ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Удосконалення кіберзахисту безпроводових інформаційно-комунікаційних каналів передачі даних об'єкту інформаційної діяльності»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Юрій ІВАНОВ

Виконав: здобувач вищої освіти групи СЗДМ 61
Юрій ІВАНОВ

Керівник: НІМЧЕНКО Тетяна
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____ _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Іванову Юрію Леонідовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Удосконалення кіберзахисту безпроводових інформаційно-комунікаційних каналів передачі даних об'єкту інформаційної діяльності»
керівник кваліфікаційної роботи НІМЧЕНКО Тетяна, к.т.н., доцент

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: бездротові технології збору та обробки інформації; системи, стандарти та мережі збору та обробки інформації; види, типи, стандарти бездротових систем, їх описи, можливості, переваги та недоліки; опорна локальна бездротова мережа збору та обробки інформації.
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
4.1. Огляд застосування бездротових технологій передачі даних в системах збору інформації;
4.2. Аналіз властивостей стандартів збору та передачі даних в бездротових мережах;
4.3. Дослідження напрямків підвищення ефективності застосування бездротових технологій в системах збору інформації.

5. Перелік графічного матеріалу: ___Презентаційний матеріал на _____слайдах._____

6. Дата видачі завдання_____15.10.2025_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Юрій ІВАНОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Тетьяна НІМЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 76 сторінок, має 22 рисунки, 6 таблиці. Список використаних джерел містить 32 найменування і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності кіберзахисту безпроводових інформаційно-комунікаційних каналів передачі даних об'єкту інформаційної діяльності.

В кваліфікаційній роботі проведено огляд застосування бездротових технологій передачі даних в системах збору інформації. Проаналізовано властивості стандартів збору та передачі даних в бездротових мережах. Досліджено напрямки підвищення ефективності застосування бездротових технологій передачі даних. Розроблено практичні рекомендації щодо вибору технології збору та передачі даних в бездротовій мережі визначеної конфігурації.

Апробація:

Н.О. Струк, М.С. Максимчук, Ю.Л. Іванов, Структура, перелік та зміст конфіденційної інформації комерційної торговельної установи та канали її несанкціонованого доступу. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.36-37. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: БЕЗДРОТОВІ ТЕХНОЛОГІЇ, БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ, ДИСКРЕТНІ ДАНІ, МОДУЛЯЦІЯ, WPAN, WLAN, WMAN, WWAN, WI-FI, IEEE, ТОЧКА ДОСТУПУ, АДАПТЕР, АУТЕНТИФІКАЦІЇ, ШИФРУВАННЯ, WPA2, WARDRIVING, 802.11AC, MU-MIMO

ABSTRACT

The qualification work consists of an introduction, three sections, general conclusions, a list of sources used, the total volume of the work is 76 pages, has 22 figures, 6 tables. The list of sources used contains 32 names and takes up 3 pages.

The purpose of the qualification work is to increase the effectiveness of cyber protection of wireless information and communication channels of data transmission of the object of information activity x.

The qualification work reviews the use of wireless data transmission technologies in information collection systems. The properties of data collection and transmission standards in wireless networks are analyzed. Directions for increasing the effectiveness of the use of wireless data transmission technologies are investigated. Practical recommendations for choosing a technology for data collection and transmission in a wireless network of a certain configuration are developed.

Approbation:

N.O. Struk, M.S. Maksymchuk, Yu.L. Ivanov, Structure, list and content of confidential information of a commercial trading institution and channels of its unauthorized access. All-Ukrainian scientific and practical conference: Current problems of information and communication systems security. Kyiv, November 5, 2025, Kyiv: RVC DUIKT. – 2025. P.36-37. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: WIRELESS TECHNOLOGIES, WIRELESS SENSOR NETWORKS, DISCRETE DATA, MODULATION, WPAN, WLAN, WMAN, WWAN, WI-FI, IEEE, ACCESS POINT, ADAPTER, AUTHENTICATION, ENCRYPTION, WPA2, WARDRIVING, 802.11AC, MU-MIMO

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

IoT	–	(Internet of Things) – Інтернет речей
БД	–	База даних
БСМ	–	Бездротова сенсорна мережа
КМ	–	Комп’ютерна мережа
НСД	–	Несанкціонований доступ
ОС	–	Операційна система
СВ	–	Сенсорний вузол
ПЗМ	–	Пропускна здатність мережі

ВСТУП

Створення мережі збору та управління даними є постійною справою в багатьох наукових галузях та галузях промисловості. Одним із прикладів цього є бездротова мережа передачі даних.

Бездротові технології мають значний потенціал для розвитку, що підвищить стабільність та ефективність країни щодо всіх систем, що, у свою чергу, визначатиме технологічну основу модернізації. Першочерговим завданням під час проектування бездротових локальних мереж є вирішення питань завадостійкості, енергоспоживання та забезпечення відповідної швидкості передачі даних та безпеки.На поточний момент нам доступно безліч бездротових технологій, таких як Wi-Fi, Bluetooth, WiMAX, ZigBee, GPRS, NFC, LTE і т.д. Тема їх критики, оцінки, порівняння та аналізу з метою визначення способів вирішення конкретного технічного завдання зі створення бездротової мережі збору та обробки інформації є значною.

Метою кваліфікаційної роботи є підвищення ефективності кіберзахисту безпроводових інформаційно-комунікаційних каналів передачі даних об’єкту інформаційної діяльності.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

– Проведено огляд застосування бездротових технологій передачі даних в системах збору інформації;

– Проаналізовано властивості стандартів збору та передачі даних в бездротових мережах;

– Досліджено напрямків підвищення ефективності застосування бездротових технологій передачі даних;

– Розроблено практичні рекомендації щодо вибору технології збору та передачі даних в бездротовій локальній мережі збору та обробки інформації.

Об’єкт дослідження. Бездротові технології передачі даних

Предмет дослідження. Бездротова мережа передачі даних в локальній мережі збору та обробки інформації.

Розділ 1.
ОГЛЯД ЗАСТОСУВАННЯ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАННИХ В СИСТЕМАХ ЗБОРУ ІНФОРМАЦІЇ

1.1 Основи процесу передачі інформації в бездротових технологіях

Вважається, що відправною точкою історії бездротових технологій є момент, коли радіосигнал був переданий на відстань наприкінці 19 століття. Після цього, протягом наступного півстоліття, з'явилися такі технології, як частотно-модульоване радіомовлення, бездротові телефони та мережі зв'язку. Таким чином, у 90-х роках бездротові технології стали звичайним явищем у нашому повсякденному житті.

Бездротові технології, фактично, є особливим прикладом інформаційних технологій, який використовується, коли сигнал має бути переданий між двома або більше об'єктами без використання дроту для їх з'єднання. Цей тип передачі використовує різноманітні типи випромінювання, включаючи інфрачервоне, оптичне, лазерне та радіохвилі. Ми зосереджуємося на методі використання радіохвиль, основні ідеї, пов'язані з цим методом, будуть розглянуті нижче [1,2].
Виражаючи сигнал як функцію часу, його можна розділити на два типи: аналоговий та цифровий. Аналоговий сигнал - це фізичний процес, який служить засобом передачі інформації в просторі та часі. У цьому процесі немає пауз або перерв, інакше він вважається сигналом, інтенсивність якого поступово зростає з часом. Цифровий сигнал представлений як серія дискретних значень, що означає, що це сигнал з постійною інтенсивністю певного рівня протягом певного періоду часу, після чого відбувається значна зміна. Приклади аналогових та цифрових сигналів наведено на рис. 1.1.[3]

Періодичний сигнал, який також називають періодичним сигналом, є найпростішою формою сигналу. Прямим прикладом аналогового сигналу є синусоїда, а прямим прикладом цифрового сигналу – меандр, що показано на рис. 1.2.[3]

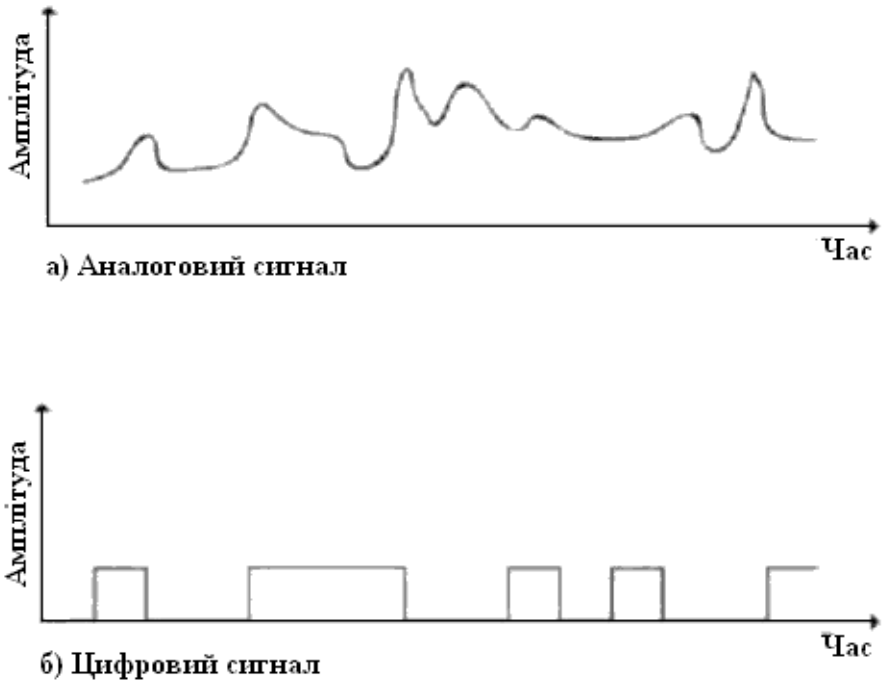


Рис. 1.1 Схематично зображено сигнали:
а) аналоговий, б) цифровий

Математичне визначення: сигнал s (t) є періодично тоді і тільки тоді, коли [2,3]:

$$s(t+T) = s(t), \text{при} -\infty < t < +\infty$$

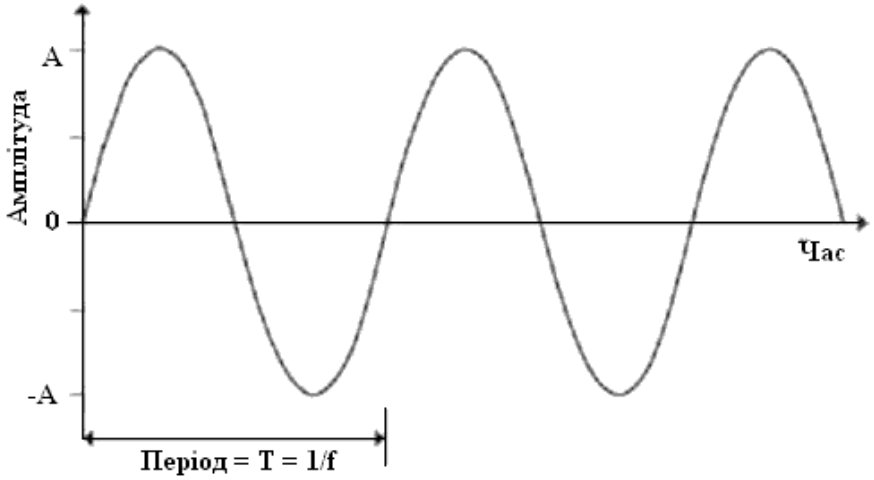
де постійна T є період сигналу.

Первинний аналоговий сигнал вважається синусоїдою. Амплітуда цього сигналу максимальна, а його фаза дорівнює φ, обидві з яких визначаються частотою f та фазою. Частота повторення сигналів є їхньою частотою та вимірюється в герцах. Зрештою, фаза – це різниця в часі між T.

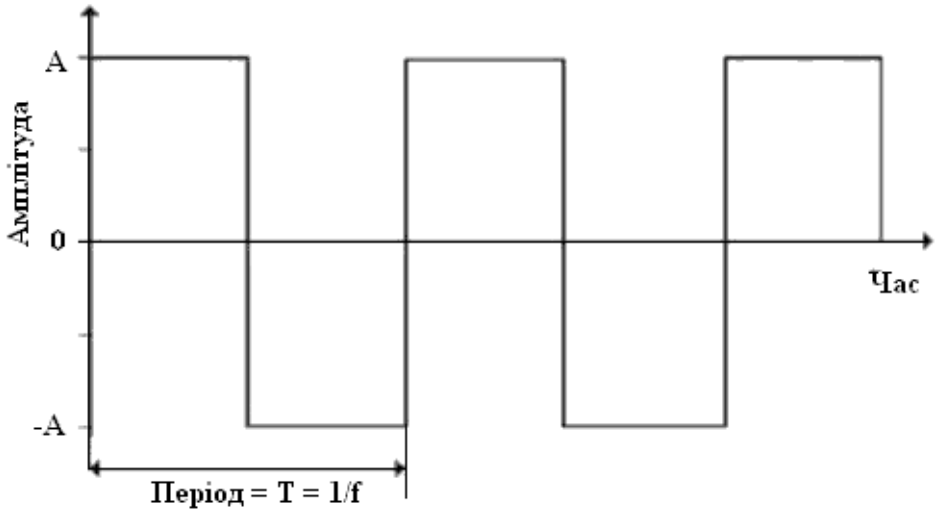
Синусоїдальний сигнал представлений в наступному вигляді [2,3]:

$$s(t) = A\sin(2\pi ft + \varphi).$$

де $\lambda = v\ T$.



а) Синусоїдальний сигнал



б) Прямокутний сигнал

Рис. 1.2 Періодичні сигнали

Два ідентичні сигнали, один записаний у просторі, а інший у часі, пов'язані між собою. Взявши довжину хвилі сигналу за його довжину хвилі, можна припустити, що швидкість поширення сигналу дорівнює v. Тоді період і довжину хвилі можна записати як, що також є співвідношенням [2,3].

Щоб отримати електромагнітний сигнал будь-якої бажаної форми, необхідно застосувати аналіз Фур'є, який є просто процесом об'єднання кількох різних синусоїд з однаковою амплітудою, фазою та частотою. Аналогічно, будь-яку електромагнітну форму хвилі можна перетворити на періодичний аналоговий сигнал.

Діапазон частот, яким визначається певний сигнал, називається його спектром.

Цифровий сигнал можна представити як [3,4]:

$$s(t) = \mathrm{A} \times \frac{4}{\pi} \sum_{k=1,3,5\ldots}^{\infty} \frac{\sin(2\pi k f t)}{k}$$

З цієї точки зору, сигнал, що містить нескінченну кількість частотних компонентів, також має нескінченну смугу пропускання.
З вищесказаного можна зробити такі висновки. Під час передачі сигналу через будь-яке середовище, він обмежений смугою пропускання системи передачі. Крім того, вартість передачі зростає разом зі збільшенням смуги пропускання. Очевидно, що на практиці інформація має бути представлена у вигляді цифрового сигналу з обмеженням смуги пропускання мовлення, однак це призводить до спотворень, що викликає перешкоди та проблеми з прийомом, в результаті чого виникають помилки. У бездротових технологіях використовуються аналогові сигнали (хвилі, що безперервно змінюються) та цифрові дані (текст, числа та графіки). В результаті виникає необхідність модуляції сигналу, що ілюструється передачею низькочастотного аналогового сигналу (голосу) в канал з високочастотної області спектру (телебачення). [1,4].

Під час процесу модуляції використовується одна або декілька властивостей сигналу, ці властивості використовуються для перетворення цифрового сигналу в аналоговий (рис. 1.3) [1,3,4]:

- Фазова модуляція;
- Амплітудна модуляція;
- Частотна модуляція;

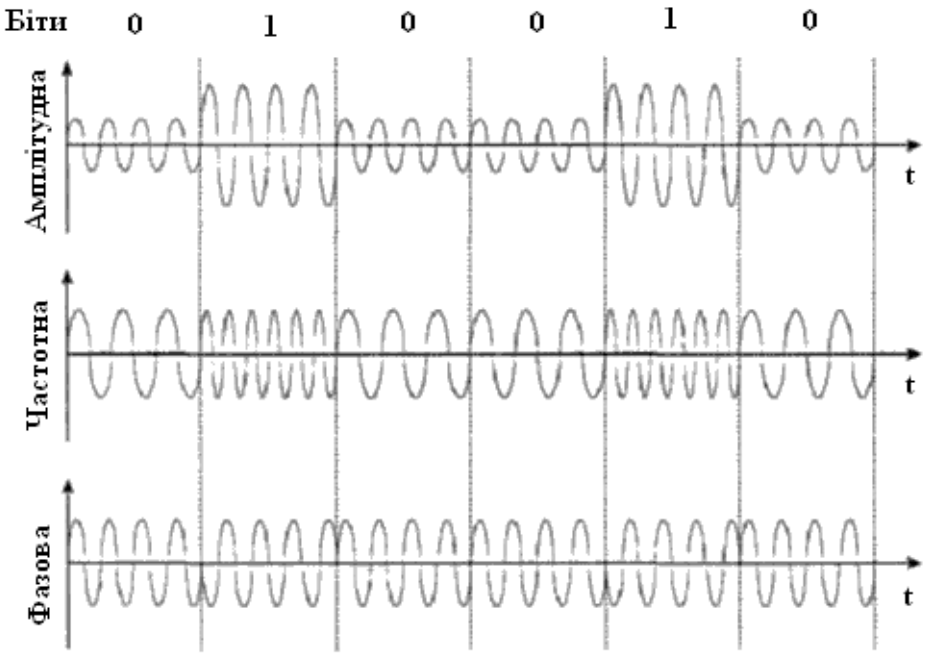


Рис. 1.3 Види модуляції дискретних даних аналоговими сигналами

1.2 Класифікація бездротових технологій

Сьогодні бездротові технології представлені різноманітними технологіями, які в основному поділяються за їхнім цільовим призначенням. Однак існують альтернативні способи їх класифікації на класи [6,7]:
1. Комунікаційна діяльність (рис. 1.4);
Бездротові глобальні мережі (WWAN) – це особливий тип топології.

Бездротові мережі міського масштабу (WMAN);
Бездротові персональні мережі (WPAN);
Бездротові локальні мережі (WLAN);
Операторскі;
Багато точкові;
Корпоративні;
Прямий зв'язок (direct-to-direct);
2. Область застосування

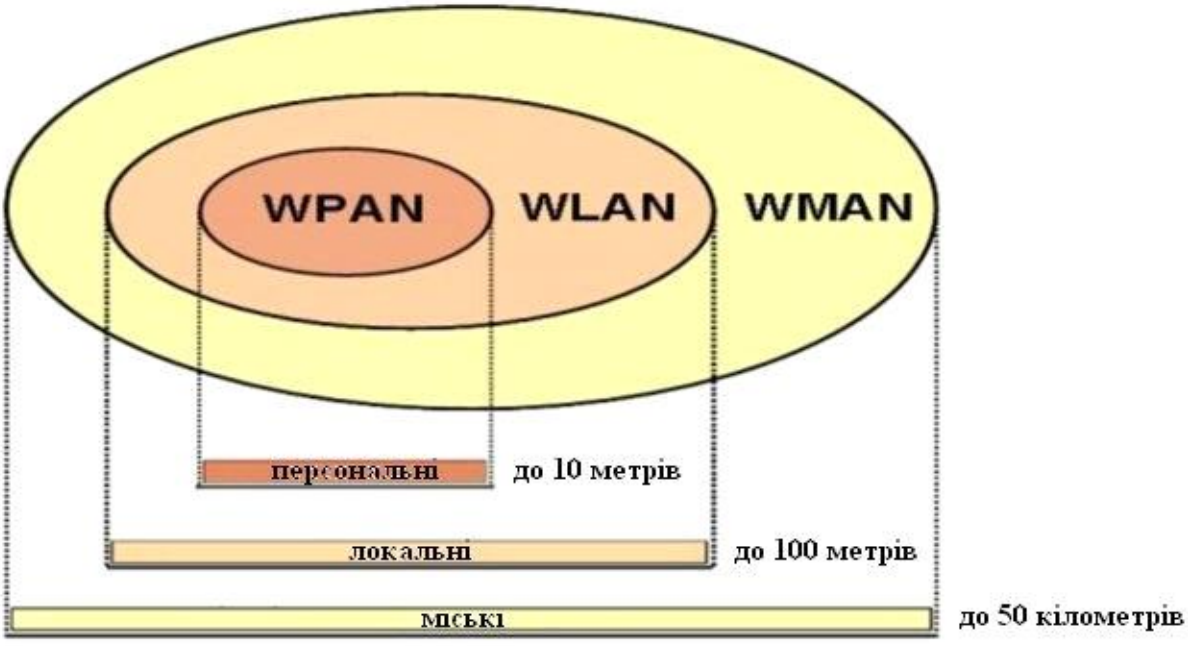


Рисунок 1.4 Радіус дії бездротових мереж

Давайте обговоримо різні типи бездротових технологій детальніше, використовуючи найважливіший приклад, який стосується дальності зв'язку, оскільки це найважливіший аспект.

