ніж символ. Це зменшить кількість даних, які можна надіслати, так як пауза буде збільшуватися.

Символи ставатимуть довшими прямо пропорційно кількості використаних піднесучих. Таким чином, захисний інтервал установленої довжини менше впливатиме на кількість даних, які можуть бути передані, так як символ перенесення даних переважатиме над захисним інтервалом.

Мультиплексування з кодованим ортогональним частотним поділом каналів практично нечутливе до завмирань та короткочасним завадам.

Також, треба врахувати технологію MIMO (множинного входу – множинного виходу).

Сигнал на вході двох приймальних антен, спотворюється шумом, який не корельований між антенами, таким чином об’єднавши два сигнали, можна отримати кращий сигнал. Рознесення також можна досягти за допомогою кількох передавальних антен методом просторово-часового кодування (STC).

Все це свідчить про прямий взаємозв’язок завадостійкості з енергетичною та частотною ефективністю бездротових сенсорних мереж. Їх одночасне підвищення впливає на надійність роботи в цілому, як системи. Завадостійкість приймання сигналів в системі MIMO суттєво залежить від вибору методу обробки сигналів на приймальному боці. Існуючі методи обробки сигналів, які

забезпечують задану якість передачі інформації, мають високу обчислювальну складність, тому виникає необхідність удосконалення цих методів.

ЛІТЕРАТУРА:

1. Смоляр В.Г., Тишко С.А., Слюсарь І.І. Системи управління, навігації та зв'язку. – К.: Центральний науково-дослідний інститут навігації та управління, 2011. – Вип. 1(21). – С. 268-271.

2. Вісник Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Комунікаційні та інформаційні системи. Випуск № 1. – Київ: ВІТІ, 2021. – 122 с.

3. https://silvustechnologies.com

4. https://uk.wikipedia.org/wiki/MIMO.

IMPROVING THE OPERATION OF THE SENSORY METERING BEYOND ADDITIONAL CHANNELS IN CONNECTION WITH ADVANCED SENSITIVITY

***I. Diudiuk**, Master's Student,*
***O. Fomin,** PhD, Associate Professor*
National University "Yuri Kondratyuk Poltava Polytechnic"

ДОДАТОК Г

Презентаційний матеріал

Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут інформаційних технологій і робототехніки

Кафедра автоматики, електроніки та телекомунікацій

Удосконалення роботи сенсорної мережі за допомогою каналів зв'язку з підвищеною завадостійкістю

Кваліфікаційна робота магістра

Виконав:
Магістрант д6ТТ групи Дюдюк І.М.

Керівник:
к.т.н., доцент Фомін О.С.

Полтава 2025

Актуальність досліджень БСМ очевидна. Їх використовують в багатьох галузях: це моніторинг ситуативної обстановки військ, погоди, екології, та ін. З удосконалюванням технологій та різних виробництв, потреба в WSN буде тільки збільшуватиметься. Основними завданнями WSN є: періодичний вимір показника; детектування події; вимірювання показника за запитом.

Метою роботи є удосконалення ефективності роботи БСМ за рахунок використання каналів зв'язку підвищеної завадостійкості. Щоб досягти цього необхідно вирішити наступні **завдання:**.

1. Обґрунтування напрямів підвищення завадостійкості БСМ.
2. Аналіз методів модуляції сигналів у БСМ.
3. Використання багатопозиційних сигналів у БСМ.
4. Техніко-економічне обґрунтування прийнятих рішень.

Об'єкт дослідження – процес функціонування сенсорної мережі.

Предмет дослідження – цифрова обробка сигналів.

Метод дослідження – аналітичний.

БЕЗПРОВІДНА СЕНСОРНА МЕРЕЖА

До найбільш поширених варіантів схемо-технічних рішень WSN слід віднести: DASH7, Z-Wave, Insteon, Enocean, ISA100.11a, Wirelesshart, Miwi, 6Lowpan, One-Net, Wavenis, Rubee, Zigbee (Pro).

Основна особливість ZigBee полягає в тому, що при малому енергоспоживанні підтримує не тільки прості топології мережі («точка-точка», «дерево» і «зірка»), а й mesh-топологію з ретрансляцією і маршрутизацією повідомлень. Крім того, специфікація ZigBee (базується на IEEE 802.15.4) містить можливість вибору алгоритму маршрутизації, в залежності від вимог ПЗ та стану мережі.

