Plag

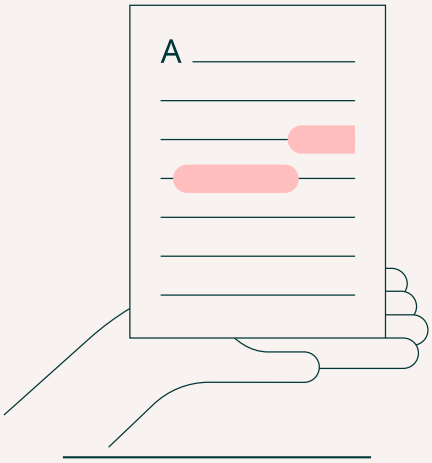
Звіт про оригінальність

● Оцінка схожості 16%

● Ризик плагіату НАЙВИЩИЙ

Olga Kagalo 2025-06-19 23:10

Посилання на звіт: 10mDL / Посилання користувача: qEAc



Ось вона –
Ваша звіт про оригінальність!

Ми раді повідомити, що перевірка вашого документа завершена, і результати вже готові! Наші алгоритми старанно працювали, щоб знайти збіги в наших базах даних.

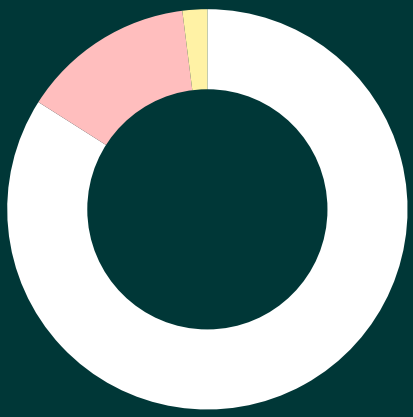
На наступних сторінках ви знайдете результати перевірки:

Бали
Збіги
Посилання

Ваш документ було перевірено за такими джерелами:

- ✓ База даних інтернет-джерел
- ✓ База даних наукових статей
- ○ Глибока перевірка (наш вдосконалений алгоритм)

Бали



Збіги тексту	14%
Перефразування	2%
Цитований текст	0%
Неправильне цитування	0%
Збігів не знайдено	84%

Ризик плагіату НАЙВИЩИЙ

Ризик плагіату вказує, як збіги тексту розподілені по документу. Вищий ризик виникає, коли збіги з'являються близько один до одного, наприклад, у тому самому абзаці або розділі.

Оцінка схожості %16

Оцінка схожості показує, скільки слів або символів у вашому документі збігаються з текстами інших документів, включаючи перефразовані тексти або неправильні цитати.

Збіги

1 ПРИНЦИПИ ДОСЛІДЖЕННЯ ТА ФУНКЦІОНУВАННЯ МЕРЕЖІ IOT

1.1 Основні поняття архітектура та терміни, що характеризують мережу IoT

Мережа наступного покоління (NGN) – це інфраструктура з пакетною комутацією, яка забезпечує послуги електрозв'язку та використовує різноманітні широкосмугові технології транспортування, у тому числі з функцією якості обслуговування (QoS). Вона надає послуги без залежності від конкретних технологій транспортування, що використовуються.

Пристрій – це технічний засіб, який має основні можливості зв'язку, а також додаткові функції, такі як вимірювання, виконання операцій, збереження та обробка даних.

Інтернет речей (IoT) – це глобальна мережа, яка об'єднує фізичні та віртуальні об'єкти, забезпечуючи їх взаємодію та спільне використання інформаційних технологій для надання різноманітних послуг.

Архітектура пристроїв Інтернету речей включає чотири основних рівні: рівень сенсорів, мережевий рівень, рівень обробки даних та додатковий рівень з використанням рис.1.1. Нижче наведено детальний опис кожного з цих рівнів.

Рисунок 1.1 – Структура мережі Інтернету речей

На рівні датчиків головною метою є збір інформації про різні параметри навколишнього середовища за допомогою різноманітних периферійних пристроїв. Цей рівень включає різні типи датчиків, які вимірюють різні параметри. Для ефективного збору та передачі даних з датчиків до оброблювального блоку пристрою, використовується концентратор датчиків. Концентратор є центральною точкою з'єднання для декількох датчиків і забезпечує передачу даних до оброблювального блоку. Для забезпечення зв'язку між датчиками та оброблювальним блоком використовуються різні транспортні механізми, такі як Inter-Integrated Circuit (I2C) або Serial Peripheral Interface (SPI). Ці механізми забезпечують передачу даних між датчиками та програмними додатками для збору та обробки інформації.

Датчики в пристроях Інтернету речей можуть бути класифіковані на три основні категорії:

– Датчики руху, вони вимірюють зміни у русі та орієнтації пристроїв. Тут можна виділити два типи рухів: лінійний та кутовий. Лінійний рух відноситься до прямолінійного переміщення пристрою, тоді як кутовий рух вимірює обертальні зміни.

– Датчики навколишнього середовища, ці датчики, такі як датчики світла та тиску, реагують на зміни у параметрах навколишнього середовища. Вони допомагають пристроям приймати автономні рішення відповідно до отриманих даних. Наприклад, вони застосовуються у розумних замках, системах домашньої автоматизації та освітленні.

– Датчики місцезнаходження, ці датчики взаємодіють з фізичним розташуванням пристрою. Серед них можна виділити магнітні датчики, які допомагають фіксувати орієнтацію пристрою, та GPS-датчики, які використовуються для навігаційних цілей.

Мережевий рівень в мережі IoT використовується для забезпечення комунікаційного каналу між датчиками та іншими підключеними пристроями. Цей рівень реалізується через різноманітні комунікаційні технології, такі як Z-Wave, LoRa, Wi-Fi, Bluetooth та інші, що дозволяють ефективно передавати дані між різними пристроями всередині мережі IoT.

Рівень обробки даних в мережі IoT відповідає за аналіз та обробку зібраних даних, які надходять від датчиків. Цей рівень виконує аналіз і приймає рішення на основі результатів обробки. У більшості IoT пристроїв, таких як смарт-годинники, розумні домашні системи та інші, рівень обробки даних також може зберігати отримані результати для подальшого використання. Крім того, він може передавати оброблені дані з одного пристрою на інший через мережевий рівень.

Рівень додатків в мережі IoT відображає результати аналізу та обробки даних, що проводиться на рівні обробки даних, за допомогою різних додатків на пристроях IoT. Цей рівень орієнтований на користувачів і відповідає за виконання різноманітних завдань для них. Наприклад, через рівень додатків користувач може керувати розумним будинком, взаємодіяти з розумними транспортними системами та виконувати інші завдання, пов'язані зі зручністю та автоматизацією в їхньому повсякденному житті.

1.2 Основний механізм функціонування Інтернету речей

На рис. 1.2 зображено схему простої мережі Інтернету речей (IoT). Найпростіша мережа IoT може складатися з трьох основних компонентів: сенсорів, які збирають дані, пристроїв для передачі цих даних (наприклад, мікроконтролерів або модулів зв'язку) і

сервера або хмари, де дані аналізуються та обробляються.