1.2.1 Бездротові персональні мережі

Бездротові персональні мережі використовуються для підключення різних пристроїв у обмеженому просторі. Команда IEEE охарактеризувала протокол 802.15, який описує принципи, що лежать в основі цього протоколу. Наприклад, зосередимося на технології Bluetooth.
Протокол Bluetooth вирізняється своїми видатними показниками: економічністю, дальністю та швидкістю. Фундаментальна концепція його створення полягає у створенні бюджетного, універсального та надійного радіоінтерфейсу. Ця технологія сприяє зв'язку між великою кількістю пристроїв у різних режимах передачі сигналу, особливо щодо даних та мультимедіа.
Ідея роботи походить від взаємодії радіохвиль. Радіозв'язок відбувається в незаконно володіному діапазоні ISM 2,4-2,483 ГГц. Використовується метод FHSS для перемикання між частотами.

Переваги стандарту [8]:
Низька вартість;
Передавані дані повинні бути захищені.
Стандартизація та сумісність;
Різноманітність та універсальність.

Як негативний аспект можна назвати високе енергоспоживання та низьку швидкість передачі даних.

Сформована область застосування описана в [7,8]:
Комунікаційне обладнання та технологічні засоби;
Доступ та керування віддаленими системами за допомогою телеметрії;
Автомобільна електроніка.

1.2.2 Бездротові локальні мережі.

Бездротові локальні мережі використовуються для підключення різних пристроїв до локальної мережі без необхідності кабельних з'єднань. Команда IEEE, використовуючи протокол 802.11 як приклад, описала типові умови роботи цих пристроїв, які включають понад 20 сертифікатів. Наприклад, зосередимося на найважливішій технології Wi-Fi.
Стандарт 802.11 був розроблений для задоволення потреб створення локальної мережі з кількох комп'ютерів. Кабельні мережі вирізняються вимогою до великої кількості додаткової праці, пов'язаної з встановленням джгутів проводів у межах передбачуваних зон використання. Бездротові мережі Wi-Fi позбавлені цих негативних аспектів. Усі пристрої можна з'єднати, використовуючи мінімальну кількість ресурсів.
Робочі діапазони та методи модуляції відрізняються залежно від використовуваного стандарту.
Переваги технології включають [8,9]:

Компактність;
Високу швидкість передачі;
Дані стандартизовані та сумісні, а також високий рівень організації даних.

Різноманітність компонентів для різних цілей;
Високу швидкість передачі даних.

Недоліками є відносно високе споживання енергії та відсутність захисту від кібератак.
Регіони застосування визначалися властивостями стандарту Wi-Fi.
Комп'ютерне обладнання,
Громадські місця;
промисловість;

• Приватні бездротові мережі;
• Телеметрія та пристрої дистанційного керування.

1.2.3 Бездротові мережі міста

Бездротові міські мережі – це виділена пропускна здатність для доступу до мережі через радіо. Команда IEEE створила стандарт 802.16, який описує необхідні умови для такої взаємодії між пристроями. Наприклад, зосередимося на найважливіших аспектах технології WiMAX.
Розробники завжди боролися з проблемою «останньої милі» (шлях між пристроєм користувача та точкою доступу провайдера). WiMax забезпечує доступ та з'єднує точки Wi-Fi одна з одною, ви можете створювати віддалені точки доступу без обмежень географічним розташуванням, він також забезпечує системи дистанційного моніторингу тощо.
Методи та діапазони варіації суттєво відрізняються залежно від стандартів і будуть перераховані нижче в порівняльній таблиці.
Переваги стандарту [7,8,11]:

Легкість підключення;
Охоплення території;

Мобільність

Якість передачі

Високий ступінь стандартизації;

Гнучкість.

До недоліків належать відсутність підготовки законодавчого органу, брак частот та проблеми з впровадженням технології. Ця технологія в основному використовується для надання послуг організаціям та окремим особам через високошвидкісний доступ до Інтернету.

1.2.4 Бездротові глобальні мережі топологія

Бездротові глобальні мережі (Wireless WAN) – це найновіший стандарт для передачі інформації в бездротовій мережі на високій швидкості, що використовує мобільні телефони та різні пристрої з протоколом LTE.
Цей стандарт був розроблений 3GPPortium і є природним прогресом для операторів стільникового зв'язку в GSM/UMTS. У буквальному перекладі це означає «довгостроковий розвиток». Впровадження нового методу цифрової обробки сигналів та нової форми передачі даних у мобільних мережах сприяло збільшенню швидкості передачі даних [8,10,11].

Частота, на якій працює технологія, становить від 800 МГц до 3,5 ГГц.
Використовуються три різні типи модуляції: QPSK, 16QAM та 64QAM.
Переваги стандарту:
Низька затримка;
Висока швидкість;
Підвищена стабільність;
Доступність.
Недоліками є потенційні відмінності в робочих частотах різних країн.
Технологія LTE в основному використовується для доступу до Інтернету через IP-протокол та стільниковий зв'язок.

Давайте обговоримо важливі аспекти розглянутого матеріалу. Для зручності аналізу та сприйняття інформації основні стандарти сучасних бездротових технологій наведено нижче (Таблиця 1.1).

Таблиця 1.1

Стандарти бездротової передачі даних

Технологія	Стандарт	Область застосування	Пропускна здатність, Мбіт/с	Дальність зв'язку	Модуляція, доступ до середовища	Частотний діапазон, ГГц
Bluetooth	802.15.1	WPAN	до 0,7	до 10 м	FHSS	2,4
	V4.0		до 2.3	до 60 м	ГМСК	2,4
	V5.0		до 5	до 100 м	ФГМСК	2.4
Wi-Fi	802.11g	WLAN	до 54	до 140 м	DQPSK	2,4
	802,1 B		до 300	до 250 м	64QAM	2,4 або 5
	802,1 лак		до 1000	до 500 м	256QAM	5-6
WiMAX	802.16г	WMAN	до 75	до 50 км	OFDM	1,5-11
	802.16е	WWAN	до 40	до 5 км	OFDM	2-13
	802,16м		до 1000	до 100 км	COFDM	2-66
LTE	LTE	WWAN	до 100	до 15 км	OFDM	0,8-3,5
	Розши-рений		до 1000	до 100 км	COFDM	0,8-3,5

Раніше згадувалося, що з розвитком технологій стандарти набувають все більшої популярності та намагаються конкурувати один з одним в одних і тих самих практичних застосуваннях та сегментах ринку. Кожен з них має свої недоліки та переваги. Наразі вибір технології переважно базується на успіху маркетингових кампаній, а не на технічних характеристиках.

1.3. Актуальні стандарти бездротових мереж

Скорочена форма «Wi-FI», що походить від англійського Wireless Fidelity (здатність бездротової передачі), сьогодні є брендом Wi-Fi Alliance, який зазвичай асоціюється з відповідністю певного пристрою специфікаціям цього бренду. Цей скорочений термін був похідний від маркетингової кампанії, спрямованої на збільшення кількості користувачів, як аналог Hi-Fi.
Початок розповіді слід віднести до 1985 року під час офіційного визнання використання діапазонів ISM усіма учасниками. Через шість років голландська компанія першою випустила готовий продукт, який передавав дані бездротовим способом. Технологія називалася WL і використовувалася виключно для підвищення якості касових систем.
Перший міжнародний стандарт передачі інформації був затверджений у 1997 році Інститутом інженерів з електротехніки та електроніки (IEEE). Його номер документації - 802.11 [8,11].
Для налаштування мережі Wi-Fi необхідні як приймачі, так і точки доступу. У виробничому секторі також необхідні бездротові комутатори для керування точками доступу.
Wi-Fi приймач використовується для підключення телефону або комп'ютера до бездротової мережі. Сучасні ноутбуки та мобільні телефони мають компоненти Wi-Fi. Для доступу до мережі адаптер може підключатися як до точки доступу, так і до інших прослуховувачів. У першому сценарії результуюча непряма мережа між вузлами називатиметься Ad Hoc (походить від латинського терміна, що означає «випадок»). У другому сценарії режим називається інфраструктурою.

Точка доступу – це автономний модуль, який функціонує для зв'язку між прослуховувачами та дротовою частиною мережі. Як правило, вона складається з мікрокомп'ютера та приймача-передавача. Серед різних способів роботи точок доступу, поряд з основним режимом, слід виділити бездротовий міст та ретранслятор. У першому сценарії пристрій використовується для об'єднання двох окремих бездротових мереж. У другому режимі пристрій здійснює зв'язок між точками доступу. Доступ до мережі здійснюється через передачу сигналів по радіоканалу.

Бездротові комутатори використовуються, коли необхідне централізоване адміністрування та підтримка точок доступу. Вони пропонують широкий спектр можливостей, включаючи [9,10]:

Керування безпекою;
Спостереження за користувачами;
Керування пропускною здатністю;
забезпечення стабільного прийому даних;
• Балансування навантаження;
Централізоване управління трафіком.
Для діапазону частот 2,4–5 ГГц існує безліч стандартів, пов’язаних із групою IEEE 802.11. Сьогодні три найпоширеніші типи:
802.11g;
802.11n.
802.11ac.
Їхні характеристики наведено нижче (Таблиця 1.2).

Таблиця 1.2

Порівняльна таблиця актуальних стандартів Wi-FI

Стандарт	**802.g**	**802,1 n**	**802,1 ac**
Дальність зв'язку	до 140 м	до 250 м	до 500 м
Ширина каналу	до 20 МГц	до 40 МГц	до 160 МГц
Частотний діапазон	2,4 ГГц	2,4 ГГц або 5 ГГц	5-6 ГГц
Тип модуляції	DQPSK	64QAM	256QAM
Пропускна здатність	до 54 Мбіт/с	до 300 Мбіт/с	до 1000 Мбіт/с
Сумісність	802,11 б/н	802.11 a/b/g	802.11 a/b/g/n
Рік сертифікації	2003 рік	2009 рік	2013 рік

Вперше квадратурний метод модуляції був застосований у стандарті 802.11n, що позитивно вплинуло на пропускну здатність, а також на дальність зв'язку бездротової мережі. Режим передачі 256QAM, що використовується в цифрових передавачах, що вимагають стабільності з точки зору стійкості до перешкод та широкої зони мовлення, використовується у стандарті 802.11ac, цей стандарт визначає вищу швидкість передачі даних.

Важливо визнати, що, незважаючи на ідентичну конструкцію канального рівня, фізичні компоненти бездротових мереж різних стандартів сімейства 802.11 відрізняються. Різноманітність модуляції, кодування та відмінностей у швидкості пояснюється фізичною конструкцією.

У 2003 році був затверджений протокол IEEE 802.11g, цей протокол базується на частотному спектрі 2,4 ГГц. Він описує подібні швидкості передачі, як і 802.11a [9,11,12].

1.3.1 **Стандарт IEEE 802.11g.**

Під час розробки цього стандарту було досягнуто компромісу в галузі схем цифрової модуляції. Він виражається в поєднанні двох технологій: OFDM (ортогональне частотне мультиплексування) та PBCC (згорткове кодування двійкових пакетів). Як результат, основною технологією в стандарті є OFDM, а додатковою - PBCC.

Щодо питання кодування та модуляції сигналів, виникають такі питання [11-14].
По-перше, необхідність підтримки низького рівня сигналу через використання смуги частот ISM. Це досягається за рахунок використання технології розширення спектру, яка фактично зменшує потужність та "затьмарює" передачу спектру по всій смузі.
По-друге, для забезпечення конкурентоспроможності швидкість передачі має бути максимальною, що, у свою чергу, призводить до збільшення ширини спектру, що недопустимо через обмеження ISM.
По-третє, забезпечення високої стійкості до шуму.

Як видно, вищезазначені умови суперечать одна одній, що пояснюється тим, що кодування та модуляція – це спроби знайти золоту середину між, як кажуть, «золотою серединою».

1.3.2 Стандарт IEEE 802.11n

Протокол IEEE 802.11n базується на частотних діапазонах 2,4 ГГц та 5 ГГц. Він підходить для використання з 11b/11a/11g. Сам стандарт був випущений 11 вересня 2009 року. Він описує максимально можливу швидкість передачі до 300 Мбіт/с [11,12].

Основним нововведенням стандарту є використання технології MIMO (рис. 1.5) [11,12], що покращує функції MAC та збільшує ширину каналу.

Технологія MIMO має кілька входів та виходів. Це радіосистеми, які мають велику кількість окремих шляхів для надсилання та отримання інформації, що передбачає наявність щонайменше 4 антен у передавачі та приймачі. Ця технологія дозволяє підвищити ефективність спектру, розширити діапазон частот та значно вищу швидкість передачі даних. Іншими словами, ця технологія дозволяє шифрувати вторинні дані, що також відоме як швидке кодування STC. Простими словами, технологія пояснюється паралельним прийомом високошвидкісного потоку OFDM для певної кількості передач, яка залежить від кількості каналів антени.

Залежно від збільшення кількості антен у пристрої, завадостійкість та якість передачі даних зростатимуть, що в першу чергу пов'язано зі збільшенням кількості просторових каналів. І навпаки, вартість кінцевого пристрою зростає через збільшення складності обробки сигналу.

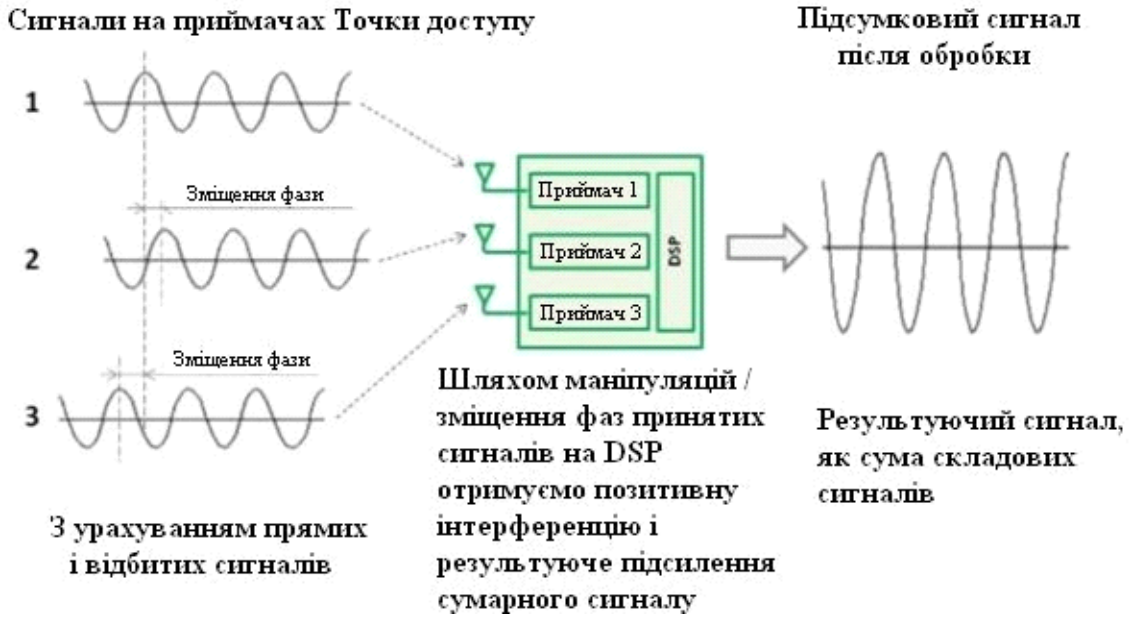


Рис. 1.5 MIMO. MRC - поліпшення сигналу від клієнта до пункту доступу.

1.3.3.Стандарт IEEE 802.11ac

Даний стандарт працює в частотному спектрі 5 - 6 ГГц. Підтримується сумісність з 11b / 11a / 11g / 11n передбачена фізичної архітектурою. Протокол сертифікований 12 жовтня 2013 року. Надає швидкості передачі в теорії при 8 * MU-MIMO до 1 Гбіт / с [13,14].

Основний вплив на поліпшення характеристики зв'язку вплинуло використання двох нових технологій. Beamforming (рис. 1.6) [12] – (дослівно «формування променя») спосіб активної зміни спрямованості несучого сигналу. Обов'язкова для стандарту функція забезпечує максимальну ефективність мовлення, враховуючи локацію користувачів. Так само представлено поліпшення MIMO, а саме MU-MIMO.

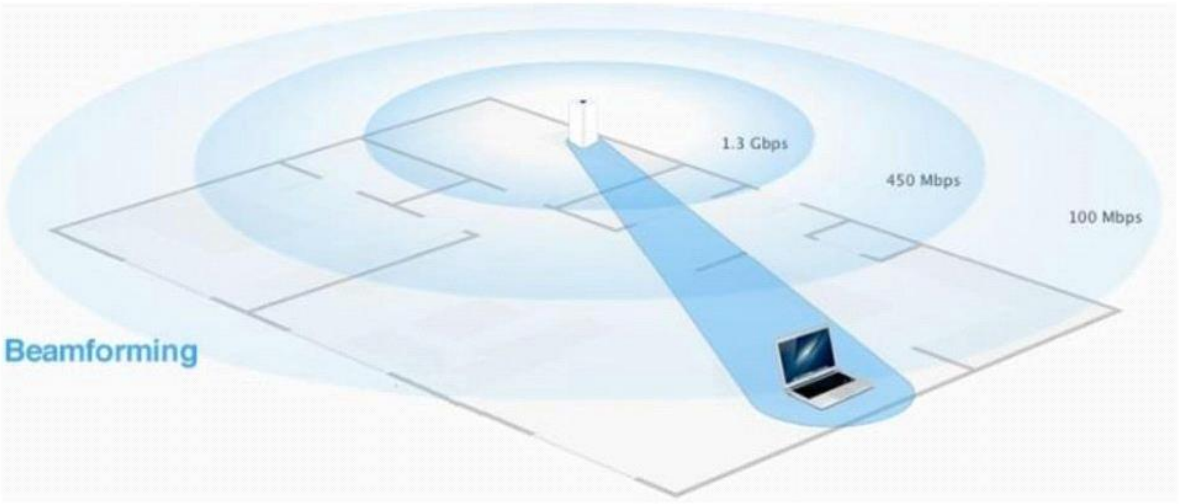


Рис. 1.6 Приклад функціонування технології Beamforming.

1.3.4 MU-MIMO (рис. 1.7) [12,13].

У вищеподаних стандартах призначені для користувача пристрої виявлялися послідовно, що обмежувало кількість фактично використовуваної ємності мережі. Технологія MU-MIMO нівелює цю проблему, дозволяючи робити набагато більше, використовуючи аналогічний доступний спектр [12,14].