Вході досліджень встановлено, що для каналів зв'язку WSN властиві наступні ефекти та явища: асиметричність каналів; нестабільність каналів; варіації рівня потужності сигналу на тривалих проміжках часу; непередбачуваність.

Вони мають сильний вплив на роботу всієї мережі в цілому (втрата зв'язку, зниження зв'язності мережі, помилки в локалізації та ін.), а саме головне – впливають на протоколи верхніх рівнів.

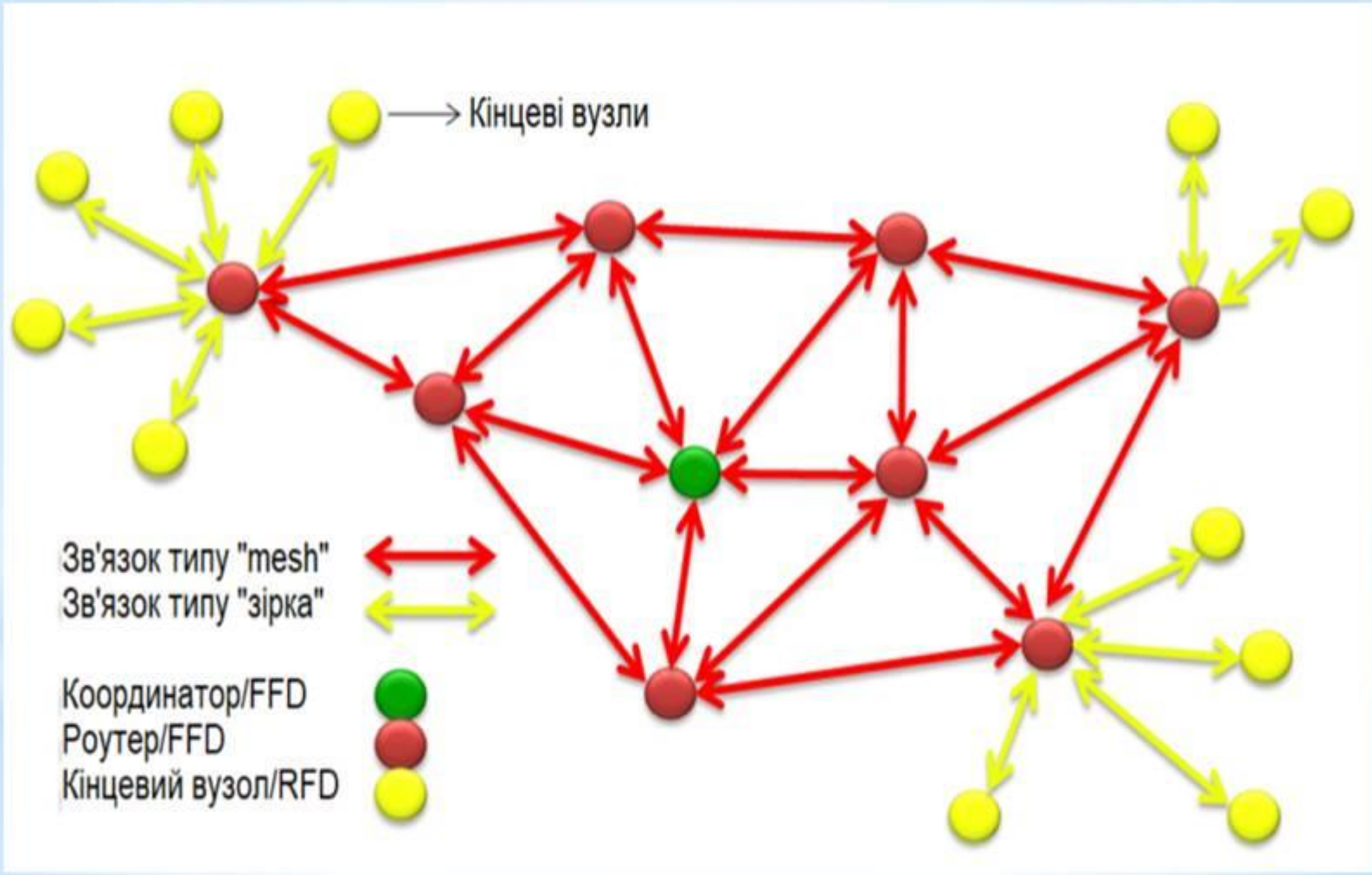
Як наслідок, для захисту WSN доцільно використовувати: механізми резервування транспортного середовища; завадозахищені технології передачі даних на фізичному рівні; впровадження надширокосмугових систем зв’язку (діапазон 3,1÷10,6 ГГц зі смугою пропускання > 500 МГц).