Рисунок 1.2 – Структура IoT

Сенсори розміщені у середовищі, яке вони моніторять (наприклад, в землі для вимірювання вологості, в промисловому обладнанні для виявлення відхилень у роботі тощо). Вони збирають дані про стан оточуючого середовища, які потім передаються через пристрої передачі даних.

Пристрої передачі даних можуть бути зв'язаними з сенсорами безпосередньо або через бездротові мережі, такі як Wi-Fi, Bluetooth, або навіть через провідне підключення. Вони отримують дані від сенсорів і пересилають їх до сервера або хмари, де дані обробляються.

Сервер або хмара приймає дані від пристроїв передачі даних, аналізує їх і може вживати різні заходи, такі як зберігання, візуалізація або навіть надсилання команд для керування пристроями на основі зібраних даних.

Принцип роботи Інтернету речей (IoT) ґрунтується на наступних основних етапах:

– Сенсорний рівень. 9 На цьому етапі дані збираються за допомогою різноманітних сенсорів або пристроїв зібрання інформації. Ці дані можуть включати інформацію про температуру, вологість, рух, освітлення тощо.

– Мережевий рівень. Після збору даних вони передаються через мережу до центрального вузла або хмарного сервісу для подальшої обробки та аналізу.

– Обчислювальний рівень. 9 На цьому етапі дані обробляються, аналізуються та інтерпретуються. Можливі дії 9 на цьому етапі включають у себе фільтрацію даних, виявлення патернів та виконання різних алгоритмів аналізу даних.

– Дієвий рівень. Після обробки дані можуть бути використані для прийняття рішень або взаємодії зі світом. Це може включати автоматизацію пристроїв, надсилання повідомлень або звітів, керування системами тощо.

На першому етапі роботи IoT датчики або пристрої збирають різноманітні дані з оточуючого середовища. Це можуть бути прості вимірювання, такі як температура або вологість, або складніше, наприклад, запис відео на відеокамеру відеоспостереження.

9 Крім того, на цьому етапі можуть використовуватися не лише датчики, але й різноманітні пристрої. Наприклад, смартфон – це пристрій, обладнаний кількома датчиками (камера, акселерометр, GPS тощо). Смартфон виконує роль не лише датчика, а й комплексного пристрою, здатного аналізувати та обробляти дані.

Таким чином, 9 на цьому етапі інформація збирається з навколишнього середовища за допомогою датчиків або пристроїв, які можуть виконувати різні функції, що допомагають збирати дані для подальшої обробки та аналізу.

На другому етапі роботи IoT дані, зібрані датчиками або пристроями, передаються до хмарних сховищ за допомогою різних методів зв'язку. Це може включати стільникові мережі, супутникові мережі, Wi-Fi, Bluetooth, технології малопотужних широкосмугових мереж (LPWAN), або підключення безпосередньо до Інтернету через Ethernet.

Кожен метод підключення 16 має свої переваги та обмеження, такі як споживання енергії, діапазон покриття та пропускна здатність. 16 Вибір конкретного методу залежить від конкретних вимог і умов використання IoT в конкретній області.

Незалежно від методу підключення, головна мета - це передача даних до хмарного сховища для подальшої обробки, аналізу та використання. Це дозволяє зберігати дані в безпечному та доступному місці, забезпечуючи їх доступність з будь-якого пристрою або місця через Інтернет.

Після того, як дані потрапляють до хмарного сховища, вони піддаються обробці за допомогою програмного забезпечення. Цей процес може включати різноманітні операції, спрямовані на аналіз, інтерпретацію та використання отриманих даних.

Наприклад, програмне забезпечення може виконувати аналіз отриманих даних для виявлення певних патернів або трендів. Це може включати перевірку температурних даних на відповідність певним стандартам або порівняння їх з попередніми вимірами для виявлення змін.

Крім того, обробка даних може включати ідентифікацію об'єктів на відео, отриманому з камери відеоспостереження. Наприклад, програмне забезпечення може використовувати алгоритми комп'ютерного зору для виявлення рухомих об'єктів або навіть розпізнавання осіб для забезпечення безпеки в приміщенні.

На етапі передачі інформації на інтерфейс користувача, інформація яка була оброблена і аналізована, передається кінцевому користувачеві через різні інтерфейси. Це може включати сповіщення користувача, такі як електронні листи, текстові повідомлення або сповіщення в додатках. 26 Наприклад, користувач може отримати текстове повідомлення, яке попереджає його про високу температуру в холодильному приміщенні його компанії.

Крім цього, користувач може мати доступ до інтерфейсу, через який він може активно перевіряти систему. Це може бути мобільний додаток або веб-сторінка, через які користувач може перевірити стан системи, наприклад, переглянути відеозаписи з відеоспостереження в своєму будинку.

Проте це лише частина можливостей. Залежно від програми IoT, користувач може взаємодіяти з системою на відстані та впливати на її роботу. Наприклад, він може дистанційно регулювати 26 температуру в приміщенні за допомогою мобільного додатка на своєму телефоні.

Деякі дії можуть виконуватися автоматично, без прямого втручання користувача. 21 Наприклад, система може автоматично регулювати температуру в приміщенні відповідно до попередньо встановлених правил або повідомляти відповідні служби про події безпеки без необхідності у втручанні користувача.

Отже, система IoT забезпечує передачу корисної інформації користувачеві через різноманітні канали зв'язку та надає можливості для взаємодії та контролю за системою як на відстані, так і автоматично.

1.3 Розгляд моделі IoT згідно рекомендації Y.2060

На рис. 1.3 показана стандартна модель 20 Інтернету речей (IoT) [4], яка описана в рекомендаціях Y.2060. Ця модель складається з чотирьох основних рівнів, а також з двох додаткових рівнів: рівня управління та рівня безпеки.

Основні рівні включають:

– Рівень застосування. Цей рівень охоплює всі різноманітні застосування Інтернету речей, включаючи промислові, побутові, медичні та інші.

– Рівень підтримки послуг та додатків. На цьому рівні забезпечується інфраструктура для підтримки різноманітних послуг та додатків, що працюють в середовищі Інтернету речей.

– Мережевий рівень. Цей рівень включає в себе мережеві технології, необхідні для забезпечення зв'язку між пристроями та системами в Інтернеті речей.

– Рівень пристроїв. На останньому рівні знаходяться самі пристрої, які 20 збирають, обробляють та передають дані.

20 Додаткові рівні включають:

– Рівень управління. Цей рівень відповідає за управління ресурсами, конфігурацією та координацію різноманітних компонентів системи Інтернету речей.

– Рівень безпеки. Останній рівень забезпечує захист від різних загроз та атак на систему Інтернету речей, включаючи захист від несанкціонованого доступу, втрати даних та інших потенційних загроз.

Рисунок 1.3 – Еталонна модель IoT

Прикладний рівень в Рекомендації Y.2060 не розглядається.

– Можливості транспортування, які забезпечують з'єднання для передачі даних, пов'язаних з послугами та додатками IoT, а також інформації щодо контролю та управління, пов'язаних з IoT.