Рис. 1.7 Приклад функціонування технології MU-MIMO.

Використовується динамічне групування клієнтів, в якому задіяна функція управління діаграмної спрямованості для можливості паралельної передачі просторово рознесених променів до кожному користувачеві. Для забезпечення роботи технології, функціонал повинен бути доступний на вході і виході з'єднання. Реалізація можлива в двох варіантах: SDMA і Downlink MIMO. У першому випадку використовуються відрізняються просторові потоки для передачі даних відповідним користувачам, у другому ж відбувається процес поділу OFDM даних на безлічі, необхідні для оперативного надання користувачам потрібної кількості піднесуть. Таким чином 802.11ac надає якісну можливість повної реалізації стелі швидкостей для інфраструктур з високим показником кінцевих користувачів.

1.4 Висновки по розділу

1. Подано основи передачі інформації в безпровідних технологіях. Показано, що Бездротові технології - по суті, є окремим випадком інформаційних технологій, який використовується коли необхідно передати сигнал між двома і більше об'єктами, при цьому не використовуючи дроти для їх зв'язку.

2. Визначена класифікація бездротових технологій передачі даних та

подано опис визначених типів.

3. Подано порівняльні характеристики основних стандартів сучасних бездротових технологій та подано їх опис.

Розділ 2 АНАЛІЗ ВЛАСТИВОСТЕЙ БЕЗДРОТОВИХ МЕРЕЖ

2.1 Технологій бездротових сенсорних мереж

Для передачі даних по бездротових мережах для побудови IoT надзвичайно важливі наступні властивості: ефективність при низьких швидкостях роботи, відмовостійкість, адаптивність мережі, можливість самоорганізації.

Таким чином, варто приділити основну увагу технологіям ZigBee, AMT +, Bluetooth LE і IEEE 802.11 ah [14,15].

2.1.1 ZigBee (802.15.4)

Протокол ZigBee є набором розріжених протоколів верхнього рівня, котрі регламентуються стандартом IEEE 802.15.4 [14,15,16].

Варто згадати, що основною особливістю технології ZigBee є те, що при малому енергоспоживанні вона здатна підтримувати не тільки стандартні прості топології мережі, зокрема «точка-точка», «дерево» і «зірка», але і специфічну порожнисту топологію - mesh, яка самоорганізується і самовідновлюється з ретрансляцією і маршрутизацією повідомлень. Також на додачу технологія ZigBee дозволяє вибрати алгоритм маршрутизації, в залежності від вимог додатку і стану мережі, механізм стандартизації додатків – профілі додатків, бібліотека стандартних кластерів, кінцеві точки, прив'язки, гнучкий механізм безпеки. ZigBee забезпечує простоту розгортання, обслуговування і модернізації.

Назва технології навіяна поведінкою бджіл, після повернення їх до вулика [16,17].

2.1.2 Bluetooth LE

Ця технологія була прийнята спеціальною групою користувачів Bluetooth в 2007 р і спочатку отримала назву Bluetooth Ultra-Low-Power, а потім Bluetooth Low Energy (Bluetooth з низьким енергоспоживанням) [10,15]. Мета розробки

даної технології полягала в тому, щоб забезпечити пристроям з обмеженим ресурсом живлення постійне підключення до ВІП сетів Як правило, ВІП сет Bluetooth LE працюють упродовж багатьох років без необхідності заміни батарей. Зазвичай вони використовують плоскі круглі батареї, наприклад, популярні CR2032 [10,15].

Мережа Bluetooth LE відома також як Bluetooth v4.0 і є частиною загальнодоступною специфікації Bluetooth. Пристрої Bluetooth v4.0 не завжди можуть підтримувати інші версії Bluetooth. Однак більшість ВІП сетів Bluetooth від провідних виробників підтримують функціональність як Bluetooth, так і Bluetooth LE [10,15].

2.1.3 ANT +

Це фірмова безпровідна технологія з низьким споживанням, яка працює в діапазоні 2,4 ГГц. Вона була створена у 2004р. компанією Dynastream [10,15,17].

Головним призначенням цієї технології є встановлення зв'язку між давачами. Технологія ANT + використовує протокол ANT і забезпечує функціональну сумісність пристроїв в керованої мережі, що дозволяє об'єднувати всі пристрої ANT + в мережі. Подібно Bluetooth LE пристрої ANT можуть працювати від плоскої круглої батарейки CR2032 роками.

Пристрої ANT+ не підлягають випробуванням на функціональну сумісність, які проводяться для інших стандартних технологій [10,15]

2.1.4 IEEE 802.11ah

Це специфікація одного з набору стандартів зв'язку через бездротову локальну мережеву зону з діапазонами частот 0,9, 2,4, 3,6 і 5 ГГц, що дасть їм можливість інтегруватися в існуючу екосистему Wi-Fi.

Сигнали бездротових мереж IEEE 802.11ah, що передаються в діапазоні 900 МГц, легко проникають через стіни, але не володіють високою пропускною здатністю - швидкість передачі даних при цьому може складати від 100 кбіт / с

до 40 Мбіт / с [10,15]. Технологія подібного роду обіцяє бути корисною для численних давачів і зондів, що розміщуються в житлових будинках і комерційних будівлях. Стандарт 802.11ah може розглядатися як конкурент протоколів IoT Bluetooth LE та ZigBee. Використовувані у промисловості безпровідні пристрої IEEE 802.15.4 можуть працювати від батареї протягом тривалого часу, проте дальність і доступні швидкості передачі даних дуже низькі. Крім того, оскільки швидкості IEEE 802.15.4 недостатні для передачі відеопотоків, IEEE 802.11ah також може бути використаний в цих сценаріях для передачі зображення з камер спостереження [15].

2.2 Область застосування бездротових мереж

IoT є концепцією обчислювальної мережі для фізичних об'єктів (інша назва - «Інтернет речей»), котрі оснащені вбудованими технологіями властиво для взаємодії один з одним чи із зовнішнім середовищем. Тут розглядається організація таких мереж як певне явище, котре може змінити економічні та суспільні процеси, що виключає з частини дій і операцій участь людини [13,18].

У 2008-2009 роках відбувся перехід від так званого «Інтернету людей» до IoT (рис. 2.1) [18], тобто кількість елементів, під’єднаних до мережі, стало більшим, ніж кількість всіх людей, які проживають на нашій планеті.

Рис. 2.1 – Варіанти елементів концепції IoT

Термін IoT вперше був запропонований співробітником Массачусетського технологічного інституту Кевіном Ештоном в 1999 р. В цьому ж році з'явився Центр автоматичної ідентифікації (Auto-ID Center), основним напрямком якого стала радіочастотна ідентифікації RFID і сенсорні технології, завдяки чому ця концепція змогла набути широкого поширення [13,18].

Наступні пристрої з нашого повсякденного середовища можна привести як приклад пристроїв, потенційних для впровадження в світ IoT [13,18]:

- побутова техніка, в тому числі будильники, цифрові камери, домашні аудіо- та акустичні системи;
- кухонна техніка і побутові прилади, в т.ч. холодильники, кавоварки, сушарки, різні світильники, кондиціонери, термостати і посудомийні машини;
- пожежно-охоронні системи управління, такі як детектори диму, пожежні насоси, системи моніторингу для догляду за літніми людьми, камери з давачами руху, домашні охоронні системи, сейфи;
- музичні інструменти;
- роботи;
- товари для фітнесу і здоров'я: пристрої, що стежать за фазами сну, крокоміри, датчики ваги, кров'яного тиску та інших параметрів [13].

Цю концепцію, як правило, пов'язують з розвитком БСМ.

В даний час знаходиться на підйомі розвиток технології БСМ (рис. 2.2) [18].

БСМ – це розподілена мережа, що самоорганізується, стійка до виходу з ладу окремих елементів і здатна обмінюватися інформацією по бездротовому з'єднанню [11,13].

Кожен елемент такої мережі володіє автономним джерелом живлення, також передавачем / приймачем та мікрокомп’ютером. Зона охоплення становить від кількох метрів до декількох кілометрів, в залежності від антени і типу модуля, також через можливість передачі повідомлень від одного

елемента до іншого. Зв'язок між будь-якими двома кінцевими точками може здійснюватися через ретранслятор (в тих випадках, коли радіус охоплення цих пристроїв не допускає їх взаємного виявлення).

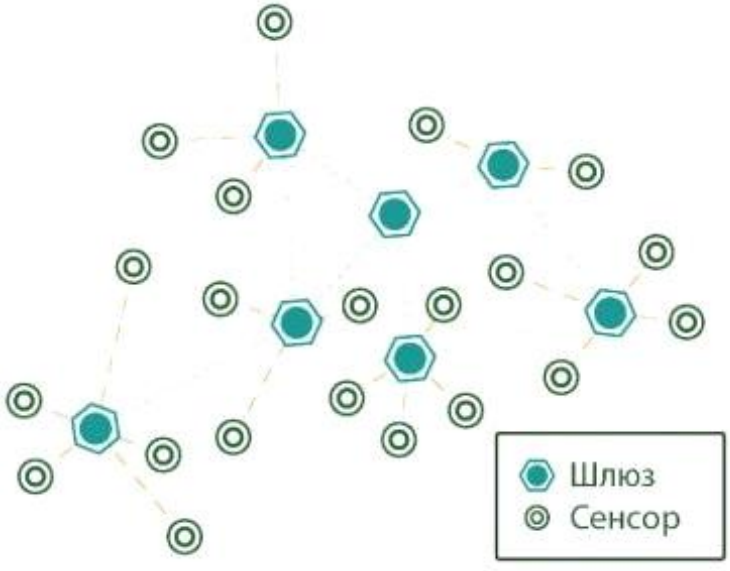


Рис. 2.2 – Бездротова сенсорна мережа

Отже, пристрої з невеликим радіусом можуть взаємодіяти один з одним з використанням ретрансляторів. Як правило, БСМ використовується для збору даних з пристроїв, оснащених давачами температури, освітлення, вологості, тобто, мають відношення до моніторингу. Наприклад, мініатюрні датчики можуть бути використані в медицині для моніторингу стану пацієнта. Пристрій, який пацієнт носить з собою, може контролювати роботу життєво важливих органів, у випадку небезпеки, повідомити лікаря про проблему [13,18].

Невеликий розмір пристроїв дозволяє провести не тільки поверхневий огляд пацієнта, а й досліджувати внутрішні органи. Так, наприклад, під час гастроскопії в державних лікарнях і клініках використовують спеціальні апарати з гастроскопічною трубкою, яку не всі пацієнти можуть проковтнути. Сьогодні на ринку для проведення таких досліджень вже існують спеціалізовані пристрої в формі таблеток (рис. 2.3). Ці пристрої мають запас автономного живлення, достатній для безперервної роботи впродовж 24 годин, в тому числі, відправки показів іншого пристрою, який пацієнт упродовж цього

часу носить з собою. Після цього у лікаря буде можливість проаналізувати результат і поставити діагноз [18].

Рисунок 2.3 – Гастроскопічна капсула

Сенсори можуть використовуватися для контролю за автоматичним ввімкненням світла, коли людина входить в кімнату, для управління будь-якими пристроями системи «Розумний будинок» (рис. 2.4) (включення кондиціонера, обігріву підлоги ін.) [13].

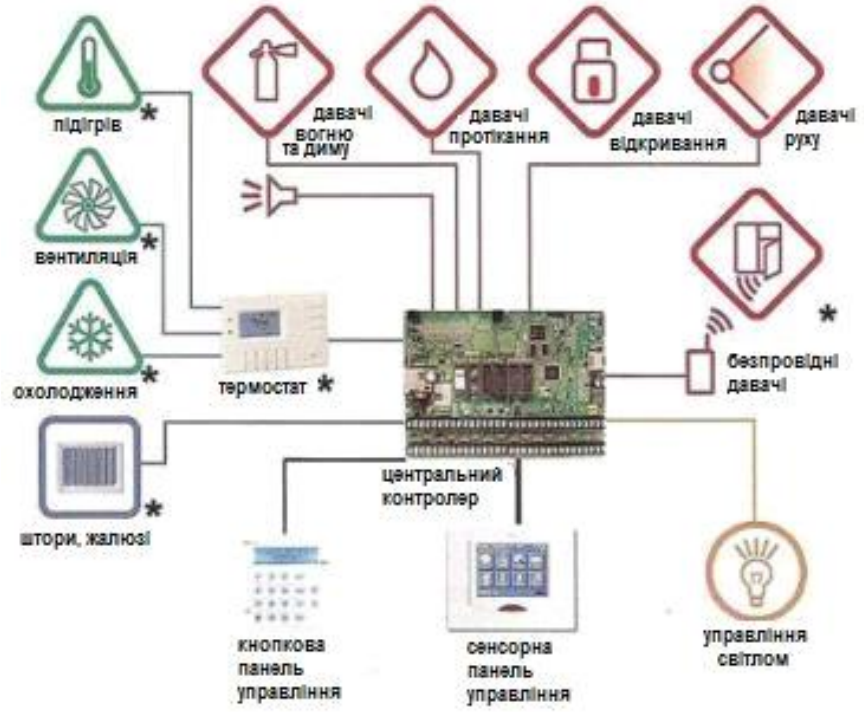


Рисунок 2.4 – Типова схема системи «розумний будинок»

Іноді необхідно контролювати рухливість або пошкодження будь-яких об'єктів, де проблематично прокладати кабель. Для цього, знову-таки,

вигідніше використовувати сенсорні мережі, оскільки давачі оснащені автономними блоками живлення є бездротовими.

Крім того, технологія бездротового зв'язку у сенсорній мережі може бути використана для передачі аудіо даних - в системі внутрішнього домофонного зв'язку, в мультимедійній системі з низьким енергоспоживанням [13,18].

Основна проблема концепції IoT сьогодні - це відсутність стандартів в цій галузі, що призводить до утруднення інтеграції існуючих на ринку рішень і перешкоджає появі нових.

На додачу до питань про стандарти, є й інші потенційні перешкоди на шляху до IoT. Серед них - розміри створюваної інфраструктури, і необхідні для збору інформації та аналізу пристроїв категорії IoT сервера збереження та обробки даних. Є також деякі політичні та законодавчі обмеження, нормативні акти, які призводять до уповільнення розвитку концепції, в тому числі підвищеної уваги до контролю конфіденційності персональних даних [13,18].

2.3 Продуктивність мережі

Її можна виміряти, використовуючи кілька показників, ПЗМ буде одним з таких показників. Вона відображає кількість інформації, яка може бути передана в мережі за певну часову одиницю [5,6].

Як одиниці для вимірювання використовуються, як правило, пакети (кадри) чи біти. Отже, ПЗМ визначається в бітах за секунду або ж в пакетах за секунду.

Виконання вимірювання ПЗМ в бітах за секунду дозволяє точнішу оцінку для швидкості передачі інформації, на відміну від застосування пакетів.

У всіх протоколах присутній заголовок, котрий містить службову інформацію, а також поле даних, де наявна користувацька інформація. Зокрема, в мінімальному кадрі для стандартного протоколу Ethernet поле даних має розмір 46 байтів, а решту з 64 байт відіграють роль службової інформації. При вимірі ПЗМ в пакетах за секунду, відсутня можливість

відділити службову інформацію від користувацької, в той час як при побітовому вимірюванні це є можливим [5,6].

Для тестування ПЗМ його простіше провести на прикладному рівні.

Досить заміряти час передачі файлу визначеного розміру між клієнтом та сервером і поділити розмір на витрачений час. Для того, щоб виміряти загальну ПЗМ мережі необхідно використовувати спеціалізовані інструменти, зокрема аналізатори протоколів або RMOM- і SNMP-агенти, які входять до складу ОС, різне комунікаційне обладнання або спеціальні мережеві адаптери [5,6].

ПЗМ також може вимірюватися через дві будь-які двома чи вузли мережі. В цьому випадку, отримане значення ПЗМ буде змінюватися в відповідно до того, між якими вузлами будуть проводитися вимірювання при однакових мережевих умовах. Так як в мережі зазвичай одночасно знаходиться велика кількість ПК і серверів, тому повну характеристику ПЗМ мережі дасть набір ПЗМ, заміряних для різних комбінацій взаємодіючих між собою ПК - це так звані матриці трафіку вузлів мережі. Також існують спеціалізовані програмні засоби вимірювання, котрі можуть побудувати таку матрицю для кожної точки мережі [5,7].

Оскільки дані в КМ при проходженні шляху до точки призначення, як правило, мають декілька транзитних етапів, тоді як критерій ефективності варто брати пропускну здатність стосовно кожного окремого вузла мережі - деякого визначеного сегменту чи каналу, або і пристрою [5,7].

Властиво знання загальної ПЗМ між двома точками комп’ютерної мережі не в змозі надати всієї інформації щодо можливих методів її підвищення через те, що із показників неможливо зрозуміти, власне котра з проміжних стадій обробки пакетів максимально заважає роботі мережі. Таким чином, дані щодо пропускної здатності окремих вузлів мережі будуть корисними для прийняття рішень щодо її можливої оптимізації [5,7].

2.4 Надійність мережі

Важливо мати уявлення про кілька аспектів, які власне і визначають поняття надійності. Зокрема для технічних пристроїв, показниками надійності є такі: інтенсивність відмов, середній час напрацювання на відмову, імовірність відмови. Проте, ці показники корисні лише для оцінки надійності, як правило, простих елементів та пристроїв, що перебувають у одному із двох станів одночасно - працездатному і непрацездатному. Реальні складні системи, які складаються з безлічі пристроїв і елементів, на додачу до згаданих станів мають додаткові проміжні стани, що не враховуються цими характеристиками. Тому для коректної оцінки надійності реальних складних систем використовується інший набір атрибутів [5,7].

В їх числі є коефіцієнт готовності або, власне, готовність - показує частку визначеного часу, упродовж якого може початися використання система. Ця характеристика може покращитися через введення до складу системи надлишковості: деякі ключові елементи дублюються в декількох екземплярах, з тією метою, щоб при виході з ладу одного них, інші зможуть забезпечити якісну роботу всієї системи [3,5].

Високонадійна система повинна, принаймні, мати високий ступінь готовності, але цього недостатньо. Також потрібен захист даних від спотворень та їх коректне збереження. Крім того, повинна бути наявною узгодженість (несуперечливість) даних [5,7].

Так як КМ заснована на механізмі передачі пакетів інформації власне між кінцевими точками, тому імовірність доставки вузла призначення пакетів без спотворень є однією з характерних властивостей надійності. Також поряд з цим показником можуть бути використані і інші характеристики: ймовірність втрати пакетів (без відносно до її причини – через відсутність шляху до власне працездатного призначення, через різну контрольну суму, через переповненість буфера маршрутизатора і т.д.), можливість спотворення окремих бітів даних, коефіцієнт, який визначається відношенням пакетів, які доставлені, до

втрачених [5,7].

Іншою характеристикою загальної надійності мережі є відмовостійкість. В даному випадку, це здатність системи приховувати відмови окремих елементів від користувача. Наприклад, в разі, коли копія таблиці БД є одночасно збереженою на кількох серверах, користувач може не помітити реальну відмову одного з них. Так у відмовостійкої системи поломка одного з її елементів може привести до несуттєвого зниження якості роботи системи (деградації), але в жодному разі не призведе до повної її зупинки. Так, якщо один з файлових серверів вийде з ладу, збільшиться тільки справжній час доступу до БД завдяки зменшенню ступеня розпаралелювання виконуваних запитів, проте в загальному система буде здатна коректно працювати [5,7].