Таким чином, можливо сформувати наступні вимоги до WSN.

1. Стійкість до активних радіозавад.
2. Виявлення підміни вузлів.
3. Наявність резервних маршрутів передачі даних.
4. Виявлення та запобігання спробам реконфігурації мережі, підміни адресної інформації, несанкціонованої «перепрошивки» пристроїв,
5. Стійкість до викривлення та фільтрації кадрів.

Подальші дослідження доцільно спрямувати на підвищення завадостійкості каналів зв’язку WSN.

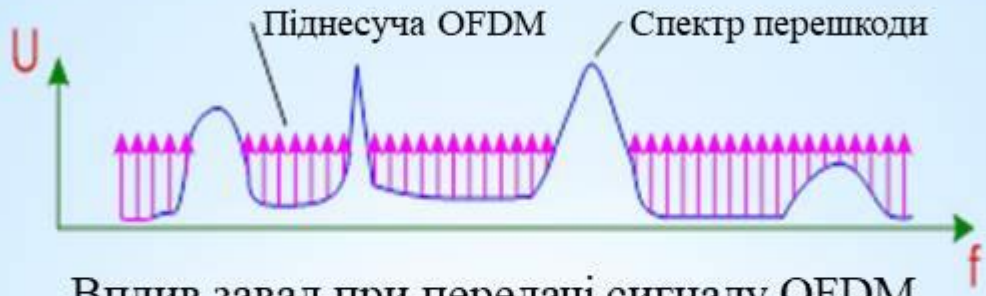
Типова структура мережі



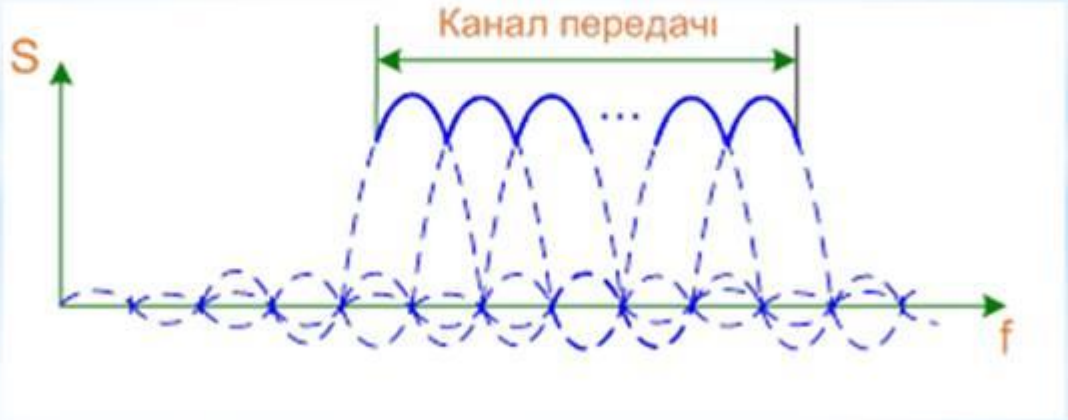
На даний час, в якості пріоритетних шляхів оптимізації БСМ на рівні системи передачі даних слід вказати про використання завадостійкого кодування, сигнально-кодових конструкцій, багатопозиційних сигналів та їх комбінацій.

В свою чергу, заслуговують уваги напрямки, що спираються на впровадження інноваційних технологій, які отримали значне поширення в більше розвинутих мережах, наприклад: 8021.11ac(ax), 5G, MU-MIMO, Massive MIMO та ін.

