ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення автоматизованих систем

Пояснювальна записка

до кваліфікаційної
роботи на ступінь вищої
освіти магістр

на тему: «**РОЗРОБКА МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ДАТЧИКІВ ТА СЕНСОРІВ В ІНТЕЛЕКТУАЛЬНІЙ МЕРЕЖІ МІСТА»**

Виконав: студент 6 курсу,

групи ІСДМ–61 спеціальності 126

Інформаційні системи та технології

(шифр і назва спеціальності)

Воїнов Ю.Ю.

(прізвище та ініціали)

Керівник Бондарчук А.П.

(прізвище та ініціали)

Рецензент_____

(прізвище та ініціали)

Київ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти - «Магістр»

Спеціальність - 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ

Завідувач кафедри Інженерії

програмного
забезпечення
автоматизованих систем

_____К.П. Сторчак_____

«____» _____2021 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Воїнов Юрій Юрійович

(прізвище, ім‘я, по батькові)

1.Тема роботи: «Розробка моделі інформаційної системи ідентифікації датчиків та сенсорів в інтелектуальній мережі міста»

Керівник роботи Бондарчук Андрій Петрович, професор, доктор технічних наук,

(прізвище, ім‘я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від 11.10.2021 року №170.

2. Строк подання студентом роботи 26 грудня 2021року

3. Вхідні дані до роботи:

1. Науково-технічна література;
2. Методології ідентифікації об’єктів;
3. Архітектури інтелектуальних мереж;

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно вирішити):
   1. Аналіз технологій побудови інтелектуальних інформаційних мереж;
   2. Дослідження методів ідентифікації об’єктів;
   3. Розробка моделі інформаційної системи ідентифікації об’єктів мережі.

5. Перелік графічного матеріалу
   1. Аналіз проблеми;
   2. Технологія 5G;
   3. Технологія LoRaWAN;
   4. Порівняння 5G і LoRaWAN мереж;
   5. Технології ідентифікації;
   6. Системи управління ідентифікацією;

6. Дата видачі завдання 12.10.2021

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу		
3	Написання другого розділу		
4	Написання третього розділу		
5	Вступ, висновки, реферат		
6	Розробка обов‘язкових демонстраційних матеріалів		
7	Попередній захист роботи		

Студент _____ (підпис) Воїнов Ю.Ю. (прізвище та ініціали)

Керівник роботи _____ (підпис) Бондарчук А.П. (прізвище та ініціали)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Воїнов Ю.Ю. (прізвище та ініціали) до захисту магістерської роботи

за спеціальністю 126 Інформаційні системи та технології (шифр і назва спеціальності)

на тему: Розробка моделі інформаційної системи ідентифікації датчиків та сенсорів в інтелектуальній мережі міста

Магістерська робота і рецензія додаються.

Директор інституту _____ (підпис) Бондарчук А.П. (прізвище та ініціали)

Довідка про успішність

Воїнов Ю.Ю. (прізвище та ініціали) за період навчання в Навчально-науковому інституті інформаційних технологій

з 2020 року до 2021 року повністю виконав навчальний план за спеціальністю, з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Методист інституту _____ (підпис) Алексіна Л.Т. (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент Воїнов Ю.Ю. показав гарну теоретичну та практичну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність та сумлінність до наукової роботи.

Все це дозволяє оцінити магістерську роботу студента Воїнова Юрія на оцінку "відмінно", та присвоїти йому кваліфікацію «магістр з інформаційних систем та технологій».

Керівник роботи _____ (підпис) Бондарчук А.П. (прізвище та ініціали)

" " _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерську роботу розглянуто. Студент Воїнов Ю.Ю. (прізвище та ініціали)

допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри
ІПЗАС _____ (підпис) Сторчак К.П. (прізвище та ініціали)

" " _____ 2021 року

ВІДГУК РЕЦЕНЗЕНТА
по магістерській роботі

студента *Воїнова Юрія Юрійовича*
на тему: **“Розробка моделі інформаційної системи ідентифікації датчиків та сенсорів в інтелектуальній мережі міста”.**

Актуальність:

Магістерська робота студента Воїнова Юрія Юрійовича присвячена дослідженню та реалізації інформаційних систем, що використовуються для ідентифікації об'єктів інтелектуальної мережі.

Основне завдання полягає в створенні моделі системи, яка допоможе з вирішенням проблеми ідентифікації об'єктів інтелектуальної мережі міста, а саме датчиків та сенсорів, тому тема дипломної роботи є актуальною.

Позитивні сторони:

1. Зміст магістерської роботи відповідає завданню. Робота, яку виконав *Воїнов Юрій Юрійович*, показала позитивний рівень знань і ступінь підготовленості студента до майбутньої роботи з фаху.

2. Поставлені в магістерській роботі задачі з дослідженням і розробки інформаційної системи ідентифікації виконані в повному обсязі.

3. Технічні питання викладені успішно і якісно.

4. Текст викладений кваліфіковано та ясно. Помірний обсяг використання науково-технічної літератури.

Недоліки

1. В роботі необхідно було б розглянути професійні рішення і також самі об’єкти, а саме датчики та сенсори.

2. Не повністю проаналізовані питання ідентифікації об'єктів.

Висновок: Незважаючи на недоліки магістерської роботи заслуговує оцінку *добре,* а студент Воїнов Юрій Юрійович – присвоєння кваліфікації магістр з інформаційних систем та технологій.

Якість магістерської роботи	
виконано на замовлення підприємства	
виконано за тематикою НДР	
виконано з макетом	
виконано з застосуванням ЕОМ та МПТ	
має практичну цінність	*
проект частина комплексної теми	

Підпис рецензента

(_____)

РЕФЕРАТ

Текстова частина магістерської роботи : 84 с., 3 табл., 16 рис., 1 дод., 26 джерела.

IDENTIFICATION, SENSOR, INFORMATION SYSTEM, INTELLECTUAL NETWORK, LORAWAN, 5G, NB-IOT, IOT, SMART CITY, ESIM, BLOCKCHAIN.

Об’єкт дослідження. Технології інтелектуальної мережі міста.

Предмет дослідження. Ідентифікація об`єктів інтелектуальної мережі міста.

Ціль роботи. Модель інформаційної системи ідентифікації датчиків і сенсорів у інтелектуальній мережі міста.

Методи дослідження. Для виконання завдань дослідження було використано наступні методи:

– Пошук наукових робіт та інших джерел, що мають відношення до об`єкту дослідження в Інтернеті для аналізу та оцінки. ;

– Порівняння різних технологій для визначення найефективніших та найоптимальніших варіантів реалізації;

– Підведення підсумків щодо результатів дослідження;

– Створення власної моделі інформаційної системи інтелектуальної мережі міста.

Результати та їх новизна. Досліджена ідентифікація об’єктів(датчиків та сенсорів) інформаційної системи у інтелектуальній мережі міста. Розроблені класифікація систем управління ідентифікацією та архітектура інформаційної системи мережі розумного міста.

Значимість роботи. Результати роботи можливо використовувати для досліджень інформаційних систем мереж розумних міст та побудови таких систем.

Висновки, пропозиції щодо розвитку об‘єкта дослідження (розроблення) й доцільності продовження досліджень.

ЗМІСТ

ВСТУП

Актуальність теми: Тенденція переселення людей у міста набирає обороти, як і підвищується цими людьми стандартів комфортного проживання. Відповіддю на цей попит створюються розумні міста, що використовуючи новітні технології, забезпечують надання послуг населенню. Але після створення та впровадження необхідно забезпечувати безперервну роботу і при таких великих масштабах, що надалі будуть тільки збільшуватися, необхідність у ефективній ідентифікації об’єктів мережі є досить очевидною.

Мета і завдання дослідження. Модель інформаційної системи ідентифікації датчиків і сенсорів у інтелектуальній мережі міста. Для досягнення цієї мети необхідно виконати наступні завдання:

1) Проаналізувати існуючі технології для побудови інформаційних систем для інтелектуальних мереж міст та дослідити тенденції розумних міст.

2) Дослідити загальні стандарти ідентифікації об’єктів.

3) Дослідити методи ідентифікації та розпізнання об’єктів, а саме математичні моделі, алгоритми та технології, що сприяють вирішенню завданню ідентифікації.

4) Розробити вимоги для моделі ідентифікації, а також класифікувати різновиди систем управління ідентифікацію.

5) Розробити архітектуру інформаційної системи розумного міста.

Об’єкт дослідження. Технології інтелектуальної мережі міста.

Предмет дослідження. Ідентифікація об`єктів інтелектуальної мережі міста.

Методи дослідження. Для виконання завдань дослідження було використано наступні методи:

– Пошук наукових робіт та інших джерел, що мають відношення до об`єкту дослідження в Інтернеті для аналізу та оцінки. ;

– Порівняння різних технологій для визначення найефективніших та найоптимальніших варіантів реалізації;

– Підведення підсумків щодо результатів дослідження;

– Створення власної моделі інформаційної системи інтелектуальної мережі міста.

Наукова новизна одержаних результатів.

Досліджена ідентифікація об’єктів(датчиків та сенсорів) інформаційної системи у інтелектуальній мережі міста. Розроблені класифікація систем управління ідентифікацією та архітектура інформаційної системи мережі розумного міста.

Практичне значення одержаних результатів. Результати роботи можливо використовувати для досліджень інформаційних систем мереж розумних міст та побудови таких систем.

Публікації.

1. Воїнов Ю.Ю. КОНЦЕПЦІЯ SMART CITY.

XIII Міжнародна науково-технічна конференція студентства та молоді «СВІТ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЙ». Збірник тез. – К.: ДУТ, 2021, с. 142-143.

2. Опубліковано статтю «ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ АВТОНОМНИХ ТРАНСПОРТНИХ ЗАСОБІВ ДЛЯ ВИКОРИСТАННЯ В МЕРЕЖАХ SMART CITY » у фаховому виданні «ЗВ’ЯЗОК» № 4 (2021) (готується до друку)

1 АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ МЕРЕЖ

1.1 Концепція – IoT

IoT (Інтернет речей або Internet of Things) - це мережа фізичних об'єктів, які називають «речами», в них вбудовано програмне забезпечення, електроніка, загальна мережа і власні датчики, що дозволяє цим об'єктам збирати дані і обмінюватися ними.