Ще однією ознакою загальної надійності мережі є її безпека. Фактично, це здатність самої системи захистити від НСД дані. Це набагато складніше зробити у розподіленій системі, ніж у централізованій. Мережеві повідомлення передаються, зазвичай, по лініях зв'язку, які часто проходять через спільний простір, в якому можуть бути обладнані засоби для проведення прослуховування ліній. Залишені без нагляду ПК також можуть стати слабким місцем. Крім цього, завжди існує ймовірна небезпека виконання злому захисту від неавторизованих користувачів в випадках, коли КМ має доступ до глобальних мереж загального користування [5,7].

2.5 Забезпечення безпеки технологій Wi-Fi

2.5.1 Історія розвитку.

Група 802.11 дуже швидко набрала широку аудиторію користувачів, за рахунок високої якості і зручності технологій. Тим самим викликавши підвищений інтерес в середовищі кіберзлочинів, таких як крадіжка даних і неузгоджені підключення.

Спочатку спосіб збереження інформації в таких мережах отримав назву WEP, іншими словами «Конфіденційність, аналогічна кабельному з'єднанню».

Вже з визначення малося на увазі, що буде говоритися не про дійсно хорошому рівні безпеки, а приблизно про таке ж рівні захисту, що забезпечує кабельний Ethernet. Де вся інформація транслюється у відкритому вигляді, але для доступу до них сторонніх осіб потрібні різні навички поводження з пристроями і протоколами. І також, як умільці легко отримують доступ до Ethernet для шпигунства, так і фахівці в короткі терміни зламали WEP в 2001 році. Криптоаналітики показали, що зловмисники, які мають малими ресурсами, здатні отримати доступ в мережу за одну-дві години. Отже, WEP надавала захист лише від випадково підключається до мережі сторонніх, а серйозним атакуючим групам не було ніякого діла до факту активації шифрування [19].

Пізніше IEEE формує групу 802.11i і ставить перед нею план: замінити WEP на щось більш суттєве і сумісне з уже існуючими пристроями. У підсумку ця група розробила два окремих способи: одне, так би мовити, з оглядкою назад, а інше - спрямоване в майбутнє. З огляду на продані пристрої, члени 802.11i домоглися того, щоб все вже вироблені на фабриках Wi - Fi - пристрої були сумісні з новою системою захисту TKIP [19,20].

TKIP була сумісна зі старими Wi - Fi картами - через установку оновлення прошивки. Ясно це зробили в найпершу чергу, і в 2003 році TKIP був частиною нового методу Wi - Fi - захисту, який отримав назву WPA. Більш того група 802.11i винайшла WPA2 - можний спосіб для наступних версій Wi-Fi, - погодивши в комплекті алгоритм на основі AES з довгим ключем і новим режимом роботи. Цей режим по іншому називається CCMP [19,20].

Коли завершилися роботи над винаходом, Wi-Fi Alliance опублікувало нову версію стандарту - WPA2. Так WPA мав на увазі лише шифрування TKIP, а WPA2 необхідне узгодження обох алгоритмів, TKIP і AES. З березня 2006 року Wi-Fi Alliance зробив підтримку WPA2 обов'язкової для всіх сертифікованих Wi-Fi-пристроїв [19,20].

Проте, певна безліч вразливостей, загальних у WPA і WPA2, залишають лазівки для зломщиків. Наприклад PSK.

Приземлений режим використання ключів (PSK) знайшов широке застосування приватників і невеликих організацій, де незручно і не прийнято управляти безліччю ключів з використанням серверів аутентифікації 802.1x. При PSK всі Wi-Fi- пристрої шифрує мережевий трафік за допомогою 256-бітного ключа. Цей ключ можна представляти у вигляді з 64 шістнадцяткових цифр, або як фразу з символів ASCII довжиною від 8 до 63 знаків. Якщо використовується код ASCII, то 256 біт ключа дістаються з пароля з використанням тривіальної криптографічного функції PBKDF2, яка застосовує до шифру ідентифікатор мережі SSID і проводить 4096 бітових «кеш-перетворень». На жаль, навіть при таких способах режим PSK часто виявляється недостатнім для словникових атак перебором паролів 24 - якщо, звичайно, користувач застосовує слабку парольний фразу. Слабкість ключа на основі фіксованого пароля очевидна для будь-якої криптосистеми і виправляється за допомогою вибору довгих і менш передбачуваних фраз [19,20]..

Менш помітною і тому більш вразливою виглядає наступна вроджена вразливість WPA2. А саме: зробивши криптоалгоритм TKIP в складі WPA і WPA2 сумісним з приймачами, супроводжуються давно зламаний WEP, Альянс Wi - Fi таким чином допустив, діру, яку з часом вдається збільшити для проведення серйозних нападів. Знайдена в TKIP слабкість укладена в роботі контрольних сум [19,20].

У мережі Wi-Fi, де при транслюванні високий випадок втрати біта, для виявлення помилок застосовують контрольні суми. Якщо склад пакета змінився, а сама контрольна сума не змінилася, то пакет підроблено. Хакери винайшли спосіб, який дає змогу змінювати дані в пакетах та знаходити нову контрольну суму для них, таким чином підроблений пакет видають за справжній. У своїх працях Тьюз та Бек застосували один з таких інструментів, так званий, Chopchop. Ця програма і стала відправною точкою для розширення атаки на WPA [19,20].

Тепер, щоб запобігти тривіальну атаку Chopchop, клієнт реагує відразу ж,

як тільки отримує дві невірні контрольні суми MIC в інтервалі 60 секунд. У відповідь на цю підозрілу подію клієнт відключається на одну хвилину, а потім вимагає повторення обміну ключами з точкою доступу. Точка доступу при виявленні аналогічній ситуації теж відключається на 60 секунд, а потім генерує нові ключі для кожного зі своїх клієнтів. В стандарті 802.11i допускається, щоб нові майстер-ключі створювалися за запитом без зміни початкової парольної фрази або мережевого ключа.

Ще один можливий спосіб: «отруєння ARP» дозволяє аналізувати весь трафік внутрішньої мережі компанії і знаходити будь-яку інформацію, в тому числі логіни-паролі (проте в такому випадку потрібен інсайдер з монітором трафіку).

Протокол WPA2 з кодуванням на основі криптоалгоритму AES є обов'язковим у всіх Wi-Fi-пристроях, починаючи з 2006 року і на сьогоднішній день, не показав нічого схожого на подібні уразливості. Тому для забезпечення належного рівня захисту рекомендується виставляти такі настройки безпеки мережі [19,20]:

- Назва SSID має бути унікальним для виключення злому способом словникового перебору;
- В якості методу аутентифікації вибирати режим WPA2-PSK;
- Методом шифрування вказувати AES;

Перераховані критерії забезпечують найбільш високий рівень безпеки від злому.

2.5.2 Механізм аутентифікації WPA2

WPA2 - це програма сертифікації бездротового зв'язку. Перевагами WPA є підвищений захист даних та контроль бездротових мереж. Суттєвою особливістю є сумісність безлічі бездротових пристроїв на апаратному та на програмному рівнях. Низький рівень безпеки, безсумнівно, довго залишався головних недоліком мережі W-Fi [19,20].

Перші БЛВС, реалізовані на технології VPN, надавали безпеку даних на

рівні 3, що залишало слабкість мережі IP для погроз. Здійснений на рівні 2 протокол WPA2 оберігає бездротову мережу набагато краще. Однак лише він один не здатний надати потрібний рівень безпеки корпоративної мережі. Управління ж доступом за цим протоколом в поєднанні з реалізованим протоколом аутентифікації IEEE 802.1X на портах, дає змогу зменшити безліч проблем захисту [19,20].

Протокол WEP був уразливим для атак і погано реалізовувався виробниками. У зв'язку з цим він так і не знайшов масового використання в корпоративних мережах. Слабкі місця WEP і те, що їх досить просто реалізувати в незаконних цілях, сприяли розробці стандарту 802.11i, який був сертифікований в 2004 р. Організація Wi-Fi Alliance розробила протокол WPA, в рамках проекту стандарту 802.11i, що забезпечує набагато вищий рівень безпеки, а ніж попередня версія WPA. Наявність множинних ротацій ключів і лічильника пакетів прибирають можливість атаки з відтворенням пакетів або їх повторним введенням. контроль цілісності даних, забезпечує протокол WPA, використовуючи метод 29. Даний метод зазнає атак «Brute-Force», але при цьому передача трафіку за хвилину автоматично регенерується і, якщо точка доступу заснована на WPA знаходить протягом 60с. більше однієї помилки MIC то сеансові ключі переставляються, зменшуючи, ризик атак до мінімуму. Тим часом протокол WPA2 задіє новий метод кодування, заснований на більш сильному, алгоритмі шифрування AES, ніж RC4. WPA і WPA2 мають 2 режими аутентифікації [19,20]:

- корпоративному (Enterprise);
- персональному (Personal).

У персональному режимі WPA2 із парольної фрази введеної відкритим текстом, генерується 256-розрядний ключ., Ідентифікатор SSID та ключ PSK і довжина останнього разом визначають математичний базис для створення головного парного ключа PMK, який потрібен для ініціалізації чотиристороннього квантування зв'язку та генерації сеансового ключа PTK, для взаємодії клієнтського пристрою з точкою доступу. Протоколу WPA2-Personal

має проблеми підтримки ключів і розподілу, тому його використовують в невеликих офісах, ніж у промисловості. Можливі параметри безпеки приведені в таблиці 2.2. [20].

Таблиця 2.1

Таблиця можливих параметрів безпеки

Властивості	**Статичний WEP**	**Динамічний WEP**	**WPA**	**WPA2 (для підприємств)**
Авторизація	Общий ключ	EAP	EAP , загальний ключ	EAP , загальний ключ
Шифрування	Стат-ий ключ	Сесс-ый ключ	TKП>	CCMP (AES)
Алгоритм	RC4	RC4	RC4	AES
Розподіл ключів	Одноразове,вручну	РМК	Виробниче від РМК	Виробниче від РМК
Вектор ініціалізації	Текст, 24 біта	Текст, 24 біта	Розширений вектор, 65 біт	48 біт номер пакета (PN)
Довжина ключа	64/128	64/128	128	256
Інфраструктура	немає	Радіус	Радіус	Радіус
Цілісність	32-розрядна ICV	32-розрядна ICV	64-розрядна MIC	ЕПТ / CBC

Протокол WPA2-Enterprise добре усуває проблеми з розподілом статичних ключів та адміністрування цих ключів. Інтеграція даного протоколу з багатьма корпоративними сервісами аутентифікації дає змогу здійснювати контроль доступу на базі облікових записів.

Аутентифікація відбувається між робочою станцією і центральним сервером аутентифікації. Точка доступу або бездротового контролер здійснюють моніторинг з'єднання. Стандарт 802.1X служить базою для режиму WPA2-Enterprise. До основних компонентів аутентифікації 802.1X відносяться клієнтський запит, аутентифікатор і сервер аутентифікації. Згідно зі специфікацією 802.1X, призначений для користувача запит вважається пристрій, що вимагає доступ до мережі. Зазвичай під запитом мається на увазі ноутбук або будь-яке інше мобільний пристрій. На перевірку клієнтським запитом в кінцевому рахунку виявляється встановлене на цьому пристрої ПО, ініціалізує і відповідає на команди 802.1X (рисунок 2.5) [19,20].

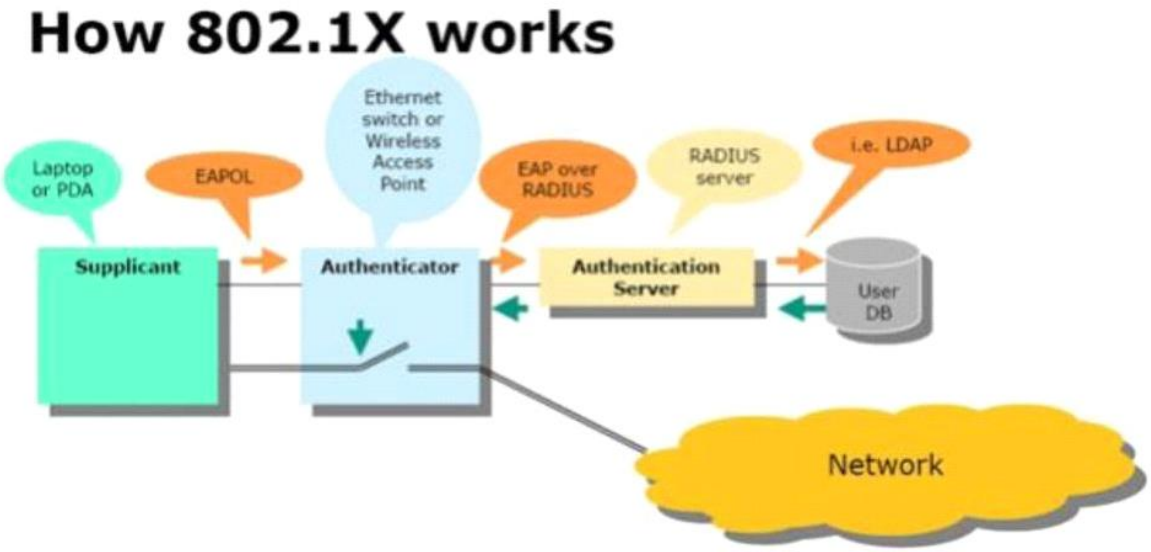


Рис. 2.5 Схема роботи 802.1x

Аутентифікатор (часто це точка доступу, але в централізованій архітектурі доступу він може розташовуватися на комутаторі / контролері) аутентифікує клієнт для доступу до мережі. Це пристрій визначає запити від клієнтського запиту, залишаючи мережевий інтерфейс закритим до тих пір, поки не отримає від сервера аутентифікації наказ на його відкриття. В свою чергу, останній приймає та обробляє запит на аутентифікацію. Хоча зазвичай в якості сервера аутентифікації використовується сервер RADIUS, в даній ситуації можна використовувати не всякий такий сервер, а лише той, що сумісний з методами аутентифікації. Клієнт і точка доступу змінюються трафіком EAP по протоколу рівня 2 EAPoL. Клієнтський запит не може спілкуватися з сервером RADIUS за допомогою протоколу рівня 3: коли точка доступу отримує трафік EAP від клієнта, вона переформовувалися його в відповідний запит RADIUS і передає серверу RADIUS на виконання (рисунок 2.6) [19,20].

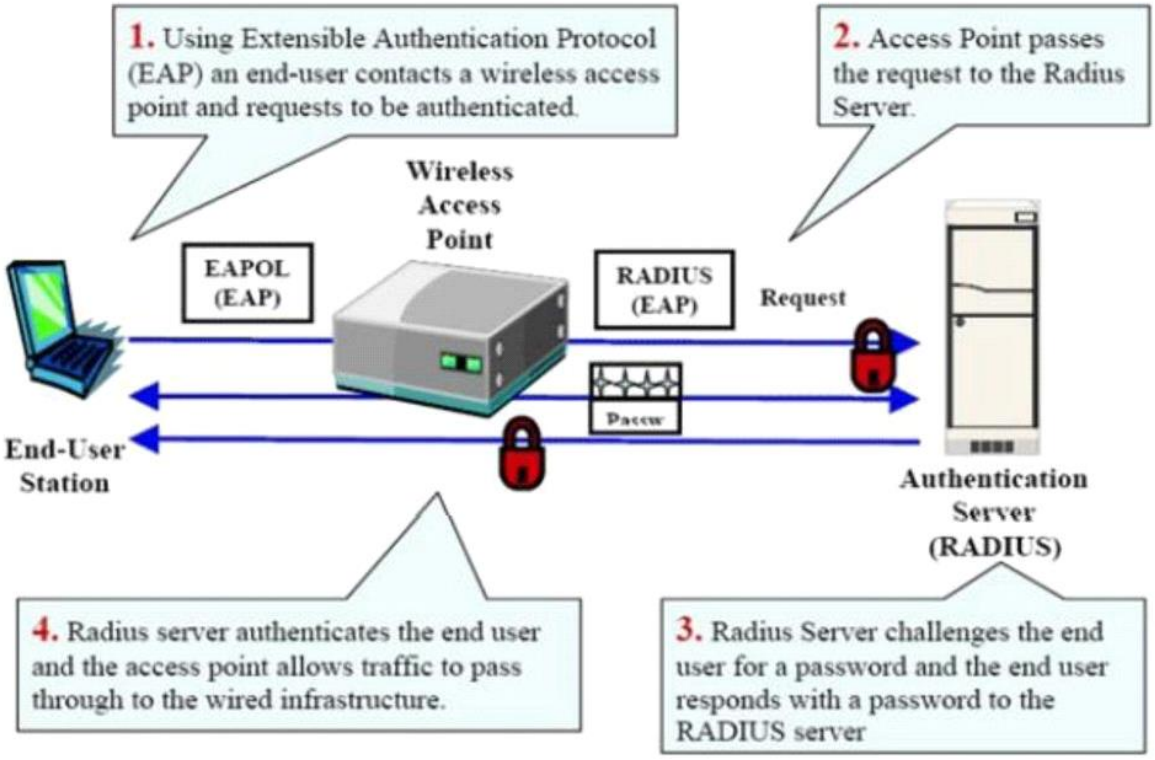


Рис. 2.6 Процедура аутентифікації

Протокол EAP є контейнерним, отже, фактично механізм авторизації виповнюється внутрішніми протоколами. Сьогодні найбільшу кількість застосувань налічують наступні [19,20]:

- EAP-FAST - дозволяє проводити аутентифікацію за логіном-паролем, трансльованого всередині TLS тунелю між отправщіком і RADIUS-сервером;
- EAP-FAST EAP-TLS - використовує інфраструктуру відкритих ключів (PKI) для аутентифікації користувача і сервера (отправщіка і RADIUS-сервера) через сертифікати, видані довіреним підтверджуючий центр (CA). Вимагає видачі та 32 установки клієнтських сертифікатів на кожен пристрій, тому підходить тільки для керованої корпоративного середовища;
- EAP-TTLS - схожий з EAP-TLS, але при налагодженні тунелю не потрібен клієнтський сертифікат. В такому тунелі, аналогічному SSL-з'єднання браузера, відбувається повторна авторизація;

• PEAP-MSCHAPv2 - схожий на EAP-TTLS в питанні первинного налагодження шифрованого TLS тунелю між користувачем і сервером, що вимагає серверного сертифіката. Далі в такому тунелі здійснюється аутентифікація по протоколу MSCHAPv2;

Архітектура EAP-кадру представлена нижче (рис 2.7) [19,20].

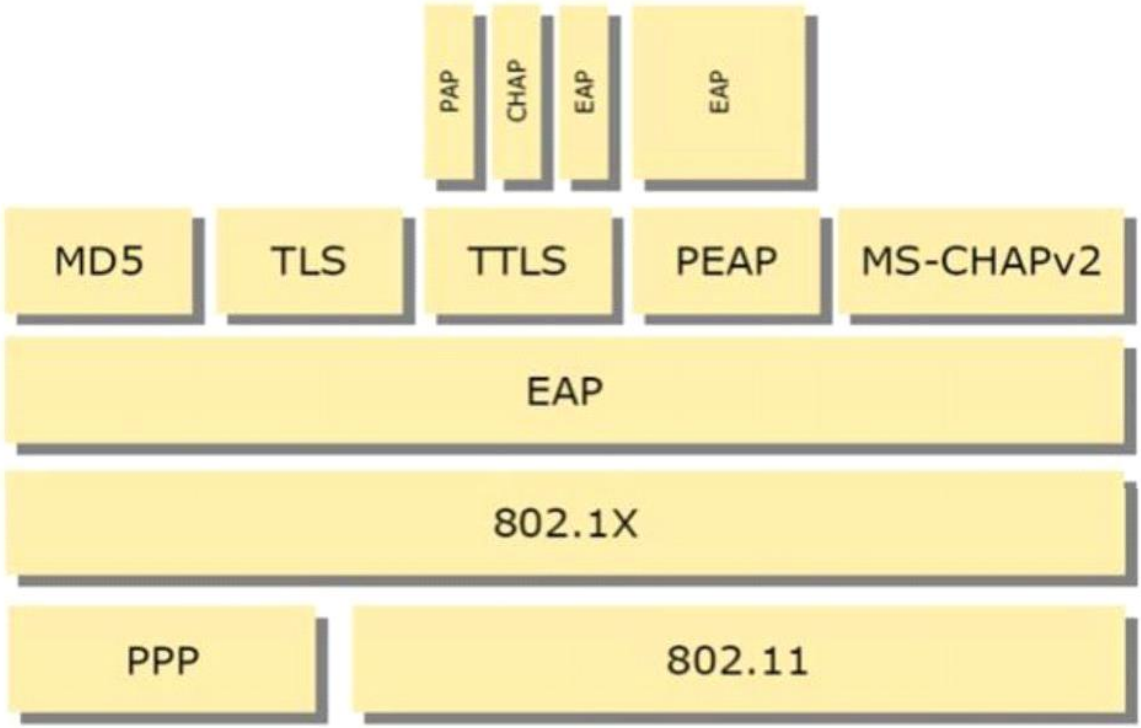


Рис. 2.7 Архітектура EAP кадру.