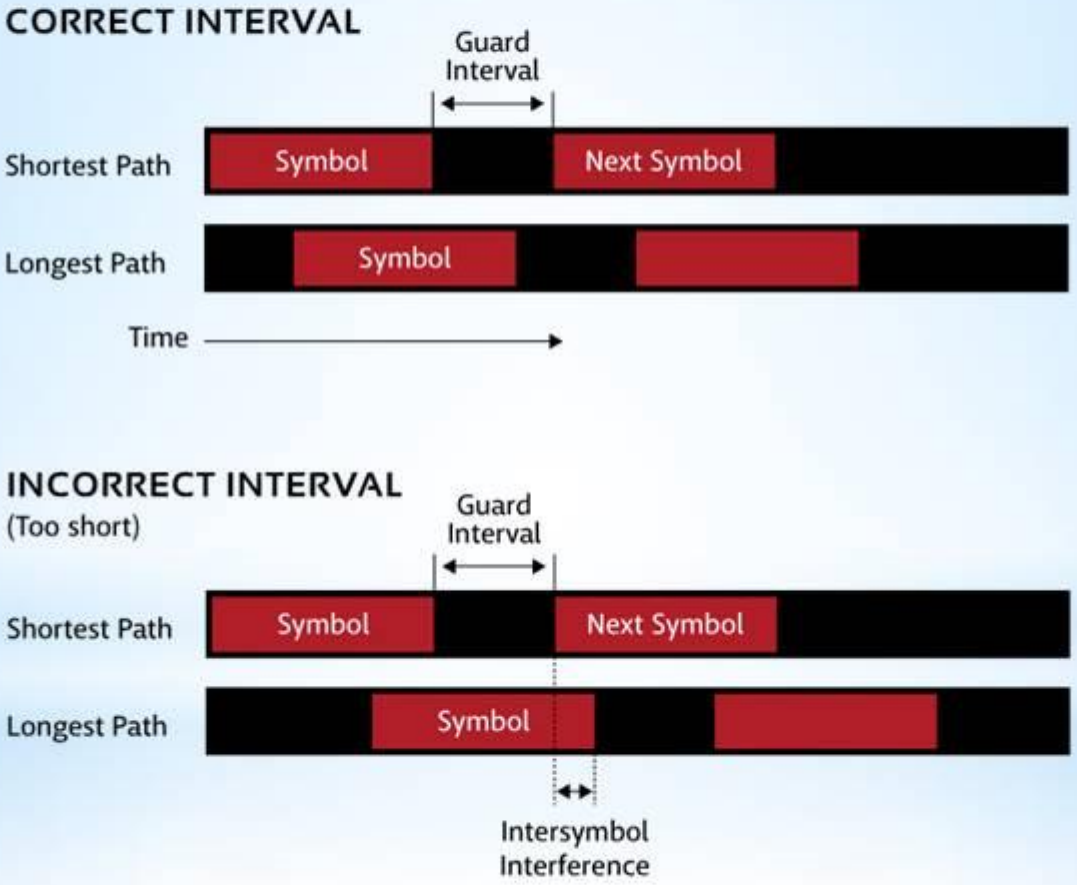
В ході досліджень запропоновано використання кількох варіантів формування багатопозиційних сигналів для радіоканалів БСМ. Замість одиничного сигналу FSK (GFSK) застосовується OFDM-подібний сигнал зі швидкістю передачі даних, яка дорівнює швидкості одного субканалу, що менше в N раз (де N – кількість субканалів, що відведені під передачу корисної інформації) у порівнянні з сигналом класичним для БСМ на основі FSK (GFSK). Підвищення енергетики може відбуватись за рахунок введення надмірності (дубльовані канали) та переваг обробки на приймальній стороні сигналів OFDM. При цьому, з'явилась можливість варіацій вибору між завадостійкістю та спектральною ефективністю радіоканалу БСМ.