Рівень пристроїв має різноманітні можливості, які можна логічно розділити на два види:

1. Можливості пристроїв:

– Пряма взаємодія 10 з мережею зв'язку, пристрої можуть збирати та передавати інформацію безпосередньо у мережі зв'язку, не використовуючи шлюз.

– 10 Непряма взаємодія з мережею зв'язку, пристрої можуть 10 взаємодіяти 10 з мережею зв'язку через шлюз. Це дозволяє пристроям отримувати та передавати інформацію за допомогою шлюзу, який обробляє комунікацію з мережею.

– Режим сну та пробудження, пристрої можуть мати можливість входити у режим сну для збереження енергії та пробудження для виконання завдань.

2. Можливості шлюзу:

– 10 Підтримка декількох інтерфейсів, шлюз може підтримувати різні дротові та бездротові технології для з'єднання з пристроями.

– Перетворення протоколу, шлюз може конвертувати протоколи, щоб забезпечити 17 сумісність між різними пристроями та мережами зв'язку. Наприклад, він може перетворювати протоколи на рівні пристроїв або мережевому рівні для забезпечення взаємодії між пристроями з різними технологіями.

Можливості управління в контексті Інтернету речей (IoT) включають традиційні класи 3 управління несправностями, конфігурацією, обліком, показниками роботи та безпекою (FCAPS), що аналогічні засобам управління в традиційних мережах зв'язку.

Можливості управління IoT можна розділити на загальні та спеціалізовані:

1. Загальні можливості управління включають:

– Управління пристроями: дистанційне керування пристроями, 17 діагностика, 3 оновлення прошивки та програмного забезпечення, а також контроль стану пристроїв.

– 3 Управління топологією локальної мережі.

3 – Управління трафіком і навантаженнями: виявлення умов перевантаження мережі та 3 реалізація резервування ресурсів для термінових або життєво важливих потоків трафіку.

3 2. Спеціалізовані можливості управління тісно пов'язані з вимогами конкретних додатків IoT, таких як:

– Контроль 3 лінії передачі електроенергії в розумних електричних мережах.

Можливості забезпечення безпеки поділяються на два види: загальні та спеціалізовані.

3 Загальні можливості забезпечення безпеки, які не залежать від конкретних додатків, включають:

– На рівні застосування, авторизація, автентифікація, збереження конфіденційності та цілісності даних, захист приватності, 17 аудит безпеки та застосування антивірусних програм.

– На мережевому рівні, 17 авторизація, автентифікація, 3 захист конфіденційності та цілісності даних передачі та сигналізації.

– На рівні пристроїв, автентифікація, 3 авторизація, перевірка цілісності пристрою, управління доступом, захист конфіденційності та цілісності даних.

3 Спеціалізовані можливості забезпечення безпеки тісно пов'язані з вимогами конкретних 3 додатків, наприклад, забезпечення 3 безпеки мобільних платежів або інших конкретних сценаріїв застосування.

1.4 Переваги та недоліки IoT

До переваг Інтернету речей можна віднести:

– Взаємозв'язок між пристроями. IoT сприяє взаємодії між пристроями, що відомо як зв'язок між машинами (M2M). Це 23 сприяє покращенню комунікації та співпраці між різними пристроями, що в результаті забезпечує більшу ефективність та зручність у використанні. Такий зв'язок дозволяє фізичним пристроям залишатися підключеними та співпрацювати один з одним, що робить систему більш гнучкою та функціональною.

– Переваги в області автоматизації та управління в IoT полягають у можливості підключення та керування фізичними об'єктами через цифрові технології та бездротову інфраструктуру. Це відкриває широкі можливості для автоматизації процесів та

контролю за ними. Без необхідності втручання людини, пристрої можуть взаємодіяти один з одним, що пришвидшує та удосконалює обмін інформацією.

– Перевага в області інформації в IoT полягає у тому, що доступ до більшої кількості даних допомагає у прийнятті кращих рішень. Незалежно від того, чи маєте ви потребу у знаннях щодо продуктів у магазині, чи ж потрібно оцінювати запаси в компанії, наявність інформації надає вам перевагу у вирішенні проблем і оптимізації процесів.

– Перевага моніторингу в IoT полягає в здатності точно вимірювати та відстежувати різні параметри. Наприклад, моніторинг може допомогти визначити кількість залишків товарів або якість повітря у приміщенні. Це надає користувачеві додаткову інформацію, яка раніше була важко доступною. Наприклад, якщо ви знаєте, що у вас закінчується молоко або чорнила для принтера, ви можете запланувати свої покупки заздалегідь, що дозволяє економити час та зусилля. Крім того, моніторинг термінів придатності продуктів може сприяти підвищенню безпеки.

– Перевага економії часу в IoT полягає в можливості оптимізувати рутинні процеси та забезпечувати швидший доступ до інформації. У сучасному світі, де час – цінний ресурс, IoT дозволяє нам ефективніше використовувати цей ресурс, звільняючи час для важливіших справ і розваг.

– Економія грошей є ключовою перевагою використання IoT. Ця технологія дозволяє оптимізувати використання енергії та ресурсів, запобігаючи витратам на непотрібне витрачання. Завдяки моніторингу та попередженню можливих проблем або поломок, IoT дозволяє ефективно управляти та зберігати енергію та ресурси, що веде до значних економічних вигод. Крім того, заощадження коштів на витрати на обладнання для з'єднання та моніторингу також сприяє широкому прийняттю IoT, що в свою чергу сприяє підвищенню ефективності та зменшенню витрат у повсякденній діяльності людей.

– Автоматизація завдань за допомогою IoT є важливою перевагою цієї технології. Вона дозволяє контролювати та автоматизувати рутинні процеси без прямого втручання людини. Зв'язок між пристроями, відомий як M2M, сприяє збереженню прозорості в процесах та рівномірному розподілу завдань. Це також сприяє підтримці високої якості обслуговування (QoS). Завдяки IoT ми можемо автоматично реагувати на надзвичайні ситуації та вживати необхідні заходи для їх вирішення.

– Взаємодія між пристроями сприяє підвищенню ефективності роботи. Це дозволяє швидко отримувати точні результати завдяки автоматизації процесів. Такий підхід дозволяє зекономити час, який можна витратити на виконання інших, більш творчих завдань, замість повторення однотипних робіт щодня.

– Завдяки IoT покращується якість життя через підвищення комфорту, зручності та ефективного управління. Ця технологія дозволяє створити сприятливіші умови для життя, забезпечуючи доступ до різноманітних сервісів та оптимізуючи використання ресурсів.

До недоліків Інтернету речей можна віднести:

– У зв'язку з підключенням пристроїв різних виробників до однієї мережі виникає проблема сумісності, яка може ускладнити їх з'єднання та моніторинг. Хоча узгодження загального стандарту може сприяти зниженню цього недоліку, технічні питання все ще залишатимуться актуальними. Навіть за наявності пристроїв 1 з підтримкою Bluetooth можуть 1 виникати проблеми сумісності. 1 Це може призвести до обмеження вибору споживачів та сприяти монополізації ринку деякими виробниками.