Призначення Інтернету речей полягає в тому, щоб мережа пристроїв самостійно звітувала в режимі реального часу, підвищуючи ефективність їх використання, передавала і повідомляла важливу інформацію швидше, ніж система, що залежить від втручання людини.

За допомогою IoT можливо зробити практично все «розумним», поліпшивши аспекти нашого життя за допомогою збору даних і алгоритму штучного інтелекту. Також можливе використання «речей» в IoT, наприклад, у вигляді імплантату для моніторингу діабету у людини або, як пристрій стеження за твариною.

Середовище IoT складається із інтелектуальних пристроїв з підтримкою Інтернету, які використовують вбудовані системи, такі як процесор, датчики та інше апаратне забезпечення, для збору, передачі і реагування на отримані дані, які вони отримують з свого довкілля. Пристрій Інтернету речей обмінюється даними датчиків за допомогою шлюзу IoT чи іншого крайового центру, де дані і передаються в хмару для аналізу або локального аналізу. Ці пристрої спілкуються з іншими спорідненими пристроями і діють на основі інформації отриманої від них. Загалом робота виконується без втручання людини, але при потребі людське втручання можливе – наприклад, для налаштування приладів, отримання даних від них або передача їм інструкцій.

Рішення IoT широко використовуються в багатьох компаніях в різних галузях(див. рис. 1.1).

Рисунок 1.1 - Галузі застосування технології IoT

Система IoT[1-2] складається із чотирьох основних компонентів, а саме:

1) Датчики і пристрої: Для того щоб зібрати інформацію про те, що відбувається навколо вас на даний момент, датчики і пристрої є ключовим компонентом, який допомагає вам отримувати дані в реальному часі з навколишнього середовища. Ці дані можуть бути різного ступеня складності. Найчастіше в IoT використовуються такі типи датчиків:

- температурний сенсор.
- датчик тиску.
- датчик наближення.
- акселерометр і датчик гіроскопа.
- ir-датчик.
- оптичний датчик.
- датчик газу.
- датчик диму.

Пристрій може мати датчики різних типів, крім зчитування виконують кілька завдань.

2) Зв'язок: всі зібрані дані відправляються в хмарну інфраструктуру. Датчики повинні бути підключені до хмари за допомогою різних засобів зв'язку. Ці засоби зв'язку включають мобільні або супутникові мережі, Bluetooth, WI-FI, WAN і т. д.

3) Обробка даних: за допомогою програмного забезпечення обробка даних відбувається після того, як дані зібрані і надходять в хмару. Можливо це просто перевірка температури, шляхом зчитування показань з пристроїв таких, як кондиціонер або обігрівач. Однак в деяких випадках обробка даних може бути дуже складною, наприклад при ідентифікації об'єктів за допомогою комп'ютерного зору на відео.

4) Інтерфейс: інформація повинна бути доступна кінцевому користувачеві будь-яким чином, що може бути досягнуто шляхом активації сигналів тривоги на їх телефонах або посилання їм повідомлення через електронну пошту або текстовим повідомленням. Іноді користувачеві може знадобитися інтерфейс, який активно перевіряє його систему IoT. Наприклад, у користувача вдома встановлена камера. Він хоче отримати доступ до відеозапису і всіх каналах за допомогою веб-сервера.

Однак це не завжди одностороннє спілкування. В залежності від програми IoT і складності системи користувач також може виконувати дію, яке може створювати каскадні ефекти. Наприклад, якщо користувач виявляє будь-які зміни температури в холодильнику, за допомогою технології IoT користувач може регулювати температуру за допомогою свого мобільного телефону.

Нижче (у таблиці 1.1) наведено деякі найбільш поширені програми застосування Інтернету речей:

Таблиця 1.1 - Програми застосування Інтернету речей

Назва	Опис
Датчики паркування	IoT-технологія допомагає користувачам в реальному часі визначати наявність паркувальних місць на своєму телефоні.
Підключені автомобілі	IoT технологія допомагає автомобільним компаніям автоматично обробляти рахунки, паркування, страхування та інші пов'язані з цим питання.
Інтелектуальний ланцюжок постачання	Допомагає відстежувати товари в режимі реального часу, поки вони знаходяться в дорозі, або змушує постачальників обмінюватися інформацією про запаси.
Smart city (Розумне місто)	Пропонує всі типи сценаріїв використання, від управління дорожнім рухом до розподілу води, видалення відходів і т. д.
Smart home (Розумний будинок)	Інкапсулює можливості підключення всередині вашого будинку. Сюди входять детектори диму, побутова техніка, лампочки, вікна, дверні замки тощо.
Розумні розетки	IoT технологія, що дозволяє віддалено включати й вимикати будь-який пристрій. Також дозволяє відстежувати рівень заряду пристрою та отримувати настроюються повідомлення прямо на свій смартфон.

Продовження таблиці 1.1- Програми застосування Інтернету речей

Назва	Опис
Інтелектуальні термостати	IoT технологія, що допомагає вам заощадити ресурси на рахунках за опалення, знаючи особливості вашого використання.
Connect Health	Концепція підключеної системи охорони здоров'я полегшує моніторинг стану здоров'я та догляд за пацієнтами в режимі реального часу. Це допомагає поліпшити прийняття медичних рішень на основі даних пацієнтів.
Трекери активності	IoT технологія, що допомагають фіксувати пульс, витрату калорій, рівень активності та температуру шкіри на зап'ясті.

Головні переваги технології IoT:

– технічна оптимізація: У цьому плані технологія IoT є дуже корисною для вдосконалення технологій і їх поліпшення. За допомогою IoT виробник може збирати інформацію з різних датчиків. Виробник аналізує їх, щоб удосконалити дизайн і зробити їх більш ефективними;

– новий вдосконалений збір даних: Традиційне збирання даних застаріло і є доволі обмежене. Тепер завдяки IoT можна швидко та ефективно обробляти дані;

– скорочення відходів: IoT надає інформацію в режимі реального часу, забезпечує ефективну роботу та управління ресурсами;

– покращене залучення клієнтів: IoT допомагає поліпшити взаємодію з клієнтами, проявляючи проблемні місця і покращуючи процес.

Недоліки технології IoT:

– безпека: Технологія IoT створює екосистему підключених пристроїв. Однак під час цього процесу система може запропонувати невеликий контроль автентифікації, не зважаючи на достатні заходи безпеки;

– конфіденційність: Використання IoT відкриває значну кількість персональних даних, вкрай детально, без активної участі користувача. Це створює багато проблем конфіденційності;

– гнучкість: Існує величезне занепокоєння щодо гнучкості системи Інтернету речей. В основному це стосується інтеграції з іншою системою, оскільки в цьому процесі залучено багато різноманітних систем;

– складність: Дизайн системи IoT також досить складний. Крім того, розгортання та обслуговування також не дуже прості;

– відповідність: IoT має власний набір правил та норм. Однак через його складність завдання дотримання вимог є досить складним.

Серед безпровідних технологій основний інтерес представляє стандарт IEEE 802.15.4, що визначає фізичний шар і управління доступом для організації енергоефективних персональних мереж, і є основою для таких протоколів, як ZigBee, WirelessHart, MiWi, 6LoWPAN, LPWAN.

Серед провідних технологій важливу роль в використанні IoT грає рішення PLC - технології побудови мереж передачі даних по лініях електропередачі, так як у багатьох додатках присутній доступ до електромереж (наприклад, торгові автомати, банкомати, інтелектуальні лічильники, контролери освітлення спочатку підключені до мережі електропостачання). 6LoWPAN, який реалізує шар IPv6 як над IEEE 802.15.4, так і над PLC, будучи відкритим протоколом, стандартизованого IETF, відзначається як особливо важливий для розвитку IoT.

1.2 Глобальні мережі 5 покоління (5G)

5G (five generation) - п'яте покоління зв'язку діюче на основі стандартів зв'язку нового покоління (IMT-2020), що йде за існуючими стандартами (IMT-Advanced). Після запуску перших 5G мереж в 2008 році, активна розробка 5G почалася тільки з кінця 2018 року - в Південній Кореї, а потім і в США. На даний момент нова технологія доступна в 37 країнах світу. Лідером по впровадженню 5G, крім згаданих Південної Кореї і США, є Китай.

Активна розробка 5G почалася в 2008 році, але запуск першої 5G-мережі відбувся в кінці 2018-го - початку 2019 року в Південній Кореї, а згодом - і в США. Нова технологія доступна в 37 країнах світу, але загальнонаціональної мережі немає ні в одній з них. Лідерами по впровадженню 5G, крім згаданих Південної Кореї і США, також є Китай.

Принцип роботи мереж п'ятого покоління полягає в тому, що дані локальної антени будь-якого приладу передаються станції. При цьому вони створюють глобальну мережу, яка з'єднується по радіохвильовим лініям певного частотного діапазону.

Інформації та пристроїв стає так багато, що нинішня еволюція до 5G виглядає логічною. Тим самим збільшується необхідність в частотах, що призводить до того, що з кожним новим поколінням діапазон радіохвиль, що використовуються зростає. Чим більше частот - тим більше можливостей доставити сигнал, а отже, тим більше покриття мережі. Чим вище частота хвилі - тим більше можна їм передати за той же проміжок часу.

Досі використовуються хвилі низької частоти, які дозволяють передавати інформацію через стіни, але програють у швидкості зв'язку.

Хвилі високої частоти можуть передавати більше інформації, але мають невеликий діапазон дії. Інша назва для високих частот – міліметрові хвилі, тому що їхня довжина становить 1-10 міліметрів. Ці хвилі швидше загасають в атмосфері та передають сигнал далі на відстань близько кілометра. Тому для використання високих частот 5G необхідно багато

передавачів і практично скрізь, інакше зв'язок буде переривatись. Саме тому одна із основних сфер застосування IoT, або всесвітня мережа взаємопов'язаних фізичних пристроїв.

Технологія мобільного зв'язку 5G має наступні характеристики:

- підвищення пікової швидкості до 20 Гбіт/с по лінії вниз (тобто від базової станції до мобільного); і до 10 Гбіт/с у зворотному напрямку;
- зростання практичної швидкості на абонента до 100 Мбіт/с і більше;
- збільшення спектральної ефективності в мережах 5G в 2-5 разів. На лінії вниз: 30 біт/с/Гц, на лінії вгору - 15 біт/с/Гц;
- підвищення енергоефективності на 2 порядки. Тепер пристрої "Інтернету речей" зможуть працювати без підзарядки акумулятора до 10 років;
- скорочення тривалості затримки на радіо інтерфейсу до 0,5 мс (для сервісів наднадійного міжмашиного зв'язку URLLC) і до 4 мс (для сервісів надширокосмугового мобільного зв'язку eMBB) ;
- збільшення швидкості пересування абонента до 500 км/ч;
- збільшення загального числа підключених пристроїв до 1 млн./Км2.