Виконавши процедуру аутентифікації 802.1X, користувач отримує від сервера аутентифікації головний ключ, який «приєднується» до поточного сеансу аутентифікації. На основі цього ключа на клієнті і на сервері аутентифікації створюється один і той же парний головний ключ PMK. Аутентифікатор отримує ключ PMK від сервера аутентифікації через попередньо визначеного атрибута 33 RADIUS. Володіючи ключем PMK, клієнт і точка доступу відтворюють парний тимчасовий ключ PTK, практично не обмінюючись ім. Така процедура генерації ключів здійсненна через використання чотиристоронього квантування зв'язку, що запобігає вчинення атак, спрямованих на перехоплення службової інформації.

WPA2 має 3 типи ключів PTK [19,20]:

- ключ підтвердження ключа KCK, що застосовується для перевірки цілісності кадру EAPOL-Key;
- ключ шифрування ключа KEK, потрібний для шифрування групового тимчасового ключа GTK;
- тимчасові ключі TK - для шифрування трафіку.

Всі «приєднані» до точки доступу бездротові пристрої повинні «вміти» розшифровувати широкомовний і багатоадресний трафік. Вони роблять це за допомогою одного і того ж тимчасового групового ключа GTK. Якщо точка доступу змінює ключ GTK - то вона виробляє новий ключ, використовуючи просте двостороннє квантування зв'язку і ключ KEK для шифрування ключа GTK.

При здійсненні клієнтським пристроєм роумінгу між двома точками доступу повний процес його аутентифікації сервером RADIUS може займати сотні мілісекунд (а то і кілька секунд), що є неприйнятним для телефонів Wi-Fi або потокових додатків ноутбуків. Тому безліч корпоративних бездротових пристроїв оснащуються такими передбаченими специфікацією 802.11i функціями, як попередня аутентифікація і кешування ключа PMK, що дозволяють мінімізувати пов'язану з роумінгом затримку. Попередня аутентифікація дозволяє мобільному клієнту аутентифицироваться на інший, розташованої поблизу точки доступу, перебуваючи «прив'язаним» до своєї первинної точки доступу. При використанні кешування PMK користувачеві, возвратившемуся з обслуговується роумінгом території - назад, не обов'язково повторне проходження авторизації 802.1X [19,20].

2.5.3 Механізм шифрування WPA2

Протокол WPA2 здійснюється на базі шифрування AES. Потребує апаратної підтримки та характеризується необхідністю величезного обсягу обчислень, які іноді відсутній в старому обладнанні. Для авторизації і підтримки цілісності даних WPA2 застосовує протокол CBC-MAC, а для

шифрування даних - режим лічильника CTR.

Повідомлення (MIC) коду цілісності протоколу WPA2 є контрольною сумою і на відміну від WEP і WPA надає цілісність даних для заголовка 802.11. Це дозволяє усунути нападу типу «Packet replay» з метою розшифровки пакетів або компрометації криптографічного інформації. Для розрахунку MIC використовується 128-розрядний вектор ініціалізації IV, для шифрування IV - метод AES і часовий ключ, а на виході маємо 128 розрядний підсумок [19,20].

Після над цим підсумком і наступними 128 бітами даних проводиться операція «виключне АБО». За допомогою AES і TK шифрується її результат, а потім над останнім результатом і наступними 128 бітами даних знову виконується операція - виключає АБО. Процедура повторюється до вичерпання всій корисного навантаження. Створені на самому останньому кроці результату, перші 64 розряду, потрібні для знаходження значення MIC.

Для шифрування MIC та даних використовується алгоритм який базуються на режимі лічильника. Як і при шифруванні вектора ініціалізації MIC, виконання такого алгоритму бере початок з завантаження 128-розрядного лічильника, де замість значення відповідного довжині даних береться значення лічильника, в поле лічильника рівного одиниці. Слідчо, для кодування кожного пакета використовується свій лічильник.

Використовуючи AES і TK шифруються перші 128 біт даних, а тоді понад 128-біт, де результатом шифрування виступає операція - включення АБО. Перші 128 біт даних дають перший 128-розрядний зашифрований блок. Процедура повторюється до повного шифрування всього 128-розрядного блоку даних. Після цього остаточне значення в полі лічильника скидається в нуль. Результат останньої операції приєднується до зашифрованого кадру. Після підрахунку MIC з використанням протоколу CBC-MAC проводиться шифрування даних і MIC. Після до цієї інформації спочатку приєднується заголовок 802.11 і поле номера пакета CCMP, пристиковується «кінцевик» 802.11 і все це разом відправляється за адресою призначення [19,20].

Розшифровка даних виконується в зворотному шифрування порядку. Для

вилучення лічильника задіюється той же алгоритм, що і при його шифруванні. Для дешифрування лічильника і зашифрованою частини корисного навантаження використовується базуються на режимі лічильника алгоритм декодування і ключ ТК. Результатом цього процесу є розшифровані дані і контрольна сума MIC. Нарешті, за допомогою алгоритму CBC-MAC, провадиться перерахунок MIC для розшифрованих даних. Якщо значення MIC не збігаються, то пакет скидається. При проходженні процедур порівняння зазначених значень, розшифровані дані йдуть в мережевий стек, а потім користувачеві.

2.5.4 Процедура пошуку і злому уразливих точок доступу бездротових мереж (Wardriving)

«Wardriving» - процедура пошуку і злому уразливих точок доступу бездротових мереж Wi-Fi індивідом або групою людей, забезпечених ноутбуком з Wi-Fi-адаптером і мають певний набір програмного забезпечення. Завдання «Wardriving» - під'єднатися до бездротової мережі з різними цілями, починаючи від безкоштовного користування інтернет з'єднанням - до корпоративного шпигунства. Потрібно згадати те - що такий злом може здійснюватися на дуже великій відстані і людина, що здійснює даний злом - може сховатися. Пошук точок доступу відбувається наступним чином: злочинець встановлює на свій ноутбук будь-який мережевий аналізатор - наприклад, InSSIDer - заходить в будь-якої транспорт і їздить по місту, в свою чергу InSSIDer пов'язаний з GPS модулем. Як результат - хакер отримує точки доступу з їх зразковим розташуванням, далі - вже йдучи на поводу особистих інтересів, локалізує потрібну точку доступу для атаки [19,20].

Для перехоплення пакетів існує спеціальний режим моніторингу (Monitor Mode). Іноді, для переведення пристрою в такий режим, необхідно встановити в систему спеціальні драйвери, які пишуться під чіп конкретного виробника.

Режим пасивного сканування також не є ліками, так наприклад програма Wellenreter здатна проводити пасивне сканування після впізнання бездротової

картки ESSID підміняє наступним: «Thiisuseduntwellenreter», а MAC-адресу змінює на будь-який. На цьому етапі, зловмисникові потрібно роздобути певну кількість пакетів, що транслюються в цій мережі, а коли це буде виконано - вже в спокійній обстановці - за допомогою програми-зломщика отримати потрібний ключ. Для цих цілей найчастіше використовується «Aircrack-ng» [19,20].

«Aircrack-ng» - це набір програм для виявлення бездротових мереж, та перехоплення даних через бездротові мережі WEP і WPA / WPA2-PSK.

2.5.4 Додаток InSSIDer

«InSSIDer» - безкоштовний додаток, здатний здійснювати діагностику Wi- Fi-мереж і моніторинг завантаженості бездротових каналів [20].

За допомогою цієї утиліти ви можете подивитися список всіх знайдених мобільних мереж і дізнатися потужність сигналу, MAC-адресу точки доступу, виробника пристрої, що використовуються канали, ідентифікатор SSID, силу сигналу, ступінь захищеності, швидкість і завантаженість мережі і багато іншого. Потужність сигналу можна побачити за допомогою наочних графіків в режимі реального часу. При використанні програми ви зможете заміряти рівень сигналу в різних приміщеннях у себе вдома або в офісі. Після цього можна вибрати найбільш вільний канал з максимальною швидкістю і мінімальними перешкодами.

В утиліті добре реалізовані можливості по сортуванню результатів сканування мереж.

2.6 Висновки по розділу

1. Подано описи основних технологій, що застосовуються для формування бездротових сенсорних мереж передачі данних. А саме, стандарти :ZigBee, AMT+, Bluetooth LE і IEEE 802.11 ah.

2. Визначено області застосування бездротових мереж та подано їх описи. А саме: IoT - «Інтернет речей»), бездротова сенсорна мережа, «Розумний

будинок».

3. Визначена продуктивність та надійність бездротових мереж. Подано описи вказаних характеристик.

4. Визначені питання забезпечення безпеки технологій Wi-Fi. Подано механізм аутентифікації WPA2 та параметри безпеки мережі. Описано механізм шифрування WPA2 та процедура пошуку і злому уразливих точок доступу бездротових мереж Wi-Fi (Wellenreter), в тому числі, за допомогою утиліти InSSIDer.

Розділ 3 ДОСЛІДЖЕННЯ НАПРЯМКІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ

3.1 Обґрунтування вибору технологій передачі даних

Для кращого розуміння зведемо основні характеристики розглянутих технологій (ZigBee, ANT +, Bluetooth LE, IEEE 802.11ah) в таблицю 3.1. У ній відображені параметри пропускної здатності (Кбіт / с), часу очікування (мс), пікового струму споживання (мА), частоти (ГГц) і дальності дії (м).

Таблиця 3.1

Основні характеристики бездротових технологій передачі даних

	Пропускна здатність	Час очікування	Піковий струм спожив	Частота	Дальність дії
ZigBee	20 - 250	10	30	0,868 - 2,4	70
ANT +	20	1,5	60	2,4	30
Bluetooth LE	305	2,5	12,5	2,4	100
IEEE 802.11ah	100 - 40000	1,5	116	0,9	100 - 1000

Побудуємо на основі таблиці порівняльні діаграми (рисунки 3.1 - 3.4), які наглядно відображають рішення, які є лідерами в тій чи іншій порівняльній характеристиці.

Як видно з діаграм, технологія ANT + поступається конкурентам за параметрами дальності і пропускної здатності, маючи досить невеликі переваги в часі готовності і піковому струмі споживання. Технологія IEEE 802.11ah обіцяє надати вкрай високі (на тлі конкурентів) показники дальності і пропускної здатності, але, в той же час, є найбільш енерговитратною.

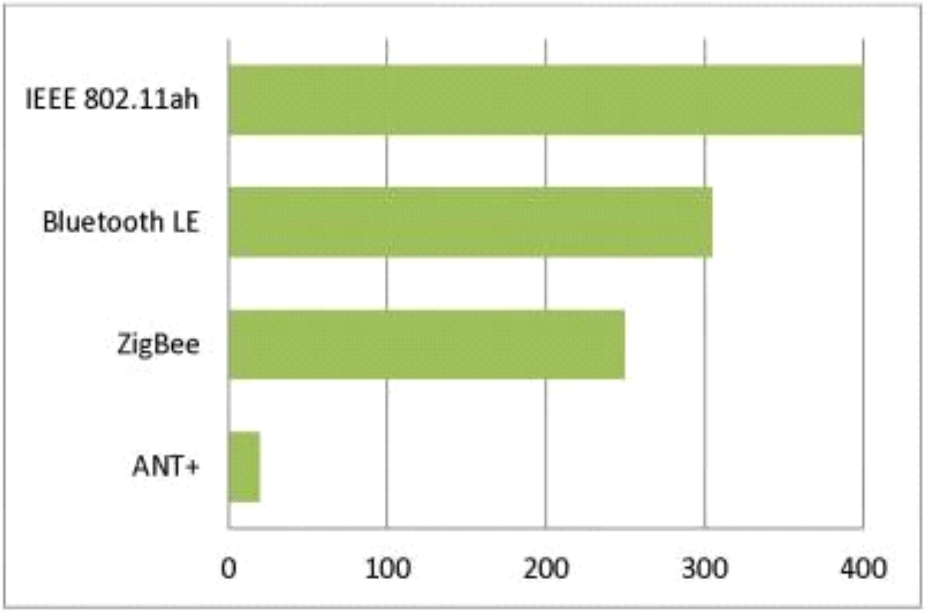


Рис. 3.1 – Пропускна здатність, Кбіт/с

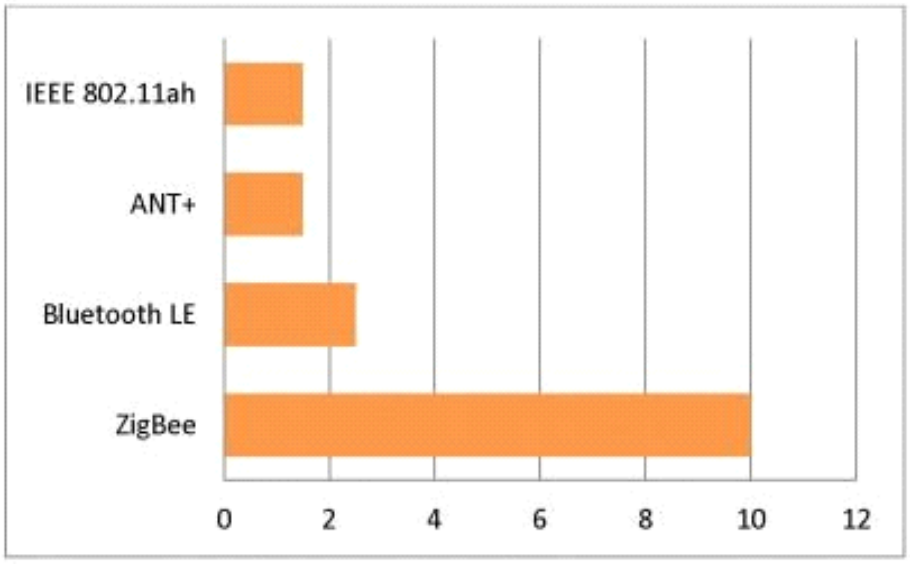


Рис. 3.2 – Час очікування, мс

Можна бачити, що технології Bluetooth LE та 802.15.4 (ZigBee) за своїми характеристикам досить близькі за значенням, і є найбільш привабливими технологіями серед розглянутих.

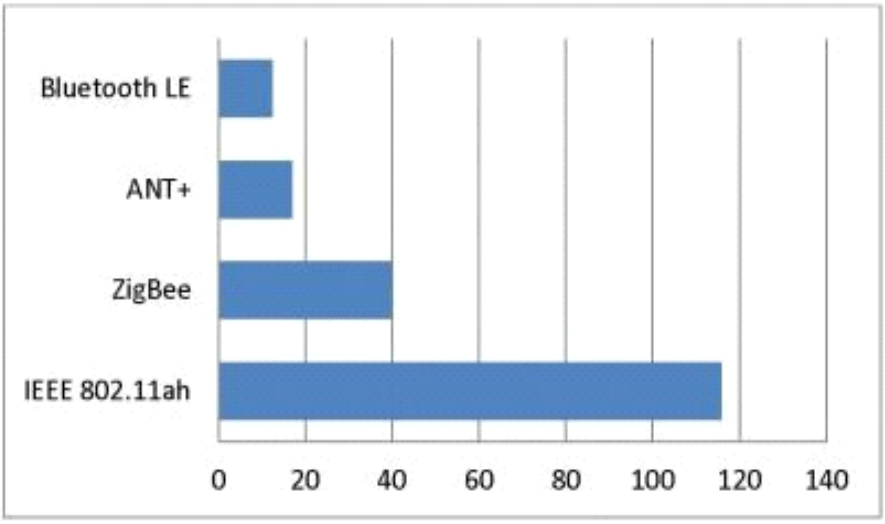


Рис. 3.3 – Піковий струм споживання, мА

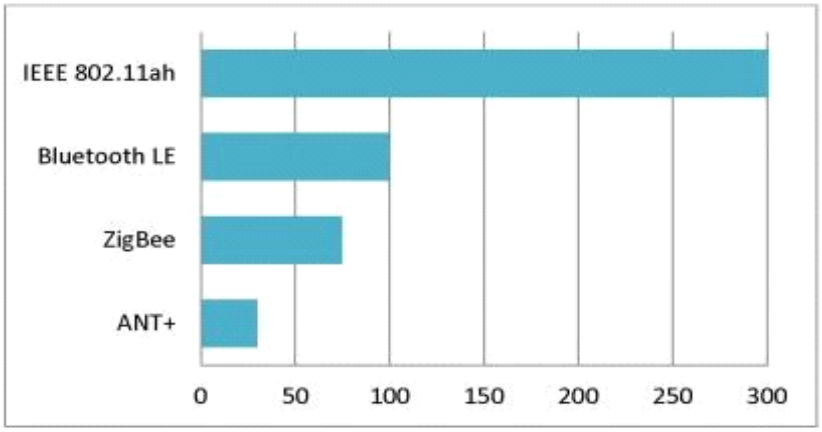


Рис.3.4 – Дальність дії, м

Проте, відповідним форматом для здійснення зв'язку в БСМ є стандарт 802.15.4 (ZigBee), так як він є відкритим, на відміну від закритою технології Bluetooth LE і володіє значною перевагою у вигляді низької вартості апаратури для реалізації.

3.2 Опис стандарту 802.15.4

Стандарт 802.15.4 служить для організації двох нижніх рівнів еталонної моделі OSI в БСМ - фізичний (PHY) і канальний (MAC). Ці шари забезпечують послуги на більш високих рівнях (рис 3.5). Інтерфейси між шарами використовуються для визначення логічних з'єднань. Фізичний рівень забезпечує дві послуги: фізичне обслуговування управління і фізичне

обслуговування даних. Задачі фізичного рівня - вмикання / вимикання радіоприймача, визначення рівня енергії, вибір каналу, прийому і отримання пакетів через фізичне середовище. Канальний рівень надає такі послуги: обслуговування управління і обслуговування даних на канальному рівні. Завдання - доступ до каналу, сигнальне управління, твердження / підтвердження доставки пакетів, роз'єднання (дисасоціація) і з'єднання (асоціація) з пристроями, забезпечення механізму безпеки [19,21].