– IoT мережа складна і різноманітна, що може створювати виклики в управлінні та підтримці. Навіть найменші помилки в програмному або апаратному забезпеченні можуть мати 1 серйозні наслідки. Навіть випадкове відключення живлення 8 може призвести до порушень у роботі системи.

Наприклад, уявіть ситуацію, коли ваша розумна система повідомляє вас і вашу дружину 1 про те, що молоко 1 закінчилося. 1 Ви обидва зупиняєтеся в магазині, щоб 1 купити молоко 1 на шляху додому, не 1 знаючи, що робить інший. 1 Це може призвести до непотрібних витрат і перевитрати ресурси.

Також можливі сценарії, коли 1 помилка в програмному забезпеченні призводить до надмірного замовлення товарів або послуг. Наприклад, якщо система автоматично замовляє нові картриджі 1 для принтера кожну годину протягом декількох днів, навіть коли вам потрібна лише одна заміна, це може викликати витрати, які можна було уникнути.

– За допомогою автоматизації рутина стає менш залежною від людської присутності, що 8 може вплинути на зайнятість некваліфікованих працівників. Внаслідок цього можуть виникнути проблеми з безробіттям 1 в суспільстві. Ця ситуація може бути вирішена шляхом введення високоякісної освіти 8 та перепідготовки працівників, щоб вони могли адаптуватися до змін на ринку праці.

8 Автоматизація може знизити потребу у людських ресурсах, зокрема серед робітників та менш освічених працівників. Це може спричинити проблеми з безробіттям, але одночасно відкриває можливості для створення нових видів робіт, пов'язаних з розвитком та підтримкою автоматизованих систем. Важливою є не тільки адаптація людей до змін, але й створення нових можливостей для їхнього професійного росту.

– З технологічними інноваціями наше життя стає все більш залежним від цифрових рішень, що 8 може вплинути на нашу незалежність та приватність. 1 Молоде покоління вже звикло до того, що багато аспектів їхнього життя контролюються за допомогою технології, такої як доступ до Інтернету через Wi-Fi. Важливо зрозуміти, який рівень автоматизації та контролю над нашими життями ми готові прийняти, зберігаючи баланс між зручністю та приватністю.

– Зі збільшенням обсягу даних, які обробляються в рамках Інтернету речей, зростає й ризик порушення конфіденційності. Наприклад, в разі виникнення помилок у роботі системи можливе навіть відкриття особистої інформації перед сторонніми. Це може включати такі деталі, як ваше фінансове становище чи покупки, здійснені вами в магазині, що може порушити вашу приватність та безпеку.

– З поширенням Інтернету речей зростає загроза безпеці. Пристрої побутового та промислового призначення, а також інфраструктура державного сектору стають більш вразливими перед потенційними кібератаками. Це може призвести до несанкціонованого доступу до особистих та конфіденційних даних, що становить серйозну загрозу як для приватності, так і для безпеки користувачів.

Після ретельного 4 аналізу переваг та недоліків моделі IoT можна прийти до висновку, що хоча переваги переважають над недоліками, проблеми 4 безпеки та конфіденційності залишаються серйозними перешкодами для повноцінного впровадження цієї технології. Тим не менш, ці проблеми не є невирішеними, і вони продовжують привертати увагу виробників та дослідників. Шлях до безпечного та приватного використання IoT вимагає спільних зусиль у сфері розробки стандартів безпеки, застосування шифрування даних та захисту від кіберзагроз.

2 ДОСЛІДЖЕННЯ ТА 4 АНАЛІЗ ПРОТОКОЛІВ ТА ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ У МЕРЕЖАХ IOT

4 2.1 Передача 4 даних 4 в IoT мережах за допомогою новітніх технологій та протоколів на великі відстані

2.1.1 LoRaWAN

У перспективі, з поширенням Інтернету речей, значна кількість пристроїв буде працювати на батарейках, тому довга автономність стане ключовою характеристикою. Для цього були розроблені 4 нові мережі, спеціально адаптовані 4 під потреби IoT, такі як 4 LPWAN (Long Power Wide Area Network). Ці мережі використовують різні технології, такі як 4 NB-IoT, Weightless, LoRa, SIGFOX та інші, для підключення широкого спектру пристроїв, які збирають дані для хмарних серверів[9].

Технологія LoRa відкриває можливість 13 демодулювати сигнали на рівні, що низьше

на 20 дБ порівняно з рівнем шумів, що є великим покращенням у порівнянні з більшістю систем, що використовують частотну маніпуляцію (FSK), які працюють на рівні 8-10 дБ вище рівня 13 шумів. Модуляція LoRa може бути використана на фізичному рівні в різних типах мереж – від mesh-мереж і мереж зірки до точка-точка та інших.

Завдяки високій чутливості (148dbm), 13 LoRa ідеально підходить для 13 пристроїв, які вимагають 13 низького споживання електроенергії та мають великі відстані між собою.

– 12 Двонаправлені кінцеві пристрої "класу С" з максимальним приймальним вікном (Bi-directional End Devices, Class C). Ці пристрої мають безперервне вікно для прийому даних, яке закривається лише під час передачі. Вони ідеально підходять для завдань, які вимагають постійного прийому 12 великого обсягу даних.

12 Рисунок 2.1 – Типи пристроїв LoRaWAN

Ці компоненти працюють разом для забезпечення зв'язку та обробки даних 12 у мережі LoRaWAN, як показано на рис. 2.2.

Рисунок 2.2 – Архітектура мережі LoRaWAN

Сервер програм (Application Server) – це пристрій, спрямований на збір інформації від кінцевих вузлів та здійснення віддаленого контролю їх роботи.

– Особливостям топології мережі, яка дозволяє ефективно координувати та обробляти дані від багатьох пристроїв.

– Адаптивній 12 швидкості передачі даних та адаптивній вихідній потужності пристроїв, які регулюються мережевим вузлом для оптимального використання ресурсів.

– Тимчасовому поділу доступу до середовища, що дозволяє кінцевим пристроям взаємодіяти з шлюзом у визначених інтервалах часу.

– Частотному поділу каналів, що дозволяє розділити доступ до радіочастотного спектру між різними пристроями.

– Особливостям LoRa модуляції, що дозволяє одночасно демодулювати сигнали на різних швидкостях передачі в одному частотному каналі.

Поява енергоефективних бездротових технологій, таких як LoRaWAN, зробила можливим будівництво глобальних мереж передачі даних, що є водночас простими в

реалізації. Їх важливі переваги включають розширений радіус дії, довгий час автономної роботи та надійне виявлення корисного сигналу навіть у присутності перешкод.

2.1.2 SigFox

Технологія SigFox відкриває нові можливості для розбудови мереж та стратегій зв'язку в Інтернеті речей. Розроблена групою з Labège, Франція, компанія SigFox є мережевим оператором, спеціалізованим на впровадженні IoT у бізнес та промисловість. Архітектура мережі SigFox схожа на традиційні стільникові мережі, такі як GSM та GPRS, проте вона відрізняється меншою вартістю та більшою енергоефективністю.

Мережа SigFox покриває зону приблизно 30-50 км у міських та сільських районах. У містах, де є багато електромагнітних шумів, діапазон роботи скорочується до 3-10 км.