Порівняння показників поколінь технологій (див. рис. 1.2 – 1.3)[3]:

4G, поточний стандарт, пропонує швидкості від 7 до 17 Мбіт / с для завантаження і від 12 до 36 для завантаження. Навпаки, швидкість передачі 5G може досягати 15 або 20 Гбіт / с.

Мережі 5G забезпечують затримку 1-10 мілісекунд проти 50 мс, доставлену 4G.

Якщо швидкість 4G досягає в середньому 10 Мб / с, а максимум - до 1 Гб / с, то 5G має середню швидкість від 50 Мб / с, а максимальна - в межах 1-10 Гб / с, і це не межа.

Таким чином, 5G зніме всі поточні обмеження на пропускну здатність, принаймні, до того часу, як використання не буде збільшуватися, аби не відставати від нього.

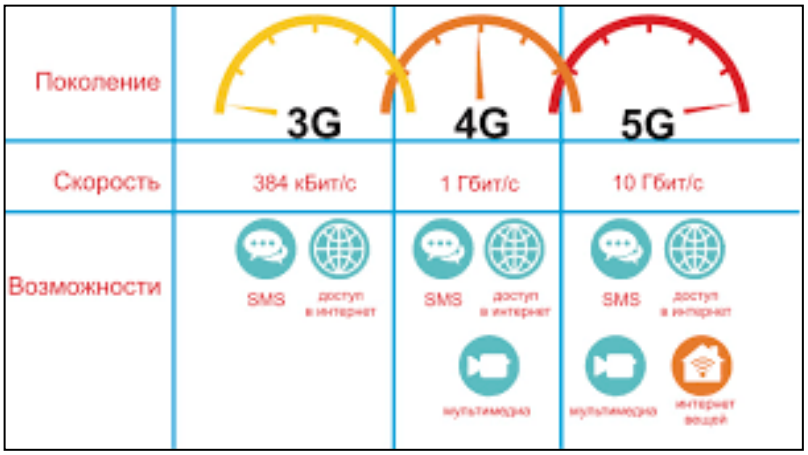


Рисунок 1.2 – Порівняння технологій 3G, 4G, 5G

		3G	4G	5G
	Deployment	2004-05	2006-10	2020
	Bandwidth	2mbps	200mbps	>1gbps
	Latency	100-500 milliseconds	20-30 milliseconds	<10 milliseconds
	Average Speed	144 kbps	25 mbps	200-400 mbps

Рисунок 1.3 – Порівняння технологій 3G, 4G, 5G

Серед важливих особливостей 5G можна навести:

1) Розбиття мережі. Ця особливість 5G полягає у можливості створювати віртуальні мережі. Підмережі, що мають різні пріоритети трафіку створюються забезпечуючи можливість, наприклад, у лікарні мати мережу, що спроектована таким чином, щоб з'єднання між хірургами та роботом було пріоритетнішим, наприклад, комунікаціям, які використовуються пацієнтами. У цьому випадку аварійні передачі можна захистити, навіть якщо мережа досягає максимальної ємності.

2) Також важливою особливістю 5G є спосіб використання частотного спектру. Щоб забезпечити надвисокі швидкості з найменшими затримками, мережі 5G використовують радіочастоти у двох групах:

– FR1, також званий діапазоном суб-6 ГГц,

– FR2 між 24 і 52 ГГц.

Останній, FR2, поширюється на надзвичайно високочастотний діапазон (КВЧ). Який визначається як смуга спектру між 30 ГГц і 300 ГГц.

Відповідно до частоти створено декілька специфікацій 5G, що користуються різними хвилями з відповідними частотами:

– низькі (до 2ГГц);

– середні (2 - 10 ГГц);

– високі (понад 10 ГГц).

Залежно від умов, використовується відповідна «версія» 5G[4], а під потреби з цих умови виділяються специфікації технології 5G:

1) URLLC (Ультранадійна комунікація з низькою затримкою або критично важлива 5G мережа) - це новий клас комунікаційних характеристик, який фокусується на максимально можливій надійності, забезпечуючи затримку за 1 мс. 5G додає системні доповнення, які забезпечують нові рівні низької затримки та надвисокої надійності. Цей варіант ідеально підходить для таких програм, як служби швидкої допомоги, служби екстреної допомоги та автономні транспортні засоби, включаючи безпілотники та промисловий Інтернет речей, а також робототехніку.

2) eMBB (розширений мобільний широкосмуговий зв'язок або високошвидкісна мережа 5G) - це переважно висока пропускна здатність даних, що забезпечує новий, ширший пропускний спроможності спектр 5G. Він забезпечує надзвичайно високу швидкість, високу ємність системи та кращу спектральну ефективність для застосувань у споживчому просторі, таких як розширені смартфони та віртуальна реальність, промислові

маршрутизатори та шлюзи, що вимагають найкращого у своєму класі з'єднання.

3) mMTC (Масивна комунікація типу машин або енергоефективна 5G) - використовує існуючу LTE LPWAN. Його основна увага зосереджена на ефективній передачі з перебоями низьких обсягів даних на пристрої та з них, які потребують широкого охоплення території та тривалого часу автономної роботи. З більшою ефективністю збільшується ємність мережі для обслуговування величезної кількості пристроїв. Цей варіант ідеально підходить для таких додатків, як розумні лічильники та програми відстеження та відстеження, які залежать не від швидкості та затримки, а від оптимальної енергоефективності.

Технології NB-IoT та LTE-M є частиною категорії mMTC 5G:

– NB-IoT (вузькосмуговий IoT) - це швидкозростаючий стандарт стільникової технології 3GPP, запроваджений у Випуску 13, який відповідає вимогам LPWAN (мережі з низькою потужністю широкосмугової мережі) IoT. Вона була стандартизована та класифікована як технологія 5G компанією 3GPP у 2016 році, і вона буде продовжувати розвиватися відповідно до специфікації 5G. Це провідна технологія LPWAN, що забезпечує живлення широкого спектра промислових пристроїв Інтернету речей, включаючи розумне паркування, комунальні послуги, носії та промислові рішення.

– LTE-M - це технологія LPWAN, прийнята 5G. І як NB-IoT, вона належить до категорії mMTC 5G. 3GPP погодилося, що технології NB-IoT та LTE-M будуть продовжувати розвиватися, як частина специфікацій 5G, а це означає, що ці технології можна використовувати сьогодні і продовжувати впродовж десятиліття чи більше, як частина еволюції 5G. NB-IoT та LTE-M будуть співіснувати з іншими стандартами 5G, і вони стануть LPWAN спектру 5G.

5G - глобальна технологія, яка послідовно впроваджується з використанням міжнародних стандартів 3GPP (3rd Generation Partnership

Project). Грунтуючись на підтримку 4G для IoT, версії 15 і 16 специфікацій 3GPP забезпечать додаткову підтримку пристроїв IoT з функціями 5G, включаючи наднадійність і низьку затримку.

Подальші удосконалення 5G, такі як сегментування мережі, непублічні мережі і ядро 5G, в кінцевому підсумку покликані допомогти реалізувати бачення глобальної мережі IoT, що підтримує величезну кількість підключених пристроїв з різними вимогами до мобільності та доступності.

5G надає ряд переваг, недоступних для інших технологій. До них відноситься гнучкість 5G для підтримки величезної кількості статичних і мобільних пристроїв IoT, які мають широкий діапазон вимог до швидкості, пропускної спроможності і якості обслуговування. Окрім можливості обслуговувати дуже широкий спектр пристроїв і їх різноманітні вимоги до обслуговування, мережі 5G також можуть безпечно обробляти величезні обсяги даних, що генеруються пристроями IoT.

У міру розвитку Інтернету речей гнучкість 5G стане ще більш важливою для підприємств[5]. 5G буде підтримувати критично важливий зв'язок з ще більш строгими вимогами до продуктивності. Наднадійність і низька затримка 5G можуть допомогти втілити в життя безпілотні автомобілі, інтелектуальні енергосистеми, поліпшену автоматизацію виробництва та інші передові програми. Збільшення кількості підключених пристроїв дозволяє створювати рішення для розумного міста і будівництва.

У містах 5G дозволить поліпшити управління дорожнім рухом, підтримуючи величезну кількість підключень Інтернету речей до світлофорів, камерам і датчикам руху. Інтелектуальні лічильники, підтримувані недорогими датчиками IoT і підключеннями 5G, будуть відслідковувати споживання енергії та сприяти скороченню споживання. Хмарні обчислення, штучний інтелект і периферійні обчислення також допоможуть обробляти обсяги даних, які генеруються IoT.

Уявіть, як розумне місто з тисячами камер може направляти людей навколо дорожньо-транспортних пригод або вказувати людям, де є місця для

паркування. Мережа 5G з IoT дозволяє автомобілям спілкуватися один з одним і з навколишнім середовищем, знижуючи ризик аварій і забезпечуючи більш ефективні схеми руху. Поєднання всього цього скоротить затори на дорогах, скоротить час у дорозі і заощадить електроенергію за рахунок скорочення часу простою транспортних засобів на червоне світло або очікування в черзі. Інтеграція AI покращить контроль трафіку.

Збільшення кількості підключених пристроїв дозволить розмістити набагато більше датчиків в розумних містах і будівлях. В даний час датчики розумного міста, як правило, щодо обмежені. Вони ставляться на ліхтарні стовпи і дуже грубо покривають територію. Добре це чи погано, але 5G дозволяє насичувати область невеликими датчиками. Це дозволяє використовувати в діапазоні від виявлення руху пішоходів до включення освітлення - з існуючими системами можуть виникнути проблеми, коли світло не може виявити нерухомої людини і відключається.

Автомобілі також можуть записувати стан свого масла або гальм, повідомляючи про це власника і безпосередньо підключаючи їх до обраного ним ремонтному центру. Не тільки це, але і безпілотні автомобілі можуть записувати і передавати дані своїм виробникам, які потім можуть використовуватися для поліпшення як програмного забезпечення, так і майбутніх проектів.