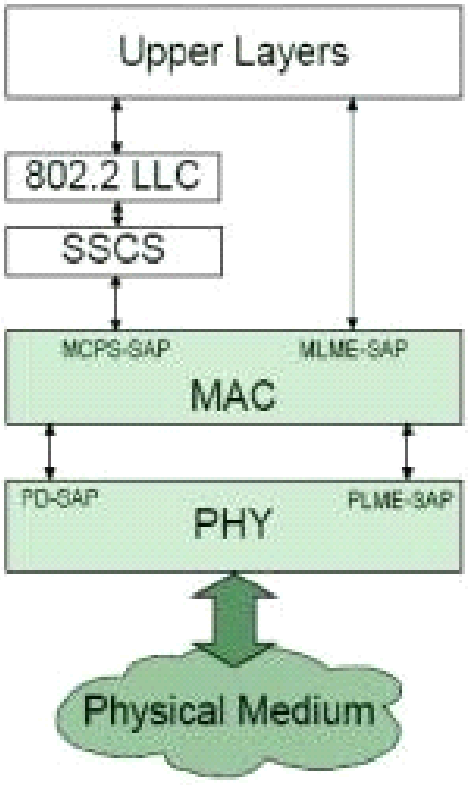


Рисунок 3.5 – Архітектура рівнів

Стандарт визначає протокол і взаємодію пристроїв в аступних неліцензованих радіодіапазонах [21]:

- 868,0 - 868,6 МГц (Європа, 1 канал);
- 902 - 928 МГц (Північна Америка, 10 каналів);
- 2450 МГц (решта світу, 16 каналів).

Швидкість передачі даних при цьому становить від 20 Кбіт / с (868 МГц) до 250 Кбіт / с (2450 МГц).

Всі пристрої стандарту можуть бути класифіковані з точки зору функціональності і призначення [16,17].

За функціональною ознакою можна виділити наступні типи пристроїв: повнофункціональний (FFD) і напівфункціональний (RFD).

Повнофункціональний пристрій може з'єднатися з будь-яким іншим, задіяним в мережі, а напівфункціональний - тільки з FFD.

Виділяють три види ZigBee- пристроїв за призначенням [16,17,21]:

- ZC або ZigBee - координатор – за визначенням є найбільш відповідальним пристроєм, котрий генерує шляхи дерева мережі і взаємодіє з іншими мережами. Таким чином в будь-якій мережі існує один ZC, який управляє мережею - присвоює ідентифікатор PAN, вибирає частоту, роздає короткі адреси.
- ZR або ZigBee – маршрутизатор - властиво може бути проміжним маршрутизатором, здійснюючи передачу даних з інших пристроїв. Крім цього, може запускати функцію додатку.
- ZED або кінцевий ZigBee - пристрій – виконує функції взаємодії з батьківським вузлом (відповідно з маршрутизатором або координатором), проте не має змоги виконувати передачу даних з інших пристроїв. Такий ZED потребує мінімальний обсяг пам'яті, отже, у виробництві, він може бути дешевше, ніж ZC або ZR [16,17].

Виділяють наступні топології мережі: «зірка» та «точка-точка» (мережа рівноправних вузлів).

Обмін даними в топології «зірка» між пристроями відбувається через центральний головний контролер, названий PAN-координатором. Він є в мережі первинним пристроєм і може отримувати живлення зі стаціонарного джерела.

У топології рівноправних вузлів («точка-точка») також присутній PAN-координатор, проте, будь-який пристрій, на відміну від «зірки», може з'єднатися з іншим пристроєм, поки вони знаходяться в межах один одного.

Таким чином, в топології рівноправних вузлів можуть утворюватися

складні мережеві форми, наприклад, петлі або кластерне дерево (рис. 3.6) або петля.

В такому випадку, RFD пристрої підключаються до деревовидної системи в кінці гілок як листовий пристрій [21].

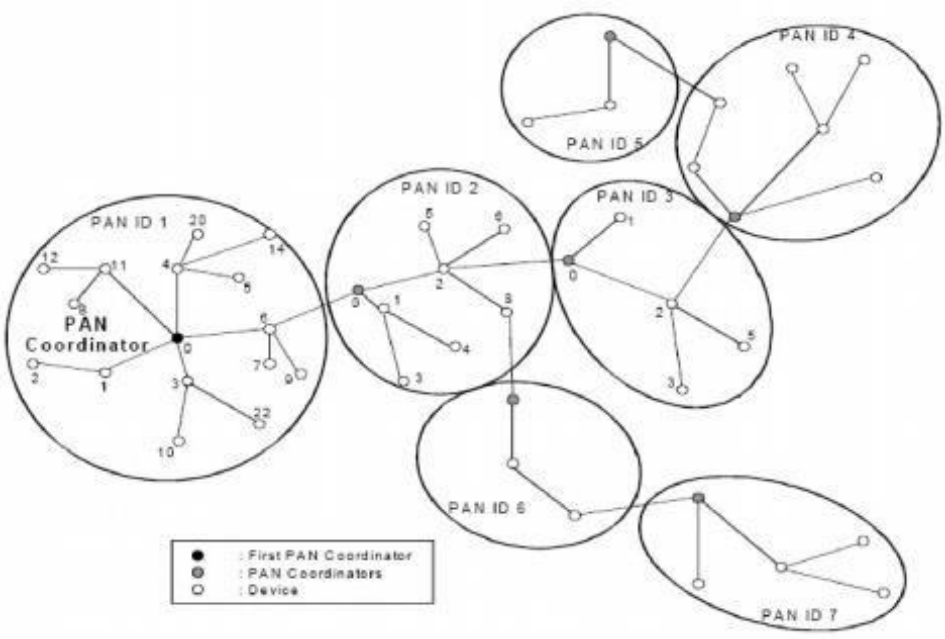


Рис. 3.6 – Кластерна топологія

Всі пристрої повинні мати підтримку унікальної 64-бітної адреси. Ця адреса береться для адресації в межах мережі. Для того щоб зменшити мережевий трафік, передбачено використання призначених координатором мережі 16-бітних адрес.

Стандарт визначає чотири типи пакетів [21]:

- сигнальний, призначений для передачі маяків координатором;
- даних, призначений для пересилання даних;
- підтвердження, що дані прийняті успішно;
- командний, призначений для керування об'єкта MAC.

Стандарт 802.15.4 передбачає захист даних з використанням симетричних ключів шифрування. Криптографічний механізм поєднує в собі:

- конфіденційність даних (передана інформації відома тільки тому, кому дана інформація призначена);

- справжність даних (захист від змін в процесі передачі);
- дублювання даних (повторна передача) [19,21].

3.3 Розробка рекомендацій по вибору стандартів 802.11n і 802.11ac

У процесі дослідження двох стандартів була зібрана тестовий майданчик (рис 3.1), що складається з однієї точки доступу і двох Wi-Fi адаптерів [13,22]:

- Точка доступу D-Link DAP2690(802.1 1a/b/g/n/ac, 3x3MIMO, 80 MHz);
- Wi-Fi приймач Asus PCE-AC68 (802.1 1ac, 3x3MIMO, 80MHz);
- Wi-Fi приймач Asus N14 (802.1 1n, 3x3MIMO, 40MHz).

Суть експерименту в послідовному зборі вимірів даних для кожного адаптера, поступово збільшуючи кількість інформаційних потоків. В процесі тестування точка доступу конфігурувати залежно від стандарту використовуваного адаптера.

Рисунок 3.7 Схематичне відображення тестового майданчика

Підсумки дослідження функціонування Wi-Fi приймачів в залежності від кількості потоків даних можна побачити в таблиці 3.2. [13,22]:

Таблиця 3.2

Порівняння продуктивності 802.11n та 802.11ac

Адаптер \ кількість потоків	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
802.11ac	168.74	293.63	351.44	385.32	414.84	425.65	440.32	442.60
802.11n	110.27	143.88	161.682	162.91	160.27			

При трансляції одного потоку інформації перевагу технології 802.11ac неочевидно: 802.11n демонструє 110Mbps при 40MHz, а 802.11ac 169Mbps при 80MHz.

Далі ж при зростанні кількості потоків Wi-Fi приймач 802.11n зупиняє ріст швидкості приймача вже на трьох потоках (162 Mbps). Одночасно інший адаптер не знижує тенденцію збільшення швидкості аж до семи потоків. Очевидно, що значення питомої швидкості на потік знижується, однак продовжує бути більш ефективним.

Нижче продемонстровано переваги технології 802.11ac (рис 3.8) [13,22].

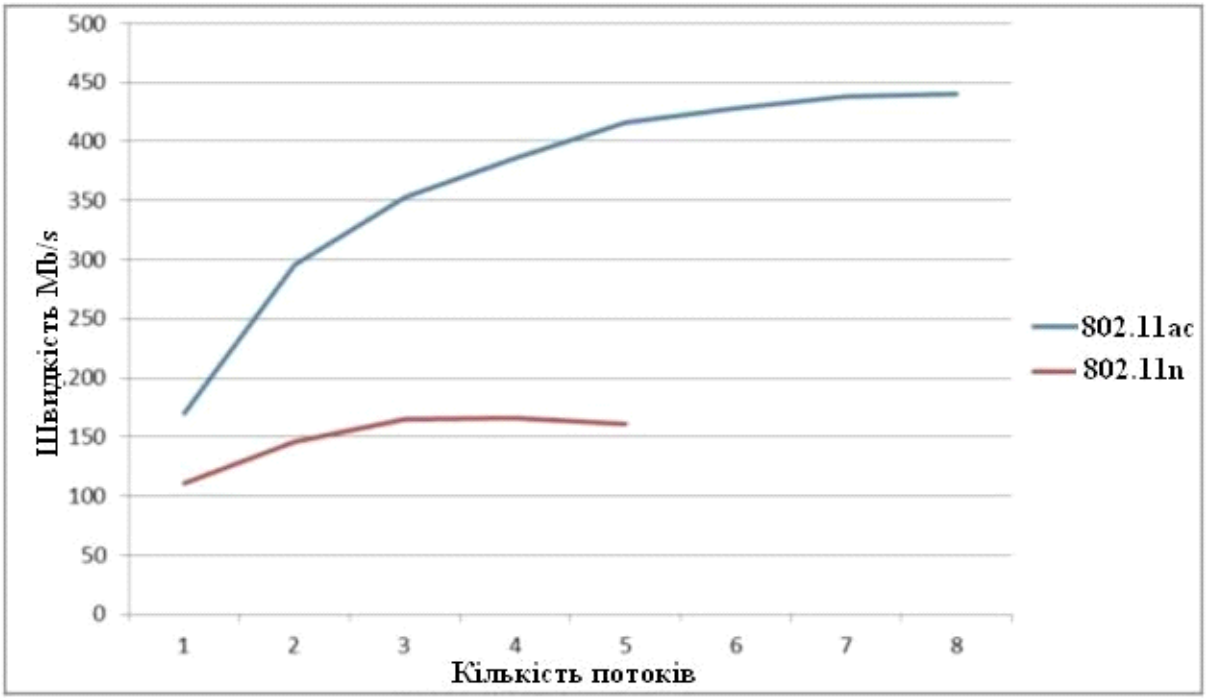


Рис. 3.8 Графіки продуктивності 802.11ac і 802.11n 3.1.

Розрахунок зони покриття Для того щоб знайти зону покриття каналу зв'язку необхідно прояснити такі поняття як [13,22]:

- відстань між об'єктами – D;
- центральна частота каналу - F;
- втрати у вільному просторі - FSL (free space loss).

$FSL = 33 + 20(lgF + lgD)$Вираз для розрахунку відстані зв'язку потрібно взяти з формули за якою розраховуються втрати у вільному просторі:

За виразом обчислюється FSL:

$$FSL = Y_{\text{дБ}} - SOM$$

де SOM це запас в енергетиці радіозв'язку прийнятий брати рівним 10 дБ достатнього для інженерного розрахунку, а сумарне підсилення системи виражається таким чином:

$$Y_{\text{дБ}} = P_{t,\text{дБмВт}} + G_{t,\text{дБ}u} + G_{r,\text{дБ}u} - P_{min,\text{дБмВт}} - L_{t,\text{дБ}} - L_{r,\text{дБ}}$$

Де $L_{r,\text{дБ}}$ - втрати сигналу в кабелі приймає тракту, $L_{t,\text{дБ}}$ - втрати сигналу в кабелі передавального тракту, $P_{min,\text{дБмВт}}$ - чутливість приймача на даній швидкості, $G_{r,\text{дБ}u}$ - коефіцієнт посилення приймаючої антени, $G_{t,\text{дБ}u}$ - коефіцієнт посилення передавальний антени, $P_{t,\text{дБмВт}}$ - потужність передавача.

В результаті отримуємо формулу для дальності зв'язку:

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

Знайдемо відстань на якому буде стабільно працювати зв'язок при схемі кодування MSC7 для точки доступу D-Link DAP2690 і бездротового адаптера Asus PCE-AC68. Їх паспортні характеристики при MSC7:

- Потужність передавача D-Link DAP2690: 14 дБмВт;
- Потужність передавача Asus PCE-AC68: 14 дБмВт;
- Чутливість D-Link DAP2690: -68 дБмВт;
- Чутливість Asus PCE-AC68: -68 дБмВт;

- Коефіцієнт посилення антени D-Link DAP2690: 6 дБи;
- Коефіцієнт посилення антени Asus PCE-AC68: 6 дБи. Втрати в антенно-фідерному тракті опускаємо.

Рішення [13,22]:

$FSL = 14 + 6 * 3 - (-68) - 10 = 90$дБЗнайдемо відстань при схемі MSC7. Параметр FSL дорівнює

Знайдемо дальність зв'язку (як приклад візьмемо сотий канал):

$$D_{MSC7} = 10^{\left(\frac{90}{20} - \frac{33}{20} - lg5500\right)} = 0{,}128 \text{ км} \approx 130 \text{ м}$$

3.4 Розробка рекомендацій по вибору і обґрунтуванню бездротових технологій

Побудова гнучких мереж збирання та керування даними є завданням, яке постійно актуальне в різних галузях науки та промисловості. Для прикладу варто перерахувати лише деякі з таких сфер застосування:

1) керування технологічними процесами на виробництві – управління роботою промислових об`єктів;

2) автоматизація досліджень у різних галузях науки – системи реєстрації результатів експерименту, контролю обладнання та вимірювальних приладів;

3) моніторинг, диспетчеризація та керування станом “чистих” кімнат у медицині;

4) застосування в побуті системи “розумного будинку” та пультової сигналізації, автоматичного збирання показників приладів обліку енергоносіїв;

5) автоматизація індивідуального обладнання – системи моніторингу стану здоров`я людини;

6) системи автоматизації навчальних стендів та обладнання.

Розвиток телекомунікаційних технологій відбувається за двома основними напрямами: збільшенням пропускної здатності каналів зв’язку та

переходом до використання мобільних технологій.

Ця тенденція спостерігається і в системах збирання та керування даними, переважно через численні вигоди, які отримують системні інтегратори та користувачі від застосування бездротових рішень.

Великої популярності набули модулі на основі систем на кристалі – інтегральних схем, в яких об'єднано в одному корпусі радіотракт однієї чи декількох технологій бездротового передавання інформації, мікроконтролер та периферійні модулі: інтерфейси, ЦАП/АЦП, програмовану логіку та ін. Все це разом з помірною ціною дає можливість створити гнучку систему збирання та керування даними для різноманітних сфер застосування.

Ефективне використання різноманітного обладнання та систем\м, об'єднаних бездротовими технологіями передбачає виконання таких вимог [23,24]:

– апаратна частина повинна бути доступною (COTS);

– забезпечення певного рівня універсальності – передбачено, що система зможе працювати з давачами різних виробників;

– кількість вузлів – 2-10 до ..100;

– доступність програмного забезпечення (ПЗ);

– низьке енергоспоживання – .розроблювана система в окремих випадках матиме безперебійне джерело живлення, але частіше її вузли будуть розташовані в місцях, важко доступних для людини, або місцях, що вимагають стерильності, наприклад, у "чистих кімнатах".

Проведемо аналіз сучасних технологій бездротового передавання даних для вибору типу мережі при створенні системи збирання та керування даними в бездротових мережах.

В якості опорної мережі для здіснення порівняльного аналізу різних стандартів оберемо мережу науково – дослідної лабораторії, яка може об'єднувати від 2 до 10 елементів системи.

Для передавання даних зараз активно використовуються такі протоколи: Z-Wave/Z-Wave Plus, ZigBee, Bluetooth Low Energy, ANT/ANT+, Wireless USB,

Wi-Fi.

У Табл. 3.3 наведено основні їх характеристики, що впливають на вибір одного з них в межах розв’язання поставленого завдання [23-26].

Таблиця 3.3

Порівняння мереж бездротового зв’язку

	ZigBee	Z-Wave	BLE	ANT	Wi-Fi	W-USB
Частотний діапазон, МГц	868/915/2400	8968/908(всі) 2400(с.400)	2400-2483	2400-2483	2483-5500	3100-10600
Швидкість передавання, Кбіт/с	20/40/250	9.6/40 (з 200 с.) 200(с.400)	1000	1000	100->54000	110000-480000
Кількість вузлів	1 маршрутизатор обслуговує до 32 вузлів	1 маршрутизатор обслуговує до 32 вузлів	1 ведучий обслуговує 7 ведених	1 ведучий обслуговує 7 ведених	Мін. 2 вузла	1 хост обслуговує до 127 вузлів
Радіус дії, м	10-100	30-100	50	30	150	3-100
Типи пристроїв чи ролі вузлів	Координатор, маршрутизатор, кінцевий пристрій	Координатор, маршрутизатор, ведений	Ведучий і ведений	Ведучий і ведений	Точка доступу, клієнт	Хост, перифе-рійний пристрій
Піковий струм спожи-вання вузла, мА	<150	21 (режим пробудження) 36 (режим передачі)	12,5	17	116 (при 1,8В)	<500

Протоколи Z-Wave Plus/Z-Wave.

Z-Wave Plus – це протокол бездротового зв’язку, розроблений для побутової автоматизації, зокрема, керування обладнанням в офісах і приватних оселях (технологія “Розумний будинок”) [26,26].

Протокол забезпечує сумісність пристроїв різноманітних виробників і працює на частотах до 1ГГц. Це дозволяє не використовувати додаткових заходів для зменшення впливу завад, які існують при роботі на частоті 2,4ГГц. В умовах прямої видимості досягається швидкість передавання даних на відстань до 30 м.

В основу Z-Wave покладено mesh-топологію, в якій кожен вузол або пристрій може приймати і передавати керуючі сигнали іншим пристроям мережі, використовуючи проміжні сусідні вузли.

Переваги протоколу [26,26]:

– віддалений моніторинг мережі через Інтернет чи мобільний телефон;

– зручність масштабування;

– мережа може бути побудована з допомогою ПЗ з відкритим кодом.

Недоліки протоколу [26,26]:

– початковий запуск мережі вимагає роботи групи висококваліфікованих спеціалістів;

– для мереж з кількістю вузлів понад 30 ціна реалізації мережі стає вищою, ніж ціна відповідних кабельних мереж;

– у зв’язку з конструктивними особливостями мережі мають обмежений радіус дії і масштаби.

Отже, можна зробити висновок про можливість використання цієї технології для комерційних застосувань за необхідності створення мережі з обмеженою кількістю вузлів.

Протокол ZigBee.

ZigBee – специфікація мережних протоколів верхнього рівня, які використовують сервіси нижніх рівнів – рівня MAC і фізичного рівня PHY [27,28]. Протокол ZigBee гарантує безпечне передавання даних при відносно невисоких швидкостях (20–40 Кбіт/с) і можливість роботи мережних пристроїв від автономних джерел живлення (батареї типу AAA).

Технологія ZigBee реалізує mesh-топологію мережі та забезпечує автоматичну ретрансляцію повідомлень з підтримкою мобільних вузлів. Сьогодні ZigBee застосовують для створення сенсорних мереж, реалізації технології “Розумний будинок”, систем комунального призначення, охоронних систем, систем керування в промисловості.

Стандарт ZigBee забезпечує найвищі швидкості передавання даних та найвищу завадостійкість у діапазоні 2,4 ГГц. Швидкість передавання даних разом зі службовою інформацією становить 250 Кбіт/с. При цьому середня

пропускна здатність вузла для корисних даних залежно від завантаженості мережі і кількості ретрансляцій у межах 5–40 Кбіт/с.