На рис. 2.3 зображена архітектура мережі технології SigFox [13]. Загальна топологія мережі розроблена для створення масштабованої, високопродуктивної системи з дуже низьким енергоспоживанням.

SigFox використовує надвузьку смугу частот UNB (Ultra Narrow Band) для підключення пристроїв до глобальної мережі. Використання UNB є ключовим фактором для забезпечення дуже низької потужності передавача, яка використовується для створення надійного з'єднання та передачі даних.

Пристрої надсилають свої дані до базової станції SigFox. Це відбувається за допомогою протоколу point-to-point (P2P). Після цього базова станція підключається до Інтернет бази даних, де дані декодуються і надсилаються. Нарешті, хмарний сервер SigFox розсилає ці дані до клієнтських серверів та платформ через API.

Рисунок 2.3 – Архітектура мережі SigFox

Технологія SigFox розроблена для ефективного використання в ситуаціях, де важливо забезпечити доступність зв'язку за низьку ціну та великій зоні покриття. Існує багато сфер, де можна використовувати цю бездротову технологію:

– Системи дому та розподілених споживчих товарів;

– Системи енергетичних мереж та зв'язку;

– Застосування в медичній сфері для моніторингу здоров'я;

– Транспортні системи та моніторинг руху транспорту;

– Віддалений моніторинг і контроль різних процесів та систем;

– Системи безпеки та захисту об'єктів.

Стандарт SigFox 18 має ряд переваг порівняно з іншими базовими технологіями LPWAN мереж. Деякі з них:

Переваги:

– велика зона покриття;

– висока проникність сигналу через перешкоди;

– довгий термін служби від однієї батареї, можливо до 20 років роботи сенсора на двох батареях AA;

– низьке енергоспоживання;

– низька вартість.

Незважаючи на ці переваги, технологія SigFox також має деякі обмеження:

– низька швидкість передачі даних;

– залежність від існуючої стільникової інфраструктури;

– обмежена стійкість до перешкод.

В більшості країн Європи та США ця технологія дійсно є популярною через свою енергоефективність та доступність.

2.1.3 NB-IoT

Технологія NB-IoT розглядається як крок у напрямку розвитку стільникового зв'язку для потреб Інтернету речей. Вона представляє собою бездротовий варіант глобальних мереж з низьким споживанням енергії і розроблена 1 для взаємодії між пристроями M2M.

NB-IoT може працювати в практично всіх тих же діапазонах 1 частот, що і 2G/3G/4G в "низьких" діапазонах, таких як 800МГц, 900МГц і 1800МГц. Використання більш високих частот 18 може призвести до більшого затухання сигналу, тому вони не так часто використовуються для NB-IoT.

Існують 1 три способи виділення частотного ресурсу для NB-IoT:

1 1.Stand-Alone 1 (автономний):

1 – 1 В цьому випадку виділяється частотний канал шириною в 200 кГц. Цей метод є найбільш ефективним 1 для роботи NB-IoT, але вимагає 1 значних ресурсів. Для його реалізації 1 може знадобитися від 300 до 600 кГц цінного спектру, включаючи захисні інтервали. У такому випадку взаємні перешкоди 1 з іншими технологіями мінімізуються 1 рис. 2.4.

1 Рисунок 2.4 – 1 Варіанти розміщення NB-IoT в режимі Stand - Alone

1 В полосі Band (в середині) використовуються ресурси для NB-IoT всередині наявної LTE несучої. Проте, 1 NB-IoT несуча має значно вищу потужність на 6 дБ порівняно з LTE ресурсами. Цей підхід сприяє ефективній утилізації частотних ресурсів, але може виникнути 1 проблема взаємного впливу з LTE мережею рис. 2.5.

1 Рисунок 2.5 – 1 Розміщення Nb IoT в режимі in Band

1 У захистній полосі частот NB-IoT 1 працює 1 в так званому захистному інтервалі. Наприклад, у смузі LTE 10 МГц, 1 500 кГц вільного спектру використовується 1 як захистний інтервал. Аналогічно режиму 1 In Band, для забезпечення 1 більшої дальності передачі, 1 NB-IoT несуча має підвищену потужність на 6-9 дБ порівняно з ресурсними блоками LTE рис. 2.6. Цей підхід дозволяє ефективно використовувати частотний ресурс та зменшує взаємний вплив на LTE мережу. Однак, 1 у цьому випадку може 1 відбуватися погіршення показників позамагістральних 1 випромінювань для LTE.

1 Рисунок 2.6 – Розміщення NB-IoT в режимі Guard Band

1 Weightless-P – це LPWAN технологія, спеціально розроблена для Internet of Things (IoT). Вона застосовується там, де необхідна довготривала робота 1 від одного заряду батареї, двонаправлений зв'язок і висока щільність кінцевих пристроїв.

У відміну 1 від інших технологій, базова 1 станція в Weightless-P має 1 повний 1 контроль над своєю мережею і кінцевими пристроями у будь-який момент. Це робить її більш розвиненою технологією порівняно з іншими LPWAN рішеннями.

Weightless-P забезпечує 14 гарантовану доставку повідомлень, що дозволяє уникнути необхідності відправляти повідомлення кілька разів, як у LoRa та SigFox. Це призводить до економії заряду пристроїв і підвищує ефективність використання енергії.

Крім того, у Weightless-P 14 використовується метод підтримки адаптивної швидкості передавання інформації, що 24 призводить до збільшення тривалості 14 роботи батареї та підвищує 14 продуктивність мережі.

1 Порівняльна характеристика технологій передачі даних на довгі відстані в мережі

IoT.

1 Таблиця 2.1 1 – 1 Порівняння основних технічних характеристик мереж з високою дальністю дії LPWAN

1 Характеристика

LoRaWAN

SigFox

NB-IoT

Weightless-P

Частотний діапазон

Sub-1 GHz

868 MHz (EU), 915 MHz (US)

Licensed bands

Sub-1 GHz

24 Швидкість передачі даних

24 Декілька кбіт/с (залежно від налаштувань)

До 100 біт/с

До 250 кбіт/с

До 100 кбіт/с

Дальність зв'язку

Декілька кілометрів до декількох десятків кілометрів

До 30-50 км (в лінії видимості)

Декілька кілометрів

Декілька кілометрів

Енергоефективність

Висока

Висока

Висока

Висока

Масштабованість мережі

Велика кількість підключених пристроїв

Велика кількість підключених пристроїв

Велика кількість підключених пристроїв

Велика кількість підключених пристроїв

2.2 Можливості бездротового зв'язку в інтернеті речей на малих відстанях

2.2.1 Z-Wave

Z-Wave – це бездротова технологія з низьким енергоспоживанням для передачі даних в інтернеті речей (IoT). Вона працює на частоті до 1 ГГц та спеціалізується на передачі простих команд для керування пристроями з мінімальними затримками. Вибір цієї частоти має на меті уникнути перешкод 2 від інших технологій, які вже використовуються в повсякденному житті, таких як Wi-Fi, особливо на частоті 2,4 ГГц.