В цілому мережі 5G використовують більш широку смугу частот, ніж їх попередники, допомагаючи досягти кращих в галузі швидкостей, надійності та ефективності, дозволяючи додавати системи наступних поколінь. Багаті і важкі пакети даних передаються з блискавичною швидкістю з непомітною затримкою в мережі.

1.3 LoRaWAN

LoRaWAN - це протокол глобальної мережі з низьким енергоспоживанням побудований на основі технології радіомодуляції LoRa.

LoRa (Long Range) - це метод модуляції, який забезпечує значно більшу дальність зв'язку (зону покриття), ніж інші конкуруючі з ним способи[7]. Метод ґрунтується на технології модуляції з розширеним спектром і варіації лінійної частотної модуляції (Chirp Spread Spectrum, CSS) з інтегрованою прямий корекцією помилок (Forward Error Correction, FEC). Термін LoRa також може відноситися до систем, які підтримують цей метод модуляції, або до мережі зв'язку, яку використовують програми IoT.

Головною перевагою LoRa є його дальність і доступність. Типовий варіант використання LoRa - це розумні міста, в яких малопотужні і дешеві пристрої Інтернету речей (зазвичай датчик або монітор), розкидані по великій території, періодично посилають невеликі пакети даних центральному адміністратору.

Через бездротову мережу LoRaWAN підключається до Інтернету і управляє зв'язком між кінцевими пристроєм і мережевими шлюзами. Тенденція використання LoRaWAN в промислових приміщеннях і розумних містах зростає через те що це дешевий і доступний протокол двостороннього зв'язку на велику відстань з дуже низьким енергоспоживанням - пристрої можуть працювати до десяти років із маленької батареї. Ним використовується не ліцензовані радіодіапазони ISM (промислові, наукові, медичні) для розгортання мережі.

Підключення пристрою до LoRaWAN загалом можливо здійснити цими двома способами:

– активація по бездротовій мережі (OTAA): пристрою необхідно встановити мережевий ключ і ключ сеансу додатка для підключення до мережі;

– активація шляхом персоналізації (ABP): пристрій жорстко запрограмований ключами, необхідними для зв'язку з мережею, що знижує безпечність з’єднання але натомість спрощує його.

При цьому специфікацією LoRaWAN передбачений широкосмуговий мережевий протокол малої величини (LPWA), призначений виключно для

бездротового підключення «речей» і орієнтований на основні вимоги до Інтернету, які пред'являються до нього, такі як безпека, мобільність і надання послуг[6].

LoRaWAN є мережевою архітектурою, яка будується в топології «зірка - зірка» (див. рис. 1.4), в якій шлюзи транслюють сполучення між кінцевими пристроями та центральний сервер[8]. За стандартними протоколами шлюз підключається до мережевого сервера через звичайні IP-з'єднання і працює як прозорий міст, виконуючи перетворення між RF-пакетами та IP-пакетами. В бездротовому зв'язку використовується перевага Long Range (Діапазон далекого Дії) для фізичного рівня LoRe, що дозволяє одноточечне з'єднання між кінцевим пристроєм і одним або декількома шлюзовими системами.

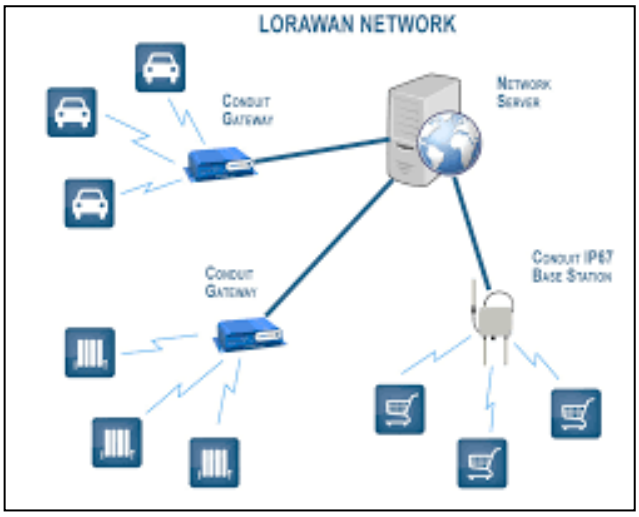


Рисунок 1.4 – Архітектура мережі із LoRaWAN

Характеристики визначають параметри фізичного рівня (LoRaWAN) пристрої для інфраструктури (LoRa) і, таким чином, забезпечують безшовну функціональну сумісність між виробниками, про що свідчить програма сертифікації.

Хоча специфікація визначає технічну реалізацію, вона не визначає будь-яку комерційну модель або тип розгортання (публічний, колективний, приватний, корпоративний), і тому пропонує галузі свободу інновацій та диференціації того, як вона використовується.

Під час буму IoT стало майже відразу ясно, що наявні стандарти передачі даних для стабільної роботи вже не актуальні.

На перший погляд, у нас вже є готові і обкатані рішення. Wi-Fi, LTE, чому не використовувати їх? Причин кілька. Уявімо собі будинок на 400 квартир, в кожному з яких коштує два водолічильника і електролічильник. Припустимо, це сучасний будинок, і кожен лічильник передає дані в Інтернет.

Обсяг. На один житловий будинок з 400 квартир доведеться 1200 лічильників-користувачів. У них буде копійчаний трафік, але якщо всі вони будуть висіти, наприклад, на базовій станції LTE, то місця для людей на цій базовій станції вже не залишиться. І це один будинок. Але ж базову станцію, зазвичай, ставлять на мікрорайон або навіть більше.

Споживання. Якщо електролічильника ще можна забезпечити харчування, то тягнути кабель до водолічильників не дуже зручно. Значить радіомодуль водолічильника повинен працювати від батареї. Але навіть хорошу батарейку Wi-Fi й LTE з'їдять за кілька діб. Ми ж хочемо, щоб міняти елемент живлення не доводилося мінімум рік.

Інші пріоритети. Нам не потрібен канал зв'язку в 5 Мбіт / с, щоб раз на добу передати, скільки кубів води набігло по кожній квартирі. Досить лічених біт. Ми обмежені за потужністю передавача, треба, щоб він не їв батарейку. Значить, можна використовувати правило «більше енергії в один біт - вище ймовірність приймання» таким чином, що канал зв'язку на мінімальній швидкості й з мінімальною потужністю гарантовано пройде потрібну відстань. Навіть якщо сигнал буде нижче рівня шуму.

LoRaWAN має три різних класи кінцевих пристроїв для задоволення різних потреб, відображених в широкому спектрі додатків:

1) Клас А - двонаправлені кінцеві пристрої с найменшою потужністю. Цей клас повинен підтримуватися всіма кінцевими пристроями LoRaWAN за замовчуванням. Передача завжди ініціюється кінцевим пристроєм і повністю асинхронна. Кожна передача по висхідній лінії зв'язку може бути відправлена

в будь-який час і за нею йдуть два коротких вікна низхідній лінії зв'язку, що дає можливість для двобічної зв'язку або команд управління мережею, якщо це необхідно. Це протокол типу ALOHA.

Кінцеве пристрій може увійти в режим з низьким енергоспоживанням в залежності від його індивідуальних налаштувань. Це робить клас А самим енергоефективним і час життя сенсора від 5 років і вище, в той же час дозволяючи здійснювати зв'язок по висхідній лінії зв'язку в будь-який час.

Оскільки зв'язок по низхідній лінії зв'язку завжди повинна слідувати за передачею по висхідній лінії зв'язку з розкладом, визначеним додатком кінцевого пристрою, зв'язок по низхідній лінії зв'язку повинна буферизованного на мережевому сервері до наступної події висхідній лінії зв'язку.

2) Клас B - двонаправлені кінцеві пристрої з певним часом очікування низхідного потоку. На додаток до початкових вікон прийому класу А, пристрої класу B синхронізуються з мережею з використанням періодичних маяків і відкривають «слоти для перевірки» низхідного потоку за розкладом. Це забезпечує мережі можливість відправляти спадну зв'язок з певною затримкою, але за рахунок деякого додаткового енергоспоживання в кінцевому пристрої. Затримка програмується до 128 секунд для різних додатків, а додаткове енергоспоживання досить низька, щоб залишатися в силі для додатків на батарейках.

3) Клас C - двонаправлені кінцеві пристрої з найменшою затримкою. На додаток до структури класу А в висхідній лінії зв'язку, за якою слідують два вікна низхідній лінії зв'язку, клас С додатково зменшує затримку на низхідній лінії зв'язку, постійно підтримуючи прийом на кінцевому пристрої, коли пристрій не передає (полудуплекс). Виходячи з цього, мережевий сервер може ініціювати передачу по низхідній лінії зв'язку в будь-який час, якщо приймач кінцевого пристрою відкритий, тому немає затримки.

Компромісом є витік потужності приймача (до ~ 50 мВт), і тому клас С підходить для додатків, де є безперервна потужність. Для пристроїв з

батарейним харчуванням можливе тимчасове перемикання між класами A і C, що корисно для періодичних завдань, таких як оновлення прошивки через ефір.

На додаток до стрибкоподібної перебудови частоти усі пакети зв'язку між кінцевими пристроями і шлюзами також включають в себе параметр «Швидкість передачі даних» (Data Rate). Вибір DR дозволяє встановити динамічний компроміс між діапазоном зв'язку і тривалістю повідомлення. Крім того, завдяки технології з розширеним спектром, зв'язок з різними DR не заважає один одному і створює набір віртуальних «кодових» каналів, що збільшують пропускну здатність шлюзу. Щоб максимально збільшити час автономної роботи кінцевих пристроїв і загальну пропускну здатність мережі, мережевий сервер LoRaWAN управляє налаштуванням DR і вихідною потужністю RF для кожного кінцевого пристрою індивідуально за допомогою схеми адаптивної швидкості передачі даних (ADR).

Швидкість передачі даних в режимі LoRaWAN коливається від 0,3 кбіт / с до 50 Кбіт / с (в режимі FSK).

Безпека є основним завданням для будь-якого масового розгортання IoT, а специфікація LoRaWAN визначає два рівня криптографії:

– унікальний 128-розрядний ключ мережевого сеансу, яким користуються між кінцевим пристроєм та сервером (NwkSKey);

– унікальний 128-бітний ключ сеансу додатка (AppSKey), яким користуються на рівні додатку.