Відстань між вузлами мережі 10–20 метрів під час роботи в приміщенні і сотні метрів при відкритому просторі, завдяки ретрансляції зона покриття мережі може бути збільшена.

Однією з переваг і водночас недоліком технології є її складність. Перевага полягає у тому, що така архітектура забезпечує високу надійність і живучість мережі, а недоліком є значна ціна побудови.

Мережу будують з використанням:

– координатора, що запускає мережу, виконує функції центру керування мережею і центру довіри – встановлює політику безпеки, задає налаштування в процесі приєднання пристроїв в мережу, завідує ключами безпеки. Очевидно, що вихід з ладу координатора спричиняє непрацездатність всієї мережі;

– маршрутизатора, який транслює пакети, виконує динамічну маршрутизацію, тому прямий зв’язок між двома кінцевими пристроями ZigBee неможливий. Розробнику необхідний і координатор, і маршрутизатор для встановлення зв’язку лише двох пристроїв.;

– кінцевого пристрою, що може приймати і передавати пакети, але не може займатися їх трансляцією і маршрутизацією. Кінцеві пристрої не можуть мати дочірніх пристроїв, а мають бути підключеними до координатора чи маршрутизатора. Саме кінцеві пристрої працюють з давачами.

Технологія ZigBee використовує 16-бітну адресацію, тобто теоретично один координатор може взаємодіяти з понад 65 000 пристроями. Разом з тим можлива робота одночасно декількох мереж. Наприклад, в готелі Aria (Лас-Вегас) [29] розміщено близько 75 000 пристроїв з підтримкою ZigBee.

Мережа такої складності вимагає знань і компетенції для налаштування та обслуговування. У зв’язку з описаними вище характеристиками цей протокол підходить для реалізації мереж зі значною кількістю вузлів корпоративного, промислового та військового напрямку, забезпечить високий рівень надійності і працездатності навіть при пошкодженні мережі.

Протоколи Bluetooth Low Energy Bluetooth Low Energy (BLE).

Протокол для створення персональних мереж, основними сферами застосування є охорона здоров'я, спорт, охоронні системи, індустрія розваг, побутові застосування, інтернет-речей (IoT) [8,9,29]. Істотною перевагою специфікації є наднизьке пікове енергоспоживання, середнє енергоспоживання і енергоспоживання в режимі простою, що дасть змогу створити систему, яка працює з давачами безперервно та не вимагає постійного джерела живлення.

Мобільні операційні системи, зокрема IOS, Android, Windows Phone і BlackBerry, а також OS X, Linux і Windows 8 мають вбудовану підтримку Bluetooth Low Energy (інша назва – Bluetooth Smart). З вищеозначеного випливає поширеність цієї технології, що є значною перевагою. BLE, на жаль, не має зворотної сумісності з попереднім (так званим "класичним") протоколом Bluetooth.

Специфікація Bluetooth 4.0 (і пізнші) фактично визначає дві бездротові технології: BR / EDR і стандарт BLE. Пристрої, в яких застосовано BLE, можуть бути як дворежимні BR / EDR / BLE (Bluetooth Smart - Ready), сумісні з класичними Bluetooth-пристроями, так і однорежимні BLE (Bluetooth Smart).

Основними блоками Bluetooth-пристроїв є [9,10,29]:

– програма – реалізує логіку роботи;

– ведучий пристрій, хост – реалізує верхні рівні стека протоколів Bluetooth;

– контролер – реалізує нижні рівні стека протоколів Bluetooth.

Комерційні продукти зазвичай виконано в одному з таких апаратних рішень:

– система на кристалі – однокристальна система, що об'єднує програму, хост і контролер, застосовується в компактних пристроях, наприклад, в давачах;

– рішення на двох мікросхемах, при якому додаток і хост з'єднано з контролером за допомогою UART, USB, SDIO і т. п. за протоколом HCI. Така

конфігурація може використовуватися, наприклад, в мобільних пристроях;

– рішення на двох мікросхемах, при якому хост і контролер з'єднано за пропрієтарним протоколом;

– програмоване радіо на кристалі – однокристальна система, яка об'єднує мікроконтролер, апаратно реалізований модуль Bluetooth та програмовану логіку. BLE визначає 40 радіочастотних каналів з кроком 2 МГц. Адаптивний механізм стрибкоподібної перебудови частоти використано для протидії перешкодам, загасанню сигналу та інтерференції. Цей механізм вибирає один з 37 доступних каналів передавання даних для зв'язку протягом заданого часового інтервалу.

Усі фізичні канали використовують GFSK-модуляцію [30]. Коефіцієнт модуляції знаходиться в діапазоні від 0,45 до 0,55, що забезпечує знижену пікову споживану потужність.

Протокол ANT/ANT+ .

ANT/ANT+ – це пропрієтарний протокол, розроблений для обміну даними з сенсорами, що знаходяться на відстані 1 – 5 м [30]. Переважно це: давачі серцевого ритму, давачі швидкості, давачі тиску тощо. Цей протокол має певні переваги над BLE в сфері енергоспоживання, а саме [8,9,30]:

– менше споживає електроенергії при оголошенні сервісу;

– менше споживає електроенергії при скануванні та ініціюванні сеансу зв`язку;

– потребує менше трансакцій для кожного етапу сеансу зв'язку;

– при відправці однакового об'єму даних пересилає менше службової інформації.

Протокол реалізує топології: точка-точка, "зірка", "дерево". Згідно з специфікацією дозволяє мережі розміром до 65533 вузлів.

ANT+ є адаптивним синхронним протоколом. Мережа утворюється логічними з'єднаннями пар вузлів. При цьому один вузол грає роль ведучого, а другий – веденого. Але тому ж веденому дозволено бути ведучим відносно

іншого вузла, з яким у нього інше логічне з’єднання.

Протокол ANT+ є протоколом з відкритим кодом, та основним недоліком його є менша поширеність порівнянно з BLE чи ZigBee.

Протокол Wireless USB (W-USB)

Wireless USB (W-USB) – технологія, створена у зв’язку з популярністю USB інтерфейсу і покликана забезпечити переваги USB у сфері бездротового зв`язку. Ця технологія забезпечує швидкість 480 Мбіт/с на відстані до 3 метрів і 110 Мбіт/с на відстані до 10 метрів, що дозволяє використовувати її в офісах, наукових і державних установах (підтримується багатьма принтерами, сканерами, цифровими камерами, жорсткими дисками тощо) та в побуті (гейм-плеї, домашні кінотеатри, побутова техніка) [8,9,32].

Wireless USB архітектура дозволяє підключення до 127 пристроїв безпосередньо до хоста, який є унікальним для системи і переважно інтегрований у комп’ютер. Для безпечного з’єднання використовуються механізми авторизації і шифрування з’єднання. Та, незважаючи на високу швидкість передавання W-USB на частоті 3.1-10.6 ГГц, модулі цієї технології є дорогими та важкодоступними в непромислових кількостях.

Протокол Wi-Fi

Wi-Fi є протоколом, що дозволяє електронним пристроям підключатися до бездротової мережі LAN, переважно з використанням 2,4 ГГц і 5 ГГц радіодіапазонів [11,15,32]. Протокол є одним з найпоширеніших, існує значний об’єм літератури, де його описано.

Цей протокол не підходить для вирішення поставленого завдання у зв’язку з такими особливостями: високе енергоспоживання, надлишковість трафіка, ненадійність з’єднання, вразливість до атак тощо.

Аналіз і вибір рішення

Протокол ANT/ANT+, незважаючи на те, що забезпечує найнижче в

середньому енергоспоживання, не підходить, оскільки не є достатньо поширеним. При використанні ANT/ANT+ система не відповідатиме пред`явленим вимогам.

Протокол W-USB є надлишковим, оскільки немає необхідності забезпечення значних швидкостей, до того ж висока ціна модулів у непромислових кількостях також стає на заваді. Протокол вимагає значних (таблиця) енерговитрат, що є неприйнятним.

Протоколи Z-Wave Plus/Z-Wave у зв'язку з складністю початкового налаштування, але більше через низьку ефективність при невеликій кількості вузлів будуть не найоптимальнішим рішенням поставленого завдання.

Протокол ZigBee – рішення для територіально розкиданих складних мереж, яким насамперед потрібно забезпечити стабільний зв`язок при надзвичайних ситуаціях. Але саме складність мережі, її налаштування та обслуговування, що забезпечує надійність протоколу, стає перешкодою при реалізації завдання. Адже необхідно, щоб розгортання системи займало як найкоротший часовий проміжок, і щоб систему було легко налаштувати. У зв`язку з цим цей протокол стає непридатним для реалізації поставленого завдання.

Протокол Wi-Fi, що показав себе в ролі провідного бездротового протоколу передавання даних для пристроїв з високим запасом електроенергії, для поставлених цілей не підходить.

Протокол Bluetooth Low Energy, на основі проведеного аналізу, є найприйнятнішим для реалізації поставленого завдання сьогодні. Звичайно, протокол має суттєві недоліки з огляду на поставлене завдання, а саме, не має стандартизованої процедури обміну між двома і більше мережами Piconet, що ускладнює об`єднання декількох мереж Piconet для проведення складніших вимірювань і аналізу більшого об`єму даних, для подальшого вдосконалення і розширення мережі.

З іншого боку, цей протокол відповідає всім висунутим вимогам, що дає можливість застосувати його для реалізації системи керування і збирання даних

при наукових експериментів, тестувань, розгортання систем вимірювання і моніторингу на короткий проміжок часу (тижні).

У зв’язку з представленими вимогами до системи раціональним рішенням буде використання протоколу Bluetooth Low Energy.

Результати аналізу дають основу для проектування бездротового модуля введення – виведення системи збирання та керування даними для проведення навчальних та наукових експериментів. Цей модуль може бути в подальшому використаний для створення мережі, що охопить лабораторне приміщення, а в перспективі і будівлю наукової установи.

Подальший напрямок роботи полягає у дослідженні основних закономірностей роботи мережі таких бездротових модулів у межах мережі Piconet, а надалі і в межах мережі Scatternet.

3.5 Висновки по розділу

1. Проведено аналіз та обґрунтовано рекомендації по вибору технологій передачі даних по бездротовим мережам

2. Показано, що технологія ANT + поступається конкурентам за параметрами дальності і пропускної здатності, маючи досить невеликі переваги в часі готовності і піковому струмі споживання. Технологія IEEE 802.11ah обіцяє надати вкрай високі (на тлі конкурентів) показники дальності і пропускної здатності, але, в той же час, є найбільш енерговитратною.

3. Встановлено, що технології Bluetooth LE та 802.15.4 (ZigBee) за своїми характеристикам досить близькі за значенням, і є найбільш привабливими технологіями серед розглянутих при формуванні локальних бездротових мереж передачі даних. А саме, протоколи передавання даних Bluetooth Low Energy як найповніше відповідає меті модернізації вибраної в роботі опорної мережі обміну даними наукової лабораторій. Пропонується використання цієї технології для проектування системи збирання та керування даними лабораторного обладнання наукових установ.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

– Проведено огляд застосування бездротових технологій передачі даних в системах збору інформації;

– Проаналізовано властивості стандартів збору та передачі даних в бездротових мережах;

– Досліджено напрямків підвищення ефективності застосування бездротових технологій передачі даних;

– Розроблено практичні рекомендації щодо вибору технології збору та передачі даних в бездротовій локальній мережі збору та обробки інформації.

1. У першому розділі кваліфікаційної роботи подано основи передачі інформації в бездротових технологіях. Показано, що бездротові технології - по суті, є окремим випадком інформаційних технологій, який використовується коли необхідно передати сигнал між двома і більше об'єктами, при цьому не використовуючи дроти для їх зв'язку. Визначена класифікація бездротових технологій передачі даних та подано опис визначених типів. Подано порівняльні характеристики основних стандартів сучасних бездротових технологій та подано їх опис.

2. У другому розділі кваліфікаційної роботи подано описи основних технологій, що застосовуються для формування бездротових сенсорних мереж передачі даних. А саме, стандарти :ZigBee, AMT+, Bluetooth LE і IEEE 802.11 ah. Визначено області застосування бездротових мереж та подано їх описи. А саме: IoT - «Інтернет речей»), бездротова сенсорна мережа, «Розумний будинок». Визначена продуктивність та надійність бездротових мереж. Подано описи вказаних характеристик. Визначені питання забезпечення безпеки технологій Wi-Fi. Подано механізм аутентифікації WPA2 та параметри безпеки мережі. Описано механізм шифрування WPA2 та процедура пошуку і злому уразливих

точок доступу бездротових мереж Wi-Fi (Wellenreter), в тому числі, за допомогою утиліти InSSIDer.

3. У третьому розділі кваліфікаційної роботи подано проведено аналіз та обґрунтовано рекомендації по вибору технологій передачі даних по бездротовим мережам.

Показано, що технологія ANT + поступається конкурентам за параметрами дальності і пропускної здатності, маючи досить невеликі переваги в часі готовності і піковому струмі споживання.

Технологія IEEE 802.11ah обіцяє надати вкрай високі показники дальності і пропускної здатності, але, в той же час, є найбільш енерговитратною.

Встановлено, що технології Bluetooth LE та 802.15.4 (ZigBee) за своїми характеристикам досить близькі за значенням, і є найбільш привабливими технологіями серед розглянутих при формуванні локальних бездротових мереж передачі даних. Показано, що протоколи передавання даних Bluetooth Low Energy як найповніше відповідає меті модернізації вибраної в роботі опорної мережі обміну даними наукової лабораторій.

В роботі обґрунтовано використання цієї технології для проектування бездротової мережі збору та обробки інформації від лабораторного обладнання наукової установи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стеклов В.К., Костик Б.Й., Беркман Л.Н. Сучасні системи управління в телекомунікаціях. – Киїів: Техніка, 2005. 400 с.

2. Сергиенко, А.Б. Цифровая обработка сигналов: Учеб. пособие / А.Б. Сергиенко. - СПб.: Питер, 2003 - 604 с.: ил

3. Прокис Дж. Цифровая связь: Пер. с англ. / Под ред. Д. Д. Кловского.— М.: Радио и связь, 2000.— 800 с.

4. Уидроу Б. Адаптивная обработка сигналов. / Уидроу Б. Стирнз С.Д.; Пер. с англ. под ред. Шахгильдяна В.В. - М.: Радио и связь, 1989. - 440 с.

5. Романова А.І. Телекомунікаційні мережі та управління. – Київ: ВПЦ “Київський університет”, 2003. 247 с.

6. Пролетарский, А.В. Беспроводные сети Wi-Fi / Пролетарский А.В., Чирков Д.Н – М.: «ИНТУИТ», 2016, 215 с.

7. Семенов, Ю.А. Алгоритмы и протоколы каналов и сетей передачи данных. Учебное пособие / Семенов Ю.А. –М.: БИНОМ, 2007. -634с.

8. Гайкович Г.Ф. Обзор беспроводных технологий для современных мобильных устройств связи // Электронные компоненты. 2017. №1. С. 65-69.

9. Рошан П. Основы построения беспроводных локальных сетей стандарта 802.11. Руководство CISCO. – Москва: Вильямс, 2014. 304 с.

10. Беспроводные технологии с низким энергопотреблением. *Время электроники*. URL: http://www.russianelectonics.ru/leader-r/review/2187/doc/58627 (дата звернення: 24.04.2021).

11. Стандарты Wi-Fi [электронный ресурс] – Режим доступу: http://viconnect.ru/

12. Кратко о MIMO [электронный ресурс] – Режим доступа: http://wi-life.ru/wifi-academy-rus/80211n-mimo-2

13. Технология сетей. Все для построения сетей [электронный ресурс] – Режим доступа: https://nettech.ua/

14. В поисках Wi-Fi [электронный ресурс] – Режим доступа:

https://xakep.ru/2016/05/26/www-3wifi/

15. Wi-Fi HaLow (IEEE 802.11ah) — дальнобойное беспроводное подключение с низким энергопотреблением для интернета вещей. URL: https://HYPERLINK "http://www.ixbt.com/news/2016/01/05/wi-fi-halow-ieee-802-11ah.html"www.ixbt.com/news/2016/01/05/wi-fi-halow-ieee-802-11ah.html

16. Беспроводные сети ZigBee и IEEE 802.15.4. *Телекоммуникационные технологии.* URL: http://www.book.itep.ru/4/41/zigbee.htm

17. Сети ZigBee. Зачем и почему: Хабрахабр. URL: https://habrahabr.ru/post/155037 (дата звернення: 20.05.2021).

18. Интернет вещей приближается: Хабрахабр. URL: https://habrahabr.ru/company/madrobots/blog/236115

19. WPA2-Enterprise, или правильный подход к безопасности Wi-Fi сети [электронный ресурс] – Режим доступа: http://habrahabr.ru/post/150179

20. Гордейчик С. В., Дубровин В. В., Безопасность беспроводных сетей. – м.:Горячая линия – Телеком, 2008, 288 с.

21. IEEE 802.15.4-2020 - IEEE Standard for Low-Rate Wireless Networks. URL: http://www. https://standards.ieee.org/standard/802_15_4-2020.html.

22. Л. Дунець, В Бекус. Дослідження показників якості передачі сигналів в бездротових локальних мережах. III Всеукраїнська науково-практична інтернет-конференція студентів, аспірантів та молодих вчених «Сучасні інформаційні системи та технології». Херсон, 30.11.2020. с.23-24.

23. Галкін П. В. Аналіз моделей та оптимізації збору інформації в бездротових сенсорних мережах // Східно - Європейський журнал передових технологій. – Харків, 2014. – Вип. 71. – С. 24–30

24. Feng Wang, Dan Wang, Jiangchuan Liu Elesense: elevator-assisted wireless sensor data collection for high-rise structure monitoring. Proceedings - IEEE INFOCOM. March, 2012

25. О. В. Тимченко, М. Ю. Зеляновський. Особливості реалізації сенсорних мереж бездротового доступу. Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України. – К.: ІПМЕ

ім. Г.Є.Пухова НАН України, 2010. – Вип. 54. – С. 137-144.

26. Carles Gomez, Joaquim Oller, Josep Paradells. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. Sensors (Basel). 2012; PP. 11734–11753.

27. Z-Wave Alliance, http://z-wavealliance.org/

28. ZigBee Alliance, http://www.zigbee.org

29. ZigBee Case Study in Large Node Network – SiliconLabs. Jan 21, 2013 https://www.silabs.com/support/training/Pages/zigbee-case-study-large-node-network.aspx

30. Sabih H. Gerez. Implementation of Digital Signal Processing: Some Background on GFSK Modulation. University of Twente, Department of Electrical Engineering.March 9, 2016

31. ANT Alliance, https://www.thisisant.com/ 8. Wi-Fi Alliance, http://www.wi-fi.org/

32.“Wireless Universal Serial Bus Specification”, http://www.usb.org/, May 12, 2005 Agere, Hewlett-Packard and others document.