Технологія Z-Wave – це рішення для повноцінного контролю над безпекою та енергоефективністю вашого будинку, з мінімальними турботами. Завдяки Z-Wave ви можете створити власну систему автоматизації, що охоплює освітлення, опалення, кондиціонування повітря, кухонні прилади та навіть системи безпеки. Ця технологія проста у використанні, енергоефективна та допомагає зекономити час.

Ця система працює через дистанційне керування і використовує радіосигнали з низькою потужністю. Завдяки своїй сіткоподібній структурі, вона охоплює всі зони будинку, проникаючи через стіни, поверхні та меблі. Це забезпечує практично 100% надійне з'єднання.

2.2.2 NFC

Безконтактна технологія NFC відрізняється від інших тим, що дає можливість двостороннього 2 обміну даними між двома активними пристроями, а не тільки передачі інформації від активного до пасивного. Її також застосовують під час роботи з радіочастотною ідентифікацією (RFID) — це дає змогу перевіряти правильність

цифрового протоколу та забезпечувати сумісність між картами RFID й мобільними пристроями. У цьому процесі аналізують найбільш істотні характеристики радіосигналу, зокрема часові показники, чутливість 2 приймача в активному режимі й 2 амплітуду несучого сигналу.

2 Рисунок 2.7 2 – Принцип роботи NFC

2 У процесі передачі інформації від активного до пасивного пристрою застосовується амплітудна маніпуляція ASK. Обидва пристрої рівноцінно функціонують та кожний із них забезпечений власним джерелом живлення. Після завершення обміну даними несучий сигнал вимикається. В результаті індуктивної взаємодії пасивний пристрій впливає на активний, змінюючи його імпеданс, що проявляється у змінах амплітуди або фази напруги на антені активного пристрою. Електромагнітний зв’язок розривається й обмін даними припиняється, щойно відстань між пристроями перевищить приблизно 20 см.

На практиці, NFC можна розглядати як розширення вже добре відомої технології радіочастотної ідентифікації RFID. RFID широко використовується в безконтактних картах та мітках. Однак NFC відрізняється тим, що вона не лише може зчитувати інформацію з пасивних електронних міток, але й забезпечує можливість двостороннього бездротового зв'язку між пристроями.

2.2.3 RFID

RFID (Radio Frequency Identification) — технологія автоматичної ідентифікації об’єктів за допомогою радіохвиль. Вона дає можливість зчитувати й записувати інформацію, розташовану в спеціальних транспондерах, що називаються RFID-мітками. Кожна система RFID містить пристрій зчитування (рідер) та транспондер (мітку).

Більшість RFID-міток складається із двох головних компонентів. Перший — інтегральна схема, яка забезпечує обробку та збереження інформації, а також демодуляцію й модуляцію радіосигналу. Другий — антена, завдяки чій роботі відбувається прийом та відправлення цих сигналів. Ефективне використання цієї технології можливе завдяки спеціалізованому програмному забезпеченню, що опрацьовує та збирає дані, отримані від транспондерів.

Розрізняють активні й пасивні RFID-мітки. Активні містять джерело електроживлення, завдяки чому можуть ініціювати передачу сигналу та розпізнаватися на великих відстанях. Пасивні покладаються на зовнішній сигнал від зчитувача для активації та відправлення своїх данних.

Рисунок 2.8 2 – Будова RFID-мітки

RFID-мітки застосовуються у різних галузях, включаючи управління товарними запасами та відстеження часу на спортивних змаганнях. Вони доповнюють систему штрих-кодів, надаючи можливість дистанційного зчитування. Мітки використовуються для маркування великої рогатої худоби з метою запису інформації про ветеринарний огляд. У транспортній галузі вони допомагають ідентифікувати автомобілі, навіть якщо вони рухаються на великій швидкості, а також використовуються авіалініями для ефективного відстеження багажу. Крім того, технологія RFID вбудовується у біометричні паспорти та кредитні картки для безпечного доступу до захищених областей.

Деякі RFID-мітки можуть бути зчитані на відстані декількох метрів від пристрою зчитування навіть без прямої видимості. Більшість міток містять текстовий запис та штрих-код як додаткові дані для прямого зчитування у випадках, коли радіочастотна електроніка недоступна.

2.2.4 Bluetooth Low Energy

Bluetooth Low Energy (BLE) – це частина Bluetooth специфікації, яка була вперше представлена у версії Bluetooth 4.0 і продовжує свій розвиток з Bluetooth 5.0. Пристрої, які використовують BLE, відзначаються низьким енергоспоживанням порівняно з попередніми версіями Bluetooth. Це дозволяє багатьом пристроям працювати протягом довшого часу без заряджання на одній невеликій батарейці типу "таблетка". За допомогою BLE можна використовувати компактні датчики, які постійно працюють і взаємодіють з іншими пристроями, що розширює можливості IoT та мобільних додатків.

BLE має три основних рівні:

1. Додатковий рівень, він відповідає за реалізацію функціональності, корисної для кінцевого користувача. На цьому рівні розробляються програми та додатки, що використовують можливості Bluetooth Low Energy.

2. Основний пристрій, або хост. Цей рівень надає верхній шар стеку протоколів Bluetooth. Він відповідає за керування взаємодією між додатками та контролером Bluetooth.

3. Контролер. Контролер відповідає за нижні рівні стеку протоколів Bluetooth. Він забезпечує безперервну роботу пристроїв на фізичному рівні та здійснює обробку радіочастотних сигналів.

Рисунок 2.9 – Архітектура BLE

У стеку протоколів Bluetooth Low Energy (BLE) рівень додатків є найвищим. Рівень хосту

включає такі підрівні:

– GAP 2 (Generic Access Profile) – відповідає за налаштування з'єднання та забезпечення загального доступу до пристрою.

– GATT 2 (Generic Attribute Profile) – визначає правила взаємодії та обміну даними між пристроями за допомогою атрибутів.

– ATT (Attribute Protocol) – забезпечує передачу даних між пристроями через атрибути.

– SM (Security Manager) – відповідає за управління безпекою та аутентифікацію пристроїв.

– 22 L2CAP (Logical Link Control and Adaptation Protocol) – забезпечує логічний контроль з'єднання та адаптацію для різних типів даних.

– HCI (Host Controller Interface) – інтерфейс хост-контролера, що дозволяє взаємодіяти з контролером Bluetooth на стороні хосту.

На рівні контролера використовуються такі рівні:

– HCI (Host Controller Interface) – це інтерфейс між хостом і контролером Bluetooth, який дозволяє хосту керувати контролером.

– LL (Link Layer) – канальний рівень, що забезпечує управління з'єднаннями та передачу даних на фізичному рівні.

– PHY (Physical Layer) – фізичний рівень, який відповідає за обробку радіочастотних сигналів та їх перетворення в цифрові дані і навпаки.

Bluetooth Low Energy (BLE) призначений для пристроїв з обмеженими ресурсами, такими як невеликі мобільні пристрої, де важлива компактність та енергоефективність. У порівнянні з класичними Bluetooth рішеннями, BLE споживає на 10-20 разів менше енергії, що дозволяє працювати пристроям протягом тривалого часу без необхідності заряджання. Крім того, він здатний передавати дані швидше - на 50 і більше разів, та на більші відстані, до 100 метрів, що робить його ідеальним вибором для реалізації різноманітних IoT та мобільних додатків.