Алгоритми AES використовуються для забезпечення аутентифікації і цілісності пакетів на мережевому сервері і наскрізного шифрування на сервері додатків. Надаючи ці два рівня, стає можливим реалізувати «розраховані на багато користувачів» загальні мережі без того, щоб оператор мережі мав видимість даних корисного навантаження користувачів.

Ключі можуть бути активовані за допомогою персоналізації (ABP) на виробничій лінії або при введенні в експлуатацію або ж можуть бути

активовані «по повітрю» безпосередньо на місці підключення (OTAA). OTAA дозволяє при необхідності повторно підключати пристрої.

1.4 Smart city

Розумне місто (Smart city) - це місце, де традиційні мережі і послуги стають більш ефективними з використанням цифрових рішень на благо жителів і бізнесу[9].

Розумне місто виходить за рамки використання цифрових технологій для кращого використання ресурсів і скорочення викидів. Це означає більш розумні мережі міського транспорту, модернізовані об'єкти водопостачання та утилізації відходів, а також більш ефективні способи освітлення і обігріву будівель. Це також означає більш інтерактивну і чуйну міську адміністрацію, більш безпечні громадські місця і забезпечення потреб старіючого населення.

Основна мета розумного міста - оптимізувати міські функції і сприяти економічному зростанню, а також поліпшити якість життя жителів за рахунок використання розумних технологій і аналізу даних. Цінність полягає в тому, як ця технологія використовується, а не просто в тому, скільки технологій доступно.

«Розумність» міста визначається за допомогою набору характеристик (див. рис. 1.5), в тому числі:

– інфраструктура, заснована на технологіях;

– екологічні ініціативи;

– ефективний і функціональність громадського транспорту;

– упевнені і прогресивні плани міста;

– люди, здатні жити і працювати в місті, використовуючи його ресурси.

Рисунок 1.5 – Smart city

Успіх розумного міста залежить від взаємин між державним і приватним секторами, оскільки велика частина роботи по створенню та підтриманню середовища, керуванню даними, виходить за рамки компетенції місцевих органів влади. Наприклад, для інтелектуальних камер відеоспостереження може знадобитися введення і технологія від декількох компаній.

Крім технологій, що використовуються в розумному місті, аналітикам даних також необхідно оцінювати інформацію, надану системами розумного міста, щоб можна було вирішити будь-які проблеми і знайти шлях їх поліпшення.

Розумне місто використовує структуру інформаційних і комунікаційних технологій для створення, впровадження і просування методів розвитку для вирішення міських проблем і створення об'єднаної технологічно підтримуваної і стійкої інфраструктури.

Розумні міста використовують різноманітне програмне забезпечення, призначені для користувача інтерфейси і мережі зв'язку поряд з Інтернетом речей (IoT) для надання загальнодоступних рішень.

З них найважливішим є Інтернет речей. Як приклад це може бути від автомобілів до побутової техніки та вуличних датчиків. Дані, зібрані з цих пристроїв, зберігаються в хмарі або на серверах, що дозволяє підвищити

ефективність як державного, так і приватного секторів і забезпечити економічні вигоди та покращення життя громадян.

Багато пристроїв IoT використовують периферійні обчислення, які гарантують, що по мережі зв'язку доставляються тільки найактуальніші і важливі дані. Крім того, запроваджено систему безпеки для захисту, моніторингу та управління передачею даних з мережі розумного міста, а також запобігання несанкціонованому доступу до мережі IoT міської платформи даних.

Поряд з рішеннями IoT, розумні міста також використовують такі технології, як:

– інтерфейси програмування прикладних програм (API);

– штучний інтелект (AI);

– послуги хмарних обчислень;

– інформаційні панелі;

– машинне навчання;

– зв’язок між машинами;

– меш-мережі.

Серед особливостей розумного міста поєднання автоматизації, машинного навчання та Інтернету речей, що дозволяє впроваджувати технології розумного міста для різноманітних додатків. Наприклад, розумне паркування може допомогти водіям знайти місце для паркування, а також дозволити здійснювати цифрові платежі.

Іншим прикладом може бути інтелектуальне управління дорожнім рухом для моніторингу потоків руху та оптимізації світлофорів для зменшення заторів, а службами спільного користування також можна керувати інфраструктурою розумного міста.

Функції розумного міста також можуть включати енергозбереження та екологічну ефективність, наприклад, вуличні ліхтарі, які приглушуються, коли дороги порожні. Такі технології інтелектуальної мережі можуть

покращити все - від операцій до обслуговування та планування до джерел живлення.

Ініціативи "розумних міст" також можуть бути використані для боротьби зі зміною клімату та забрудненням повітря, а також з поводженням з відходами та санітарією за допомогою збору сміття, урн та систем управління автопарком.

Окрім послуг, розумні міста дозволяють передбачати заходи безпеки, такі як моніторинг зон високої злочинності або використання датчиків для раннього попередження про такі інциденти, як повені, зсуви, урагани чи посухи.

Розумні будівлі також можуть запропонувати управління простором у режимі реального часу або моніторинг структурного стану та зворотний зв'язок, щоб визначити, коли необхідний ремонт. Громадяни також можуть отримати доступ до цієї системи, щоб повідомити посадових осіб про будь-які проблеми, такі як вибоїни, тоді як датчики також можуть контролювати проблеми інфраструктури, такі як протікання у водопровідних трубах.

Крім того, технології розумного міста можуть підвищити ефективність виробництва, міського господарства, використання енергії тощо.

Розумні міста можуть підключати всілякі послуги, щоб забезпечити об’єднані рішення для громадян.

Принцип роботи розумних міст[10]:

Розумні міста виконують чотири кроки для покращення якості життя та забезпечення економічного зростання за допомогою мережі підключених пристроїв Інтернету речей та інших технологій. Ці кроки наступні:

1) Збір - розумні датчики збирають дані в режимі реального часу.

2) Аналіз - дані аналізуються, щоб отримати уявлення про роботу міських служб та операцій.

3) Комунікація - Результати аналізу даних повідомляються особам, які приймають рішення.

4) Дії - Вживаються заходи для покращення діяльності, управління активами та покращення якості життя мешканців міста.

Структура ІКТ об’єднує дані в реальному часі з підключених активів, об’єктів та машин для покращення прийняття рішень. Однак, крім того, громадяни мають можливість взаємодіяти та взаємодіяти з екосистемами розумного міста за допомогою мобільних пристроїв та пов’язаних транспортних засобів та будівель. Поєднуючи пристрої з даними та інфраструктурою міста, можна скоротити витрати, покращити стійкість та спростити такі фактори, як розподіл енергії та збирання сміття, а також зменшити затори та покращити якість повітря.

Підтвердженням важливості розумного міста є те, що 54% населення світу проживає у містах, і очікується, що до 2050 року це зросте до 66%, що додасть ще 2,5 мільярда людей до міського населення протягом наступних трьох десятиліть. Враховуючи цей очікуваний приріст населення, виникає необхідність керувати екологічною, соціальною та економічною стійкістю ресурсів.

А розумні міста дозволяють громадянам та органам місцевого самоврядування спільно працювати над ініціативами та використовувати розумні технології для управління активами та ресурсами у зростаючому міському середовищі.

Перевагою розумного міста є те, що воно створює міське середовище, яке забезпечує високу якість життя мешканців, а також стимулює економічне зростання. Це означає надання набору об’єднаних послуг громадянам зі зниженими витратами на інфраструктуру.

Незважаючи на всі переваги, які пропонують розумні міста, є також проблеми, які потрібно подолати. До них належать урядовці, які дозволяють широку участь громадян. Також існує потреба у тому, щоб приватний та державний сектори приєдналися до мешканців, щоб кожен міг позитивно внести свій внесок у суспільство.

Проекти розумних міст повинні бути прозорими та доступними для громадян через портал відкритих даних або мобільний додаток. Це дозволяє мешканцям працювати з даними та виконувати особисті завдання, такі як оплата рахунків, пошук ефективних варіантів транспортування та оцінка споживання енергії вдома.

Все це вимагає надійної та безпечної системи збору та зберігання даних для запобігання злому або зловживанню. Дані розумних міст також необхідно анонімізувати, щоб запобігти виникненню проблем конфіденційності.

Ймовірно, найбільшою проблемою є підключення, оскільки тисячам або навіть мільйонам пристроїв Інтернету речей потрібно підключатися та працювати в унісон. Це дозволить об'єднати послуги та внести постійні вдосконалення у міру зростання попиту.

Крім технологій, розумні міста також повинні враховувати соціальні фактори, які створюють культурну тканину, привабливу для мешканців та створюють відчуття свого місця. Це особливо важливо для тих міст, які створюються з нуля і потребують залучення жителів.

Розумні міста пропонують багато переваг для поліпшення безпеки громадян, таких як підключені системи спостереження, розумні дороги та моніторинг громадської безпеки, але як щодо захисту самих розумних міст?

Необхідно забезпечити захист розумних міст від кібератак, злому та крадіжки даних, а також переконатися, що дані, про які повідомляється, є точними.

Для того, щоб керувати безпекою розумних міст, необхідно впровадити такі заходи, як сховища фізичних даних, стійке управління автентифікацією та рішення для ідентифікації. Громадянам потрібно довіряти безпеці розумних міст, а це означає, що уряд, підприємства приватного сектора, розробники програмного забезпечення, виробники пристроїв, постачальники енергії та менеджери мережевих послуг повинні працювати разом, щоб запропонувати комплексні рішення з основними цілями безпеки.

Ці основні цілі безпеки можна розбити таким чином:

1) Доступність - дані повинні бути доступні в режимі реального часу з надійним доступом, щоб переконатися, що вони виконують свою функцію моніторингу різних частин інфраструктури розумного міста.

2) Нечесність - дані повинні бути не тільки легкодоступними, але й точними. Це також означає захист від маніпуляцій ззовні.

3) Конфіденційність - конфіденційні дані повинні бути конфіденційними та захищеними від несанкціонованого доступу. Це може означати використання брандмауерів або анонімізацію даних.

4) Підзвітність - користувачі системи повинні нести відповідальність за свої дії та взаємодію з чутливими системами даних. У журналах користувачів має бути записано, хто звертається до інформації, щоб забезпечити відповідальність у разі виникнення проблем.