ДОДАТОК

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

УДОСКОНАЛЕННЯ КІБЕРЗАХИСТУ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ ОБ’ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Юрій ІВАНОВ

Керівник: к.т.н., доц. Тетяна НІМЧЕНКО

Київ - 2026

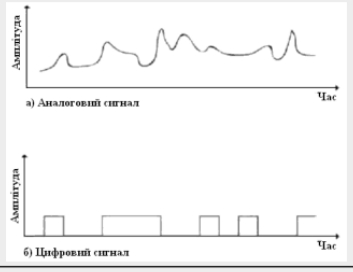
АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

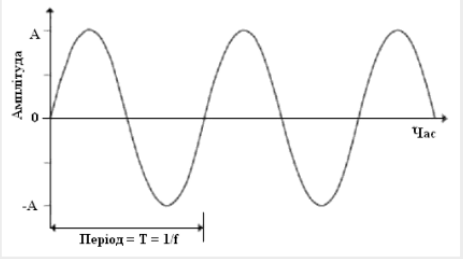
- Актуальність роботи обумовлена широким використанням бездротових технологій у системах збору та обробки інформації, а також зростанням вимог до їх кіберзахисту.
- Мета роботи - підвищення ефективності кіберзахисту безпроводових інформаційно-комунікаційних каналів передачі даних об’єкту інформаційної діяльності.
- Об’єкт дослідження - бездротові технології передачі даних.
- Предмет дослідження - бездротова мережа передачі даних у локальній мережі збору та обробки інформації.
- Завдання: оглянути бездротові технології, проаналізувати стандарти мереж, дослідити напрями підвищення ефективності та сформувати практичні рекомендації щодо вибору технологій.

ЗДОБУТІ РЕЗУЛЬТАТИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

- У першому розділі виконано огляд застосування бездротових технологій передачі даних у системах збору інформації.
- У другому розділі проаналізовано властивості стандартів збору та передачі даних у бездротових мережах, зокрема питання продуктивності, надійності та безпеки Wi-Fi.
- У третьому розділі досліджено напрями підвищення ефективності застосування бездротових технологій у системах збору інформації.
- Розроблено практичні рекомендації щодо вибору технології збору та передачі даних у бездротовій локальній мережі визначеної конфігурації.

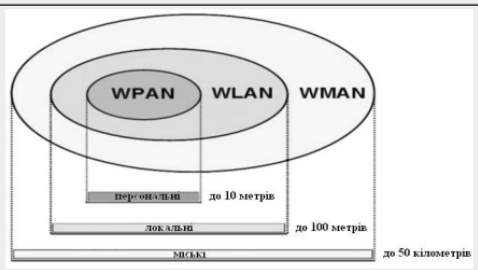
ОСНОВИ ПЕРЕДАЧІ ІНФОРМАЦІЇ У БЕЗДРОТОВИХ ТЕХНОЛОГІЯХ





- У бездротових каналах передавання інформації використовуються електромагнітні сигнали, які можуть мати аналогову або цифрову форму.
- Для практичного передавання цифрових даних через радіоканал необхідно враховувати частоту, фазу, амплітуду, період і смугу пропускання.
- Обмежена смуга пропускання каналу спричиняє спотворення сигналу, що впливає на завадостійкість, швидкість та якість приймання.

МОДУЛЯЦІЯ ТА КЛАСИФІКАЦІЯ БЕЗДРОТОВИХ МЕРЕЖ



- Для перетворення цифрових даних у сигнал радіоканалу застосовують фазову, амплітудну та частотну модуляцію.
- Бездротові мережі класифікують за масштабом дії: WPAN, WLAN, WMAN і WWAN.
- Вибір класу мережі залежить від дальності, пропускної здатності, енергоспоживання, захищеності та умов експлуатації.

СТАНДАРТИ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ТА ЇХ ХАРАКТЕРИСТИКИ

Стандарти бездротової передачі даних

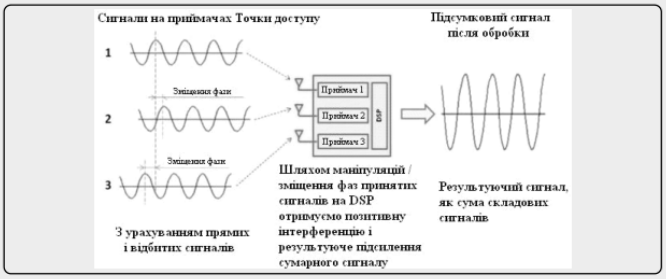
Технологія	Стандарт	Область застосування	Пропускна здатність, Мбіт / с	Дальність зв'язку	Модуляція, доступ середовища	Частотний діапазон, ГГц
Bluetooth	802.15.1	WPAN	до 0,7	до 10 м	FHSS	2,4
	V4.0		до 2,3	до 60 м	ГМСК	2,4
	V5.0		до 5	до 100 м	ФГМСК	2,4
Wi-Fi	802. llg	WLAN	до 54	до 140 м	DQPSK	2,4
	802,1 B		до 300	до 250 м	64QAM	2,4 або 5
	802,1 лак		до 1000	до 500 м	256QAM	5-6
WiMAX	802. 16r	WMAN	до 75	до 50 км	OFDM	1,5-11
	802.16e	WWAN	до 40	до 5 км	OFDM	2-13
	802,16м		до 1000	до 100 км	COFDM	2-66
LTE	LTE	WWAN	до 100	до 15 км	OFDM	0,8-3,5
	Розши-ренний		до 1000	до 100 км	COFDM	0,8-3,5

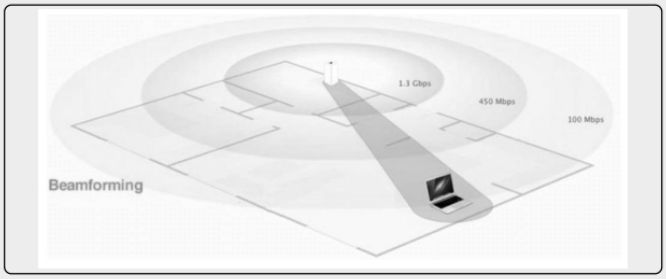
Порівняльна таблиця актуальних стандартів Wi-FI

Стандарт	**802. g**	**802,1 n**	**802,1 ac**
Дальність зв'язку	до 140 м	до 250 м	до 500 м
Ширина каналу	до 20 МГц	до 40 МГц	до 160 МГц
Частотний діапазон	2,4 ГГц	2,4 ГГц або 5 ГГц	5-6 ГГц
Тип модуляції	DQPSK	64QAM	256QAM
Пропускна здатність	до 54 Мбіт / с	до 300 Мбіт / с	до 1000 Мбіт / с
Сумісність	802,11 б / н	802.11 a / b / g	802.11 a / b / g / n
Рік сертифікації	2003 рік	2009 рік	2013 рік

- У роботі порівняно Bluetooth, Wi-Fi, WiMAX і LTE за областю застосування, пропускною здатністю, дальністю, модуляцією та частотним діапазоном.
- Для бездротових каналів використовуються різні види модуляції: FHSS, DSSS, OFDM, QPSK, 16QAM, 64QAM та інші.
- Стандарти конкурують у частині швидкості, дальності, енергоспоживання і придатності до конкретної прикладної задачі.

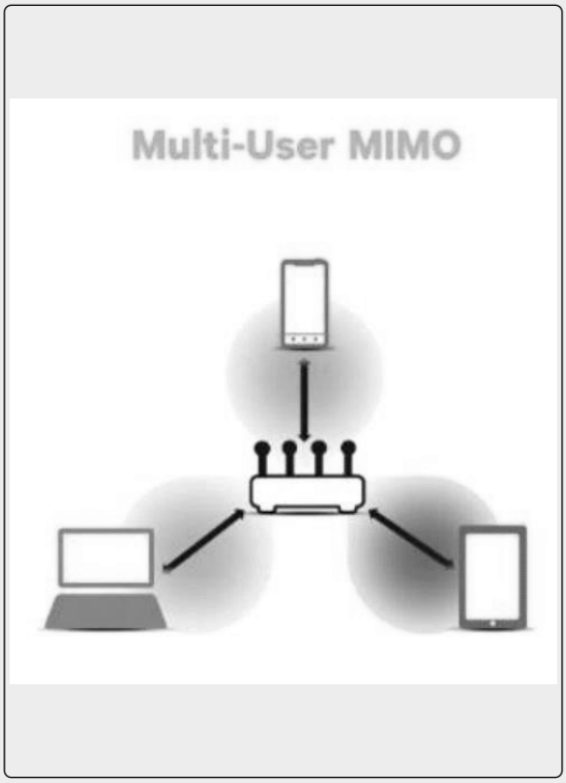
АКТУАЛЬНІ СТАНДАРТИ WI-FI ТА РОЗВИТОК IEEE 802.11





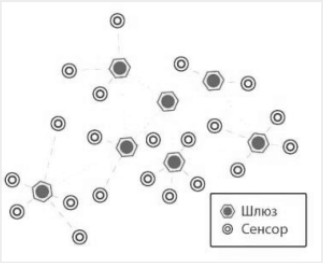
- Wi-Fi базується на сімействі стандартів IEEE 802.11 і використовується для побудови локальних бездротових мереж.
- Стандарти 802.11g, 802.11n і 802.11ac відрізняються пропускною здатністю, частотними діапазонами, модуляційними схемами та можливостями просторового мультиплексування.
- Технології MIMO і Beamforming покращують якість каналу, збільшують швидкість та підвищують стабільність з’єднання.

ТЕХНОЛОГІЯ MU-MIMO ЯК НАПРЯМ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ



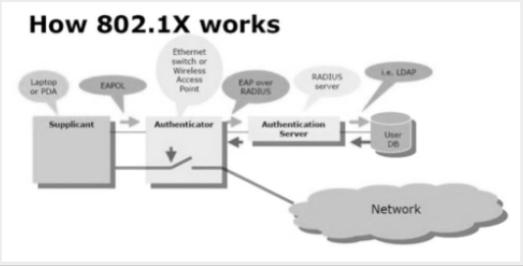
- MU-MIMO дозволяє точці доступу одночасно обслуговувати кілька клієнтських пристроїв, використовуючи просторові потоки.
- У порівнянні з традиційним MIMO технологія зменшує очікування клієнтів і підвищує сумарну пропускну здатність мережі.
- Застосування MU-MIMO є доцільним для офісних і корпоративних мереж із великою кількістю абонентських пристроїв.
- Для ефективної роботи важливими є правильне розміщення точок доступу та підтримка відповідних стандартів клієнтськими пристроями.

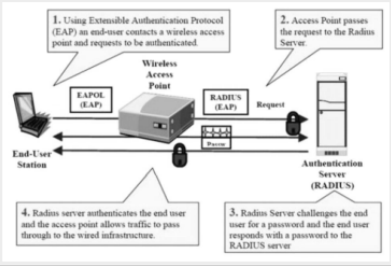
БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ ТА IOT-СЕРЕДОВИЩЕ



- Бездротові сенсорні мережі використовуються для збору даних від сенсорних вузлів у промислових, медичних, побутових і телекомунікаційних системах.
- Для IoT-рішень важливими параметрами є енергоспоживання, дальність, топологія, надійність передачі та масштабованість.
- Застосування хмарної інфраструктури дозволяє централізовано збирати, обробляти та аналізувати дані з різнорідних бездротових пристроїв.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WI-FI: WPA2 ТА 802.1X

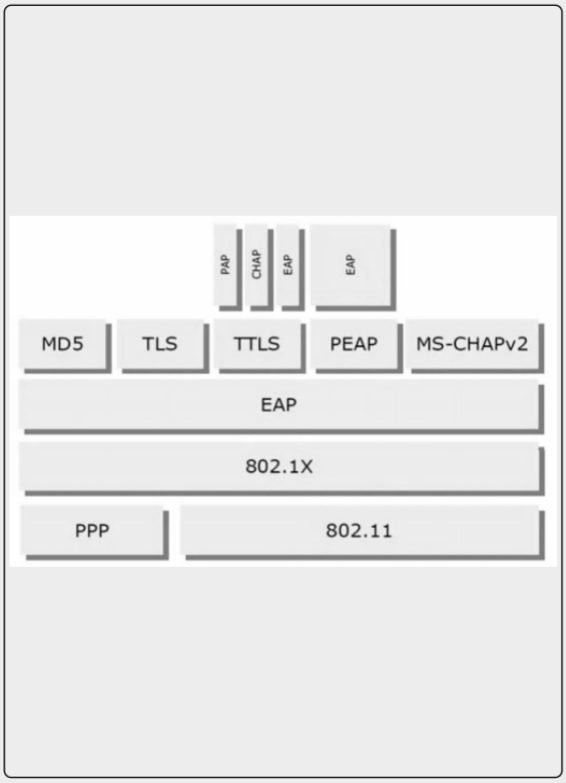




- Для підвищення захищеності Wi-Fi застосовуються механізми автентифікації, шифрування та керування доступом.
- Схема 802.1X використовує взаємодію клієнта, автентифікатора та сервера автентифікації для контролю доступу до мережі.
- WPA2 забезпечує автентифікацію користувача та формування криптографічних ключів для подальшого захисту переданих даних.

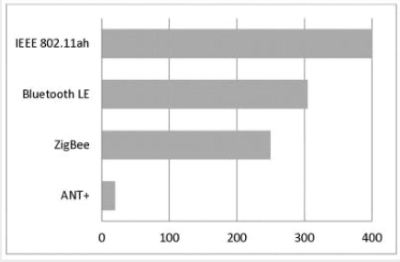
ПРОТОКОЛИ EAP ТА МЕХАНІЗМИ АВТЕНТИФІКАЦІЇ

- Протокол EAP є контейнерним механізмом, який підтримує різні способи автентифікації користувачів і пристроїв.
- У корпоративних WLAN доцільно застосовувати EAP-TLS, PEAP або EAP-TTLS залежно від вимог до сертифікатів, інфраструктури ключів та рівня захисту.
- Захист бездротового каналу повинен поєднувати автентифікацію, шифрування трафіку, сегментацію мережі та регулярний аудит налаштувань.
- Недостатній контроль параметрів точки доступу може призводити до атак на автентифікацію та перехоплення трафіку.



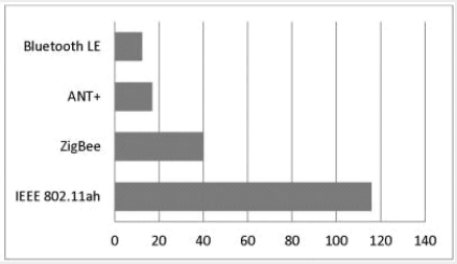
ВИБІР ТЕХНОЛОГІЙ ЗА ПРОПУСКНОЮ ЗДАТНІСТЮ ТА ЗАТРИМКОЮ

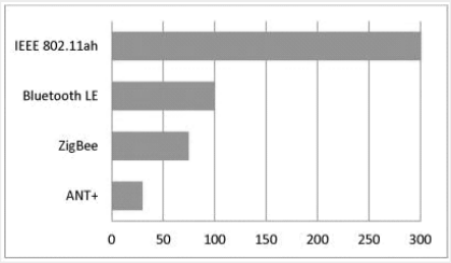
	Пропускна здатність	Час очікування	Піковий струм спожив	Частота	Дальність дії
ZigBee	20 - 250	10	30	0,868 - 2,4	70
ANT +	20	1,5	60	2,4	30
Bluetooth LE	305	2,5	12,5	2,4	100
IEEE 802.11ah	100 - 40000	1,5	116	0,9	100 - 1000



- У роботі проведено порівняння технологій IEEE 802.11ah, Bluetooth LE, ZigBee та ANT+ за ключовими характеристиками.
- Для мереж збору інформації пропускна здатність повинна відповідати обсягу даних, частоті опитування сенсорів і вимогам до часу доставки.
- IEEE 802.11ah демонструє вищу пропускну здатність, тоді як ZigBee і Bluetooth LE можуть бути доцільними для енергоощадних сенсорних систем.

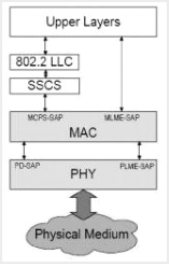
ОЦІНКА ЕНЕРГОСПОЖИВАННЯ ТА ДАЛЬНОСТІ ДІЇ

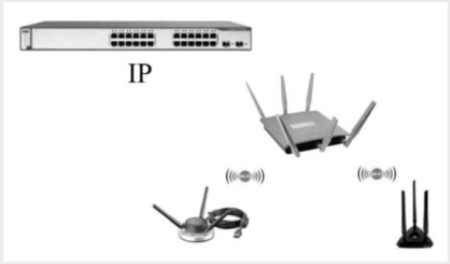




- Енергоспоживання є критичним показником для автономних сенсорних вузлів і IoT-пристроїв.
- Дальність дії визначає можливість побудови мережі без додаткових ретрансляторів і впливає на кількість точок доступу.
- Компроміс між дальністю, швидкістю та енергоспоживанням є основою вибору конкретної бездротової технології для опорної локальної мережі.

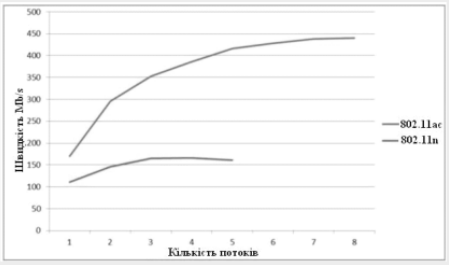
СТАНДАРТ IEEE 802.15.4 ТА БЕЗПЕКА БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ





- IEEE 802.15.4 визначає нижні рівні протоколів для низькошвидкісних бездротових персональних мереж і є основою для ZigBee-подібних рішень.
- Стандарт орієнтований на низьке енергоспоживання, просту архітектуру та підтримку сенсорних пристроїв.
- Захист такої мережі повинен забезпечувати конфіденційність, цілісність, автентичність даних і захист від повторного передавання пакетів.

РЕКОМЕНДАЦІЇ ЩОДО ВИБОРУ 802.11N ТА 802.11AC



	ZigBee	Z-Wave	BLE	ANT	Wi-Fi	W-USB
Частотний діапазон, МГц	868/915/2400	8968/908(всі) 2400(с.400)	2400-2483	2400-2483	2483-5500	3100-10600
Швидкість передавання, Кбіт/с	20/40/250	9.6/40 (з 200 с.) 200(с.400)	1000	1000	100->54000	110000-480000
Кількість вузлів	1 маршрутизатор обслуговує до 32 вузлів	1 маршрутизатор обслуговує до 32 вузлів	1 ведучий обслуговує 7 веденних	1 ведучий обслуговує 7 веденних	Мін. 2 вузла	1 хост обслуговує до 127 вузлів
Радіус дії, м	10-100	30-100	50	30	150	3-100
Типи пристроїв чи ролі вузлів	Координатор, маршрутизатор, кінцевий пристрій	Координатор, маршрутизатор, ведений	Ведучий і ведений	Ведучий і ведений	Точка доступу, клієнт	Хост, периферійний пристрій
Піковий струм спожи-вання вузла, мА	<150	21 (режим пробудження) 36 (режим передачі)	12,5	17	116 (при 1,8В)	<500

- Для опорної локальної мережі збору та обробки інформації доцільно застосовувати стандарти 802.11n і 802.11ac з урахуванням кількості адаптерів та очікуваної пропускної здатності.
- 802.11ac забезпечує вищу швидкість передавання даних і краще підходить для мереж із підвищеним навантаженням.
- Під час проектування необхідно враховувати втрати в радіоканалі, підсилення антен, потужність передавача, відстань між об’єктами та частотний діапазон.

ВИСНОВКИ

- У роботі виконано огляд бездротових технологій передачі даних і визначено їх роль у системах збору та обробки інформації.
- Проаналізовано властивості стандартів WPAN, WLAN, WMAN і WWAN, а також характеристики Wi-Fi, Bluetooth LE, ZigBee, ANT+ та IEEE 802.11ah.
- Розглянуто механізми кіберзахисту Wi-Fi, зокрема WPA2, 802.1X, EAP, автентифікацію, шифрування та контроль вразливих точок доступу.
- Обґрунтовано практичні рекомендації щодо вибору бездротових технологій для локальної мережі збору інформації з урахуванням пропускної здатності, дальності, енергоспоживання та безпеки.
- Найбільш ефективне рішення має поєднувати продуктивні стандарти 802.11n/802.11ac для опорної мережі та енергоощадні технології для сенсорного рівня.