Поміж переліченими вище перевагами, BLE відзначається також високою безпечністю, надійністю та низькою затримкою при підключенні. Ще однією важливою особливістю цього стандарту є його адаптивність у налаштуванні частоти. BLE автоматично переналаштовує свою робочу частоту для уникнення помилок передачі сигналу. Ця здатність дозволяє швидко адаптуватися до змін у середовищі, вибираючи оптимальну

частоту для мінімізації перешкод, уникнення переповнення та зниження інтерференції.

Bluetooth 5.0 був спеціально розроблений з урахуванням потреб Інтернету речей (IoT), що свідчить про його амбіції у захопленні ринку пристроїв. У порівнянні з попередньою версією 4.0, Bluetooth 5.0 значно підвищив швидкість передачі даних, наближаючись до швидкостей, що характерні для технологій HSPA і LTE, при цьому енергоспоживання залишалося на попередньому рівні. Це особливо важливо для будівництва мереж IoT, де енергоефективність має велике значення. Наразі, хоча специфікація Bluetooth 5.0 ще не так поширена, як попередні версії, з часом це може змінитися. Bluetooth 5.0, як і попередні версії, забезпечує зворотну сумісність, що робить його привабливим вибором для розвитку мобільних технологій у майбутньому.

2.2.5 Wi-Fi HaLow

Wi-Fi HaLow розширює можливості бездротового зв’язку, забезпечуючи підключення пристроїв із низьким споживанням енергії — наприклад, датчиків чи розумних пристроїв — у діапазоні 900 МГц. Протокол зберіг такі переваги попередніх версій, як безпечне підключення, сумісність та легкість розгортання.

Wi-Fi HaLow також підтримує діапазони 2,4 та 5 ГГц, завдяки чому він легко інтегрується в існуючі мережі, що налічують сьогодні понад 7 млрд пристроїв. Підключення по IP дає можливість застосовувати цю технологію в системах розумного будинку, сільського господарства, транспорту та інших галузях, а до однієї точки доступу можна під’єднати до 1000 пристроїв.

Рисунок 2.10 – Порівняльна хаоактерисика різних протоколів Wi-Fi за зоною покриття

Таблиця 2.2 – Відмінності у ключових технічних параметрах короткодіючих мереж

Характеристика

Sigfox

LoRa

NB-IoT

Частотний діапазон

868 МГц (Європа), 902 МГц (Північна Америка)

Залежно від регіону: 433 МГц, 868 МГц або 915 МГц

Різні діапазони, включаючи 700 МГц, 800 МГц, 900 МГц, 1800 МГц та 2100 МГц

Швидкість передачі даних

До 100 біт/с

До 27 Кбіт/с

До 250 Кбіт/с

Покриття

Широке покриття, охоплює великі території

Залежить від конфігурації, може мати дуже далеке покриття

Висока проникність, добре працює в затінених областях та всередині будівель

2.3 Різноманітні протоколи, призначені для обміну інформацією

2.3.1 Основні виклики, пов'язані з комунікацією в мережах IoT

Хоча окремі сенсорні вузли генерують обмежені обсяги інформації, основна ідея Інтернету речей полягає в обробці даних від багатьох таких вузлів. Це суттєво відрізняється від типових архітектур, таких як традиційні телефонні мережі або клієнт-серверні системи передачі даних.

Отже, ми стикаємося з новою моделлю архітектури: розподілена мережа, де інформація може створюватися і споживатися багатьма джерелами і одержувачами. Крім того, обсяг передаваного трафіку від сенсорного вузла може значно варіюватися. Традиційні протоколи передачі повідомлень не завжди адаптовані до таких умов.

2.3.2 Основна топологія, яка застосовується для передачі даних в мережі IoT

Подана у рис. 2.11 топологія відповідає концепції "видавець-підписник" (Publisher-Subscriber, або pub/sub), яка використовується для передачі повідомлень в Інтернеті речей. У цій схемі існує два ключових учасника: видавець, який є джерелом інформації, та передплатник, який отримує цю інформацію. Підписка - це операція, за допомогою якої передплатник отримує інформацію від конкретного видавця. Також в цій концепції важливо управляти збором інформації, встановлюючи параметри, такі як періодичність отримання даних та інші показники, залежно від конкретної реалізації.

Рисунок 2.11 – Схема сполучень, що забезпечує обмін даними між вузлами в мережі IoT

У даному контексті розглядається ситуація, коли сенсорний вузол (Node) збирає дані від різних датчиків (наприклад, вологості повітря) та передає їх згідно з параметрами передплати або на запит, або автоматично через певний інтервал часу. Часто

датчики є простими та надсилають дані 7 про контрольовані параметри безперервно. Це призводить до потреби об'єднувати датчики в вузли, які оснащені мікроконтролерами для зчитування даних та їх відправки на сервер за визначеними алгоритмами. Для взаємодії клієнтів з системою також потрібна 5 клієнтська програма (Application), що встановлюється на персональних пристроях для відображення даних з 7 датчиків або вже оброблених на сервері, а також для управління системою.

У такій топології також може бути використаний брокер (Broker), який приймає дані від видавців та передає їх 7 відповідним передплатникам. У складних системах брокер може також виконувати аналітичні операції та обробку 5 даних, що 7 надійшли на сервер. Брокер встановлює 7 пріоритети для з'єднань та формує 7 черги для передачі повідомлень, що 7 дозволяє організовувати пересилання, 7 зберігання та фільтрацію даних.

5 2.3.3 5 DDS

5 DDS (Data Distribution Service) – це протокол на рівні застосунків для машинного зв'язку в системах реального часу. Він ґрунтується 5 на моделі "видавець-передплатник". Основна функція протоколу полягає в забезпеченні 5 з'єднання між 5 пристроями за допомогою шини обміну повідомленнями рис. 5 2.12. 5 Протокол DDS може ефективно та синхронно передавати мільйони повідомлень в секунду.

5 Пристрої вимагають передачі даних з неймовірною швидкістю, вимірюваною в мікросекундах, що відрізняється від стандартних IT мереж. Звичайні TCP потоки не можуть відповідати таким вимогам, оскільки пристрої повинні встановлювати зв'язок шляхом складних маршрутів. DDS, натомість, 15 забезпечує 5 контроль якості обслуговування, багатоадресну передачу, надійність і широкий охоплюючий проміжок передачі. Ще однією перевагою DDS є можливість 5 фільтрації та відбору даних за адресами призначення, а 15 кількість одержувачів може досягати тисяч. DDS також надає спеціальні легковажні версії для компактних пристроїв, що працюють в обмежених умовах. Умови зіркоподібних мереж не підходять 5 для використання даних від пристроїв, тому DDS використовує 15 прямий шинний зв'язок між пристроями на базі 11 реляційної моделі даних, що 15 називається "шиною даних" (DataBus) - 11 мережевий аналог бази даних.