Законодавство вже впроваджується в різних країнах, наприклад, Закон про вдосконалення кібербезпеки IoT у США, який допомагає визначити та встановити мінімальні вимоги безпеки для підключених пристроїв у розумних містах.

Міста у всьому світі знаходяться на різних етапах розвитку та впровадження розумних технологій. Однак є декілька, хто випереджає цю криву, ведучи шлях до створення повністю розумних міст.

Міський штат Сінгапур вважається одним з лідерів у змаганні за створення повністю розумних міст, а камери Інтернету речей стежать за чистотою громадських місць, щільністю натовпу та пересуванням зареєстрованих транспортних засобів. У Сінгапурі також є системи моніторингу споживання енергії, поводження з відходами та використання води в режимі реального часу. Крім того, існує автономне тестування транспортних засобів та система моніторингу для забезпечення здоров'я та добробуту людей похилого віку.

В іншому місті Канзас-Сіті представив розумні вуличні ліхтарі, інтерактивні кіоски та понад 50 блоків безкоштовного Wi-Fi. Деталі

паркувального місця, вимірювання потоку руху та точки доступу пішоходів також доступні для мешканців за допомогою програми візуалізації даних міста.

Тим часом Сан-Дієго встановив 3200 розумних датчиків для оптимізації руху транспорту та паркування, а також для підвищення громадської безпеки та екологічної обізнаності. Електричні транспортні засоби підтримуються зарядними станціями від сонячних батарей до електричних та підключеними камерами для моніторингу проблем дорожнього руху та злочинності.

Системи моніторингу руху також діють у Дубаї, який пропонує телемедицину та розумні рішення для охорони здоров’я, а також розумні будівлі, комунальні послуги, освіту та туризм. У Барселоні також є розумні транспортні системи з автобусними зупинками, які пропонують безкоштовні порти Wi-Fi та USB для зарядки, а також програма обміну велосипедами та програма для розумного паркування, включаючи варіанти оплати через Інтернет. Температуру, забруднення та шум також вимірюють за допомогою датчиків, які також охоплюють вологість і кількість опадів.

1.5 Ідентифікація об’єктів мережі

Опис об'єкта часто включає різнорідні дані і метадані, які повинні бути описані в структурованої манері, так само, як і тип об'єкту, а також всі можливі дії над об'єктом. Питання ідентифікації та адресації об’єктів в такій величезній мережі, як міська є ключовим для успішної роботи усієї системи.

Ідентифікація речей (IDoT) - це область завдань з присвоєння унікальних ідентифікаторів і пов'язаних метаданих об'єктів IoT, що дозволяє їм обмінюватися інформацією з іншими сутностями в Інтернеті. При цьому «річчю» може бути будь-яка сутність, що має ідентифікатор і можливість передачі даних: і фізична, і логічна. Однак, на відміну від класичного управління ідентифікацією, в рамках IoT необхідно враховувати деякі особливості забезпечення безпеки, а саме:

Життєвий цикл. Деякі об'єкти IoT можуть мати довгий життєвий цикл. Електронна медична запис, наприклад, це логічний об'єкт, який зберігає ідентичність протягом усього життя пацієнта. З іншого боку, ідентифікатор посилки буде існувати тільки протягом процесу доставки пошти.

Взаємовідносини. Важливо розуміти, як IoT-об'єкти пов'язані з іншими сутностями, що не входять в IoT - власниками, адміністраторами, виробниками, користувачами. Власник, користувач або адміністратор пристрою може змінюватися з плином часу, що впливає на процеси ідентифікації, аутентифікації і авторизації.

Знання контексту. Процеси управління ідентифікацією та доступом повинні враховувати контекст. Наприклад, можлива така ситуація, при якій необхідно дозволити користувачеві доступ до системи, але в іншій ситуації відкрити доступ для того ж користувача буде небезпечним (скажімо, в розумній системі оповіщення про пожежу).

Механізми захисту. Методи підтвердження ідентичності в класичному управлінні ідентифікацією складалися протягом багатьох років. Аутентифікація, перевірка цілісності, відмовостійкість вбудовані в такі протоколи як SAML або OpenID. В інтернеті речей ж протоколи зв'язку часто побудовані не на основі інтернет-протоколів, а ресурси пристроїв досить обмежені. Якщо пристрій використовує всього декілька байт для передачі даних, тут не може бути місця для шифрування або інших механізмів безпеки.

Аутентифікація. Мультифакторна аутентифікація ефективна для застосування по відношенню до людей, але не пристроїв, так як багато чинників є біометричними, а пароль в M2M-комунікаціях замінюється токеном або сертифікатом.

Множинні або унікальні ідентифікатори? У разі появи глобальної схеми ідентифікації, за аналогією з IP, необхідно прояснити питання управління критичної інфраструктурою для такої схеми. Нові стандарти протоколів на основі IPv6, такі як 6LoWPAN, показують, що можна створити

ефективну схему привласнення унікальних ідентифікаторів для дуже малих пристроїв. Але для вирішення питань непересічних адресних просторів в глобальному масштабі потрібно інфраструктура, що підтримує динамічні пристрої, що постійно з'являються або зникають з мережі і переміщаються між різними громадськими структурами і закритими мережами; підтримуюча ідентифікацію та аутентифікацію користувачів і захист персональних даних; що дозволяє отримувати і обмінюватися інформацією про об'єкти та їх метаданими.

Ідентифікатори або мережеві адреси? Ідентифікатори служать унікальним покажчиком на об'єкт, тоді як мережева адреса може змінюватися в залежності від фізичного місця розташування або логічного участі в тій чи іншій мережі. У тих випадках, коли ідентифікатор і адреса розрізняються, для ідентифікації об'єктів використовуються більш підходящі схеми, такі як, наприклад, EPC для RFID-тегів або його японський аналог uCode. Точно так само можуть існувати різні схеми адресації.

Для об'єктів в інтернеті використовується IPv4 або IPv6, але об'єкти можуть використовувати і інші приватні схеми і протоколи. При цьому вони можуть бути доступні через інтернет завдяки спеціальним шлюзів, що транслює дані між глобальної і локальної мережею.

Пошук і резолюція. Пошук об'єктів є тривіальним завданням для маленьких мереж, але вимагає значних ресурсів зі збільшенням числа об'єктів. При цьому в динамічному середовищі інтернету речей автоматизовані механізми виявлення необхідні для взаємодії між об'єктами і сервісами.

Система DNS використовується не тільки для трансляції доменів в IP-адреси і навпаки, а й, наприклад, поштовими агентами для пошуку місця доставки повідомлень - загальний механізм для пошуку сервісів в домені з використанням SRV-записів і NAPTR-записів для резолюції об'єктів. Для інтернету речей існують розширення системи DNS Object Naming Service

(ONS) і Object Directory Service (ODS), а також система Handle, які використовуються для вирішення ідентифікаторів об'єктів.

Прозорість і незалежність від мережі. У комп'ютерних мережах ідентифікатори можуть містити інформацію про місце розташування пристроїв. Об'єкти інтернету речей повинні мати ідентифікатори, які не залежать від того, в якій мережі вони знаходяться або яким користувачам належать.

Можливість розширення до мільярдів пристроїв. Один з найбільш вивчених методів створення схеми ідентифікації з підтримкою мільярдів об'єктів - це використання ієрархічного найменування в залежності від контексту, місцезнаходження або домену для усунення можливих конфліктів імен.

Ефективність для дуже простих пристроїв. Об'єкти інтернету речей можуть мати дуже обмежені обчислювальні здатності (сенсори), або ж їх може не існувати зовсім (RFID-теги). Схеми ідентифікації повинні працювати навіть в таких умовах, коли, наприклад, пристрою є всього кілька кілобайт пам'яті.

Захист персональних даних. IoT-пристрої будуть збирати величезну кількість персональної інформації. Схеми ідентифікації повинні підтримувати різні рівні доступу до даних для різних користувачів і захищати зібрані дані за замовчуванням.

Гнучкість і розширюваність. Виходячи з передбачуваної кількості об'єктів, схема ідентифікації для інтернету речей повинна бути гнучкою і розширюваної.

Безпека. Більшість сучасних рішень для ідентифікації IoT фокусуються на надання масштабованості сервісу іменування і адресації, при цьому безпека перебуває на другому плані. Обов'язковий функціонал системи повинен включати в себе:

– аутентифікацію при доступі до даних в процесі пошуку або резолюції;

– авторизацію і перевірку прав при доступі до даних про іменування і адресації, перевірку таких даних на справжність;

– шифрування даних при обміні і запобігання перехоплення пакетів; запобігання маніпуляцій з кешем системи; захист від DoS-атак;

– запобігання реєстрації шкідливих об'єктів.

Ідентифікатори об'єктів - використовуються для ідентифікації фізичних або віртуальних об'єктів. Серед поширені такі системи ідентифікації, як EPC, UPC, Handle / DOI, UUID, MAC, Ecode, OID, CID.

OID є спільною схемою кодування, рекомендованої для однозначної ідентифікації об'єкта в глобальному масштабі. Сьогодні OID успішно використовується в багатьох сферах, таких як інформаційна безпека, управління мережами, сенсорні мережі, служби електронної охорони здоров'я і т.д. Понад 100 IoT компаній зареєстровані в OID через міністерства, комітети, підприємства і науково-дослідні інститути.

Базові правила кодування або BER - набір правил, що пояснює, як представити будь-яку структуру даних, описану згідно ASN.1, в вигляді послідовності 8-бітних октетів. Для того, щоб різні типи даних можна було описувати схожим чином, в X.690 була визначена загальна структура блоку закодованої інформації, яка складається з таких трьох частин:

1) Ідентифікатор - один або кілька октетів, в яких міститься інформація про тип закодованих даних.

2) Частина, що містить інформацію про довжину блоку - один або кілька октетів, в яких міститься інформація про довжину закодованих даних.

3) Частина, що містить закодовану інформацію.

Система CID (Communication Identifier) - це публічна призначена для користувача система присвоєння ID в контексті Internet of Things. Це система розподілу, управління та зберігання CID-ідентифікаторів.

Кожен CID-ідентифікатор складається з трьох частин: область сумісності, область типу та його інформаційну область. Дві перших є опціональними, але область інформації обов'язкове. Область сумісності

потрібна для сумісності з існуючими IoT ID сервісними схемами, складається ця область з 8-бітного коду країни / організації (COC) і 8-бітного коду системи іменувань (NSC).