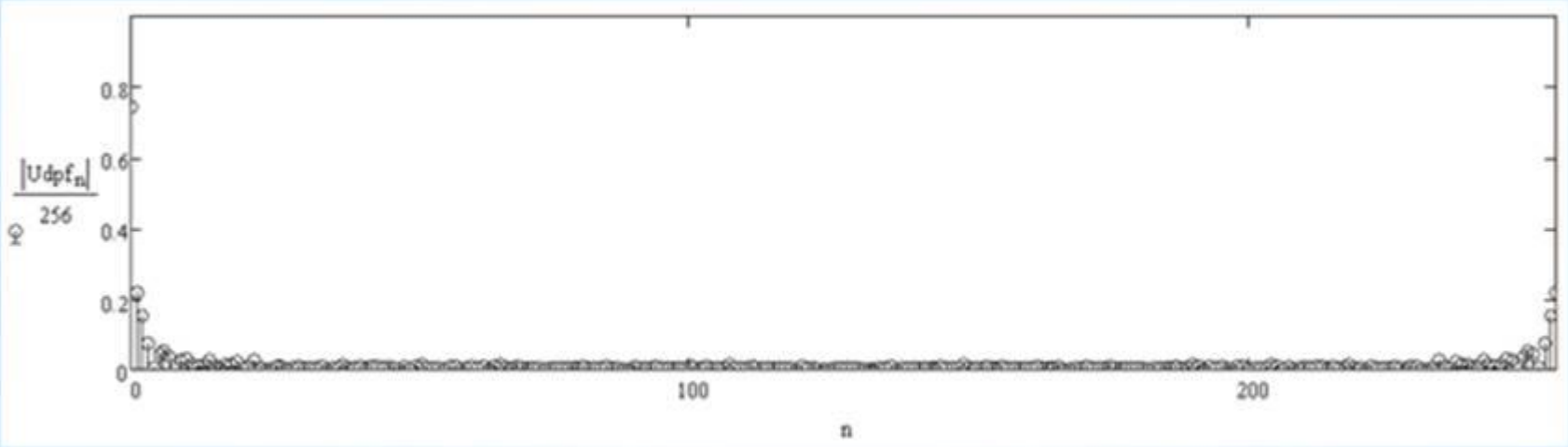


Вплив завад при передачі сигналу OFDM

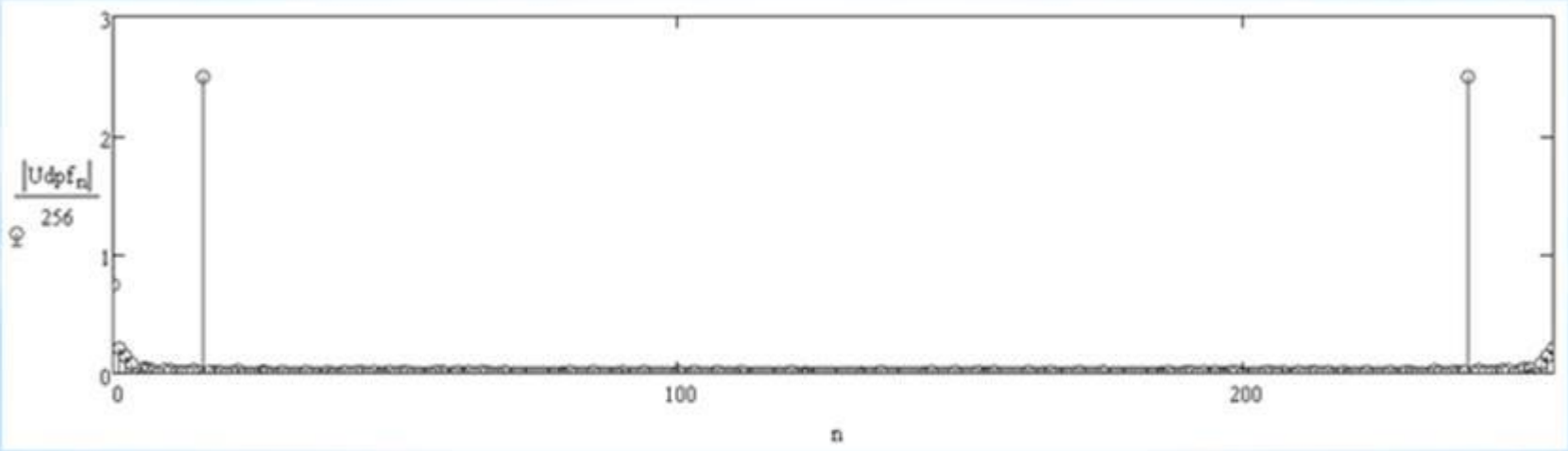


Спектр сигналу OFDM з 6-ма ортогональними піднесучими


CORRECT INTERVAL
Guard Interval
Shortest Path
Symbol
Next Symbol
Longest Path
Symbol
Time
INCORRECT INTERVAL
(Too short)
Guard Interval
Shortest Path
Symbol
Next Symbol
Longest Path
Symbol
Intersymbol Interference



Спектр інформаційного сигналу й адитивного шуму



Спектр інформаційного сигналу, адитивного шуму

та періодичної завади

ВИСНОВОК

Таким чином, результатами дипломної роботи є:

пропозиції щодо використання багатопозиційних сигналів у сенсорних мережах; результати імітаційного моделювання методу спектрального детектування сигналу в умовах впливу вузькосмугової завади. Вони можуть бути використані для подальших досліджень за даною тематикою та при побудові перспективних сенсорних мереж.