11 Рисунок 11 2.12 – 11 Принцип з’єднання пристроїв за допомогою протоколу DDS в IoT

11 З ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ 4 РОЗВИТКУ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ IOT В УКРАЇНІ

4 3.1 4 Стан 4 технологій передачі даних в Україні, досягнення та перспективи

Українські телекомунікаційні компанії розвивають 4 технології передачі даних для Інтернету речей (IoT). Основними сьогодні є LoRaWAN та NB-IoT. Їх головна відмінність у діапазонах: LoRaWAN працює на неліцензійних частотах, а NB-IoT — на ліцензійних, використовуючи існуючі мережі 4G. Вибір технології залежить від вимог кожного проекту.

Lifecell розвиває IoT-мережу за допомогою LoRaWAN, яка забезпечує покриття до 15 км та високу енергоефективність завдяки використанню діапазону 868 МГц. Вже розгорнуто понад 80 базових станцій у Києві, Львові та Кропивницькому — покрито до 90% міської території. Рішення застосовують у розумних містах, логістиці, сільському господарстві та інших галузях.

Більше 10 бізнес-компаній вже підключилися до IoT-послуг, використовуючи ці технології для обліку ресурсів, моніторингу та дистанційного управління.

У лютому 2019 року Vodafone завершив тестування NB-IoT у великих містах України. Ця технологія забезпечує стабільний зв’язок навіть у складних умовах (шахти ліфтів, підвали) та високу безпеку завдяки SIM-аутентифікації й шифруванню данних. NB-IoT дає можливість пристрою працювати до 10 років від однієї батареї та масштабувати мережу за потреби.

3.2 Майбутність технологій передачі даних в Україні

Технологія 5G сьогодні є найбільш перспективною та впливовою для розгортання IoT в Україні та у світі. Її головна перевага — висока швидкість передачі данних: до 10 Гбіт/с, що в десятки разів швидше за 4G. Це дає можливість покращити зв’язок у багатьох галузях та забезпечити нові сервіси.

5G характеризується також дуже малою затримкою — до 1 мілісекунди — завдяки чому забезпечується практично миттєва реакція та можливість розвивати інтерактивні застосунки в реальному часі.

Серед головних характеристик 5G: пікова швидкість завантаження до 20 Гб/с, швидкість завантаження до 100 Мб/с та вивантаження до 50 Мб/с для кожного користувача, можливість руху зі швидкістю до 500 км/г, швидке перемикання між режимами заощадження та активності, покращена ефективність використання радіочастот та підтримка до 1 мільйону пристроїв на кожний км^2.

Впровадження 5G дасть потужний імпульс для розумних міст, медицини, транспорту, розваг та інших галузей.

3.2.1 Медична галузь

Після впровадження технології 5G можливим стане проведення віддалених хірургічних операцій, де хірург може керувати роботизованим обладнанням на великій відстані від пацієнта. Це відкриє нові можливості для проведення складних медичних процедур у віддалених районах або навіть під час екстрених ситуацій. Крім того, завдяки використанню технології 5G, хірург може отримувати реальний час відображення візуальних та тактильних даних під час операції, що підвищить точність та безпеку процедури.

Володіючи спеціальним обладнанням, лікар зможете керувати необхідними інструментами та бути онлайн під час операцій. Завдяки технології 5G ви також зможете оперативно реагувати на погіршення стану здоров'я через спеціальні датчики або звичайні смарт-годинники. Наприклад, це допоможе у вирішенні таких проблем, як захист від падінь, який вже випробувала компанія Apple у моделі Apple Watch 4, проте без підтримки 5G ця функція ще не готова до реального використання.

Додатково, завдяки високим швидкостям 5G стане можливим швидке декодування ДНК. Навіть зараз ця процедура виконується, але вона потребує великих обсягів даних: інформація про геном однієї людини може займати до 140 гігабайт, і відправлення цих даних може зайняти лише одну-дві хвилини.

У випадку аварії або серцевого нападу ваш лікар швидко отримає інформацію та відправить карету швидкої допомоги, завдяки датчикам, розташованим у вашому пристрої. Це дозволить медичному персоналу точно визначити ваше місце знаходження та швидко надати допомогу.

3.2.2 Безпілотні авто та квадрокоптери

У майбутньому технологія 5G може значно знизити ймовірність ДТП та сприяти розвитку безпілотних автомобілів. 19 Завдяки швидкому та надійному зв'язку 5G, автомобілі зможуть швидше та точніше реагувати на зміни дорожньої ситуації, уникати транспортних пригод та обходити переповнені дороги. Це може призвести до зменшення заторів та покращення загальної безпеки на дорогах.

Безпілотні автомобілі в майбутньому будуть інтегруватися з камерами, світлофорами та іншими дорожніми системами для миттєвого отримання та аналізу інформації про стан доріг та дорожніх умов. Вони зможуть автоматично реагувати на зміни погоди та інші фактори, що впливають на 19 безпеку на дорозі.

19 Рисунок 3.3 – Принцип роботи безпілотних транспортних засобів

Максимальна дальність польоту квадрокоптерів збільшиться, і буде обмежуватися виключно потужністю акумулятора. Управління дронами буде можливе в режимі

реального часу з віддалених місць. Дрони будуть активно обмінюватися інформацією між собою, що сприятиме автоматизації їх масового використання без прямого втручання людини.

Рисунок 3.4 Квадрокоптери в розумних містах

У майбутньому квадрокоптери можна буде використовувати для пошуку людей, які заблукали в важкодоступних місцях. У разі потреби вони зможуть оперативно доставити необхідні медикаменти та речі, доки рятувальники дістануться до потерпілих.

Посилання

Це джерела виділених збігів у вашому документі. Кожен збіг позначено темно-зеленим числом, яке відповідає вказаному тут джерелу. Джерела впорядковані за схожістю — чим вищий бал, тим сильніше збіг.

#	Джерело	%
1	ela.kpi.ua	3.5%
2	duikt.edu.ua	1.9%
3	ela.kpi.ua	1.3%
4	ela.kpi.ua	1.0%
5	ela.kpi.ua	0.9%
6	duikt.edu.ua	0.9%
7	elartu.tntu.edu.ua	0.8%
8	stu.cn.ua	0.4%
9	ir.duan.edu.ua	0.3%
10	ela.kpi.ua	0.3%
11	surl.lu	0.3%
12	openarchive.nure.ua	0.3%
13	onmu.odessa.ua	0.3%
14	e-tk.lntu.edu.ua	0.2%
15	metod.vntu.edu.ua	0.2%
16	metod.vntu.edu.ua	0.2%
17	er.nau.edu.ua	0.2%
18	dspace.nuph.edu.ua	0.2%
19	e-drive.tech	0.2%
20	surl.li	0.2%
21	openarchive.nure.ua	0.1%
22	e-reading.club	0.1%
23	econa.org.ua	0.1%

#	Джерело	%
24	e-tk.lntu.edu.ua	0.1%
25	visn-it.uu.edu.ua	0.1%
26	mediacom.com.ua	0.1%

Plag

Дякуємо, що перевірили
свій документ за допомогою
Plag!