Область типу потрібна для реалізації ефективного менеджменту і статистичного аналізу IoT-ідентифікаторів, розрізняючи схеми, об'єкти найменування та області застосування різних систем найменування. Область типу складається з 4-бітного типу кодування (CT), який специфікує обсяг області інформації, 4-бітного типу ресурсів (RT), який використовується для специфікації типу IoT-ресурсу, наприклад, штрих-код, RFID, сенсор і так далі, і 8-бітного типу бізнесу (BT), який специфікує область застосування IoT-ідентифікаторів, наприклад, сільське господарство, виробництво і т.д. Область інформації необхідна для специфікації детальної інформації названих IoT-ресурсів, наприклад, сутність ресурсу, властивості і т.д.

ECODE (Entity Code) - це система ідентифікації для інтернету речей, яка запропонована організацією Article Numbering Center of China. Кожен ECODE-ідентифікатор складається з трьох різних частин, включаючи версію (V), ідентифікатор системи нумерації (NSI) і майстер даних (MD). Версія розміром 4 біта використовується для розрізнення кодових структур системи ECODE.

Ідентифікатор системи нумерації (NSI) вказує на код іншої ідентифікаційної системи. Дотримуючись розрізнення в версії, розмір NSI може бути 8 біт двійкових чисел, 4 десяткових або 5 десяткових. Майстер даних використовується для специфікації ідентифікаційних кодів галузі або прикладної системи. Він знаходиться у веденні і підтримується місцевою організацією управління кожної системи ідентифікації, включаючи структуру кодування і принцип розподілу ідентифікаторів.

Об'єкти в системі DOI можуть приймати будь-яку форму: ідентифікатор може бути призначений будь-який суті: фізичної, цифровий або абстрактної. Об'єкти в архітектурі DOA описуються як цифрові. Між

двома підходами немає конфлікту, так як будь-яка сутність може розглядатися з точки зору її цифрового уявлення.

Синтаксис складання ідентифікаторів DOA і DOI ідентичний. Ліміту на довжину самого імені або елементів суфікса або префікса не існує. Імена можуть містити будь-які друковані Unicode-символи і не залежать від регістра. Комбінація унікального префіксу, виданого конкретному реєстратору, та унікального суфікса, що видається реєстратором, очевидно, унікальна сама по собі, що і дозволяє децентралізовано реєструвати ідентифікатори.

Префікс складається з двох компонентів, директорії і реєстратора, між якими ставиться крапка (індикатор директорії у імен DOI завжди дорівнює 10). Реєстратору можуть бути видані численні префікси. Після призначення об'єкту імені, воно не може змінюватися, навіть якщо об'єкт перестав існувати, при цьому в процесі резолюції такого об'єкта має видаватися відповідне повідомлення. Резолюція - це процес, в якому ідентифікатор є запитом до мережевого сервісу на отримання актуальної інформації (даних про стан), що відносяться до визначеної сутності, найчастіше - місце розташування.

Handle System Система резолюції (дозволу; хендл; Handle system) була створена, щоб подолати обмеження функціональності існуючих систем ідентифікації об'єктів в інтернеті. Handle System підтримує множинну резолюцію, тобто відповіддю на запит може бути розташування різних примірників об'єкта, пов'язані сервіси, і будь-яка інша інформація, зазначена в метаданих об'єкта.

Комунікаційні ідентифікатори - використовуються для ідентифікації пристроїв в процесі обміну даними через мережу. До цієї категорії відноситься IPv6.

IPv6 - це шоста версія інтернет-протоколу, основною відмінністю якої від попередньої версії (IPv4) є 128-бітний формат IP-адреси замість вичерпавшого свої ресурси «звичайного», 32-бітного.

Уже до кінця XX століття стало зрозуміло, що Інтернет розрісся настільки, що запасу 32-бітних адрес виду 122.55.47.22, яких всього 4.3 мільярда на весь Інтернет, скоро може не вистачити. І регулятори Інтернету спішно розробили нову версію інтернет-протоколу, в якій IP-адреса має довжину в 128 біт і містить у собі 32 шістнадцяткові символи. У поспіху регулятори не подбали про сумісність старого і нового протоколів, що і стало причиною такої довгої затримки при переході на нову версію. До того ж, формат пакету даних в IPv6 істотно відрізняється від пакета IPv4, що робить взаєморозуміння двох версій протоколу практично неможливим.

Ідентифікатори додатків - використовуються для ідентифікації сервісів і додатків в рамках інтернету речей, наприклад URL, URI.

URI (Uniform Resource Identifier) надає можливості для ідентифікації ресурсу у Всесвітній Павутині (WWW). Кожен URI починається з імені схеми, яка, в свою чергу, специфікує ідентифікатори. Специфікація URI визначає реалізацію доступу до файлового серверу, зазвичай через http-протокол, хоча може використовуватися і інший. URI підтримує програми, які інтегрують в собі безліч ідентифікаційних рішень (наприклад, EPC і IPv6). Така інтеграція вважається важливою для деяких додатків, які виходять за рамки кількох різнорідних IoT-систем, що використовують різні ідентифікаційні технології.

URN (Uniformed Resource Name) - це специфікація для визначення ідентифікаторів ресурсів для використання в Інтернеті. RFC 2141 (старіший, ніж RFC 3986, який оголосив URN застарілим поняттям) визначав формальний реєстраційний процес в якості простору імен URN. Більшість сучасних реалізацій URN - це протокол http, який містить URL релевантного сервісу. Реєстрація URN на сьогоднішній момент має потребу адміністрування для визначення простору імен URN і перенаправлення до релевантному сервісу.

На даний момент існує кілька прикладів впровадження систем для іменування, адресації й виявлення об'єктів інтернету речей (IPv6, Handle,

EPC / ONS і ін.). Однак передчасно говорити, що якась із цих систем стане домінуючою, швидше за вони існуватимуть одночасно, обслуговуючи різні запити, сфери застосування географії. Більшість з них було створено не для інтернету речей, а для розширення можливостей адресації в інтернеті або відстеження цифрових або фізичних об`єктів.

У той же час, відкрита архітектура інтернету досі дозволяла розвивати інновації в комунікаціях і додатках без внесення фундаментальних змін в базові протоколи. Серед існуючих і апробованих технологій управління інформацією, що розділяють подібний підхід, можна виділити архітектуру DOA і її ключову частину - Handle System, яка є вже більше 15 років. Гнучкий механізм резолюції ідентифікаторів дає можливість для еволюції системи і сервісів на її основі. При цьому Handle System є розподіленою системою, функції якій розподілені між безліччю локальних провайдерів. Згодом, цілком ймовірно і поява нових систем, що володіють якостями DOA, наприклад, на основі децентралізованого реєстру[11].

1.6 Постановка задачі

Дослідити методи ідентифікації та розпізнання об’єктів, а саме математичні моделі, алгоритми та технології, що сприяють вирішенню завданню ідентифікації.

Беручи до уваги сервіси, що надаються розумними містами і використовуючи результати порівняння технологій для побудови інформаційних систем інтелектуальних мереж міста розробити вимоги для моделі інформаційної системи ідентифікації, для забезпечення оптимальної безперебійної роботи.

Класифікувати різновиди систем управління ідентифікацію. Розробити архітектуру інформаційної системи розумного міста. Підвести підсумки результатів виконаної роботи.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ ІНФОРМАЦІЙНИХ МЕРЕЖ

2.1 Ідентифікація мереж

Завданню ідентифікації присвячено неосяжну кількість робіт, що відрізняються не тільки типами об'єктів, які необхідно ідентифікувати, а й самими методами та алгоритмами ідентифікації. Велика увага у цих роботах приділяється ідентифікації лінійних динамічних об'єктів, що описуються диференціальними чи різницевими рівняннями з невідомими коефіцієнтами. Серед різноманітних алгоритмів ідентифікації, призначених для оцінювання коефіцієнтів рівнянь за даними, що спостерігаються, частіше всього використовуються рекурентні алгоритми, що дозволяють здійснити ідентифікацію нормальної роботи об'єкта[12].

Завдання ідентифікації виникає при вивченні властивостей та особливостей об'єктів з метою подальшого керування ними, або при створенні адаптивних систем, в яких на основі ідентифікації об'єкта виробляються оптимальні впливи, що управляють.

Ідентифікація об'єктів у загальному випадку полягає в визначення їх структури та параметрів за даними, що спостерігаються - вхідний вплив і вихідній величині. Об'єкти описуються диференціальними, інтегральними чи функціональними рівняннями щодо деяких координат, що характеризують їх стан.

Ідентифікація називається активною, якщо вхідний сигнал x (t) - тестовий (подається зі спеціального генератора). Якщо ж він вимірюється в процесі нормального функціонування об'єкта, то має місце пасивна ідентифікація. Визначення порядків лівої n і правої m частини диференціального рівняння називають структурною ідентифікацією, а визначення коефіцієнтів a_i , $i \in [1, n]$, і b_i , $i \in [1, m + 1]$ – параметричною ідентифікацією. Це стосується передавальної функції W (s) = B (s) A (s) , де n_i

a_i , i∈ [1, n] – порядок та коефіцієнти по лінома знаменника A (s) , а m_i b_i , i∈ [1, m + 1] - порядок і коефіцієнти полінома чисельника B(s).

Завдання визначення імпульсної, амплітудної частотної та фазової частотної характеристик називають непараметричною ідентифікацією. Суть вирішення задачі непараметричної ідентифікації зводиться до обчислення значень тієї чи іншої характеристики у кожній точці інтервалу визначення. Слід зазначити приватні постановки завдання ідентифікації, коли визначають не модель, а деякі властивості об'єкта управління, наприклад, лінійність, стаціонарність, наявність чистого запізнення. Існують два підходи, на яких базуються алгоритми ідентифікації. У першому випадку передбачається попередній збір інформації про об'єкт з подальшою її обробкою, причому місця збору та обробки можуть бути рознесені. Алгоритми, що базуються на такому підході, називають ретроспективними. Якщо шукані параметри та характеристики визначаються в міру надходження апріорної інформації, в так званому покроковому режимі, алгоритми називають рекурентними.

Рекурентні алгоритми використовуються, наприклад, при ідентифікації нестаціонарних об'єктів або за необхідності уточнення знайдених оцінок параметрів у стаціонарних об'єктах. Ідентифікацію можна проводити в покроковому режимі і без надходження нової апріорної інформації. Такі алгоритми називають ітераційними.

Ідентифікація здійснюється за допомогою настоюваної моделі тієї чи іншої структури, параметри якої можуть змінюватися[13]. За спостережуваними вхідними впливами та вихідними величинам об'єкта підбираються параметри моделі, що налаштовується, що забезпечують екстремум деякого критерію, що характеризує якість ідентифікації.

Структурна схема системи ідентифікації з градієнтною самонастроювальною моделлю (ГСМ) (див. рис. 2.1).

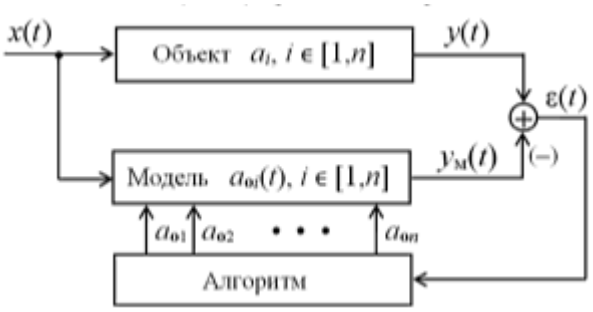


Рисунок 2.1 – Структурна схема системи

Апріорі передбачається, що існує

$$a_{oi}^{(1)}(t) = -K_i \frac{\partial J\{\varepsilon(t)\}}{\partial a_{oi}(t)},\ i \in [1, n],\ K_i > 0, \qquad (2.1)$$

де J - Вибирається критерій налаштування моделі за параметрами a_{oi} (t). Якщо припущення (2.1) виконується, то алгоритм ідентифікації (підстроювання параметрів моделі до параметрів об'єкта) має вигляд

$$a_{oi}(t) = a_{oi}(0) - K_i \int_0^t \frac{\partial J\{\varepsilon(\tau)\}}{\partial a_{oi}(\tau)}\, d\tau,\ i \in [1, n], \qquad (2.2)$$

де a_{oi} (0), i∈ [1, n] – початкові умови параметрів моделі, що задаються. Як ілюстрацію функціонування ГСМ розглянемо приклад. Нехай ідентифікований об'єкт описується рівнянням

$$\sum_{i=1}^{n} a_i y^{(i-1)}(t) = x(t).$$

Диференціальне рівняння моделі

$$\sum_{i=1}^{n} a_{oi}(t) y_м^{(i-1)}(t) = x(t).$$

Критерій налаштування параметрів моделі до параметрів об'єкта виберемо у вигляді

$$J\{\varepsilon(t) = y(t) - y_м(t)\} = \frac{1}{2} \int_{t-T}^{t} \varepsilon^2(\tau) d\tau.$$

Тоді припущення, що на інтервалі тривалістю Т (етапі підстроювання параметрів моделі)

$$a_{oi}(t) \approx \text{const}, \quad i \in [1, n],$$

можна записати

$$\frac{\partial J}{\partial a_{oi}} = \int_{t-T}^{t} \varepsilon(\tau)[-u_i(\tau)]d\tau,$$

де

$$u_i(\tau) = \frac{\partial y_M(\tau)}{\partial a_{oi}(\tau)}, \; i \in [1, n],$$

називаються функціями чутливості моделі за її параметрами і є рішенням диференціального рівняння чуттєвість

$$\sum_{j=1}^{n} a_{oj}(t) u_i^{(j-1)}(t) = -y_M^{(i-1)}(t), \; i \in [1, n],$$

з нульовими початковими умовами

$$u_i^{(j-1)}(0) = 0, \quad j \in [1, n-1].$$

При цьому алгоритм ідентифікації (2.2) набуває вигляду

$$a_{oi}(t) = a_{oi}(0) + K_i \int_{0}^{t} \int_{\tau-T}^{\tau} \varepsilon(\xi) u_i(\xi) \, d\xi \, d\tau, \; i \in [1, n].$$

Коригуючими параметрами алгоритму є час усереднення T, коефіцієнти K_i, i∈ [1, n], що коригують динаміку системи, початкові умови a_{oi} (0), i∈ [1, n].

Початкові умови слідують вибирати з фізичних міркувань під час оцінювання параметрів об'єкта у кожному даному випадку.

Що стосується коефіцієнтів K_i , i∈ [1, n] , то вони є деяким аналогом коефіцієнтів посилення систем управління та у випадку їх можна покласти рівними одиниці.

До параметра T пред'являються суперечливі вимоги, що створює проблему його вибору. З одного боку необхідно виконувати умову a_{oi} (t) ≈

const, i∈ [1, n], на інтервалі T з цієї точки зору тривалість T слід зменшувати. Чим менше T, тим менша помилка фіксації оцінок моделі у цьому інтервалі. З іншого боку, інтегральний оператор на інтервалі інтегрування [0, T] згладжує (усереднює) поміхи, що спотворюють сигнали при їх вимірі. Тому якихось конкретних рекомендацій щодо вибору параметра T немає.

Перевага ГСМ у тому, що це система замкнутого типу і якщо вихідний сигнал y (t) об'єкта спотворений центрованою і не корелюючою у (t) перешкодою δy (t), то її наявність не призводить до зміщеності оцінок a_{oi} (t), i∈ [1, n].

Недоліки ГСМ

1) ГСМ описуються системою нелінійних, нестаціонарних, інтегродиференціальних рівнянь, заданих у неявному вигляді, і тому неможна провести необхідний теоретичний аналіз як точності і швидкодії, і навіть стійкості.

2) Як правило, критерії налаштування J – не унімодальні і тому збіжність параметрів моделі a_{oi} (t) до параметрів об'єкта a_i, i∈ [1, n], буде мати місце, якщо початкові умови a_{oi} , i∈ [1, n], досить близькі до параметрів об'єкта a_i , i∈ [1, n] , а це пов'язано з необхідністю додаткової апріорної інформації.

3) Функції чутливості u_i (t) є функціональними похідними, і їх визначення через моделі чутливості справедливе лише при дуже повільній зміні параметрів моделі a_{oi} (t), i∈ [1, n]. Тому ГСМ мають принципово низьку швидкодію.

4) ГСМ характеризуються сильним взаємним зв'язком між каналами ідентифікації. Тому зі збільшенням кількості n параметрів, що підлаштовуються, швидкодія різко падає.

Структурна схема системи ідентифікації з не градієнтною моделлю, що само налаштовується (НГСМ) (див. рис. 2.2). Нехай об'єкт описується рівнянням

$$y^{(n)}(t)+\sum_{i=1}^{n}a_i y^{(i-1)}(t)=\sum_{i=1}^{m}b_i x^{(i-1)}(t)\,. \qquad (2.3)$$

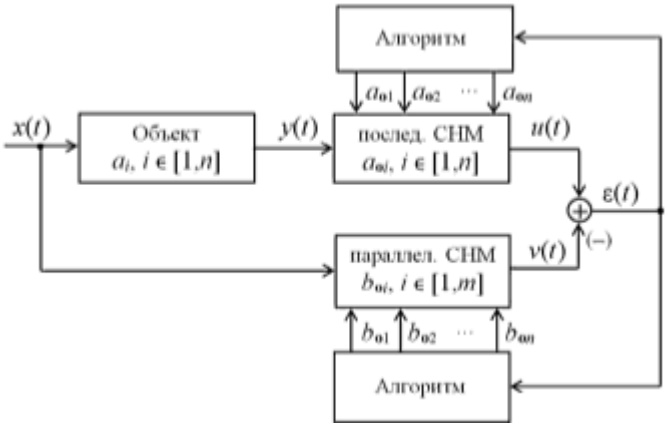


Рисунок 2.2 - Структурна схема системи ідентифікації з не градієнтною моделлю

Послідовна модель має вигляд

$$u^{(n)}(t)+\sum_{i=1}^{n}c_i u^{(i-1)}(t)=y^{(n)}(t)+\sum_{i=1}^{n}a_{0i}(t)y^{(i-1)}(t)\,, \qquad (2.4)$$

а паралельна –

$$v^{(n)}(t)+\sum_{i=1}^{n}c_i v^{(i-1)}(t)=\sum_{i=1}^{m}b_{0i}(t)x^{(i-1)}(t)\,. \qquad (2.5)$$

Коефіцієнти $c_i > 0$, $i \in [1, n]$, послідовної та паралельної моделей задаються апріорі з умови їх стійкості, а за необхідності та з додаткових умов, наприклад, забезпечення необхідної смуги пропускання паралельної моделі для згладжування поміх δx(t). Якщо ввести на розгляд неузгодженість

$$\varepsilon(t)=u(t)-v(t)\,,$$

помилку за параметрами послідовної моделі

$$e_{a_i}(t)=a_i-a_{0i}(t),\ i\in[1,\,n]\,,$$

помилку за параметрами паралельної моделі

$$e_{b_i}(t)=b_i-b_{0i}(t),\ i\in[1,\,m]\,,$$

то динаміку НГСМ можна буде описати системою диференціальних рівнянь

$$\begin{cases} e_{a_i}^{(1)} = f_{a_i}[e_{a_i}, e_{b_i}], \ i \in [1, n], \\ e_{b_i}^{(1)} = f_{b_i}[e_{a_i}, e_{b_i}], \ i \in [1, m]. \end{cases}$$

Алгоритм ідентифікації синтезується за умов стійкості

$$\lim_{t\to\infty} e_{a_i}(t) = 0 \ \text{и} \ \lim_{t\to\infty} e_{b_i}(t) = 0,$$

В якості критерію стійкості можна використовувати, наприклад, другий метод Ляпунова або метод гіперстійкості Попова.

При використанні другого методу Ляпунова вибирається функція Ляпунова, наприклад у вигляді

$$V(t) = \frac{1}{2}\left[\sum_{i=1}^{n} K_{a_i} e_{a_i}^2(t) + \sum_{i=1}^{m} K_{b_i} e_{b_i}^2(t)\right] > 0, \qquad (2.6)$$

де K_{ai} і K_{bi} визначають швидкість збіжності алгоритму і задаються з умови корекції динаміки системи ідентифікації, причому $K_{ai} > 0$, і є [1, n], $K_{bi} > 0$, і є [1 , m] , зокрема їх можна покласти рівними одиниці.

Згідно з критерієм Ляпунова стійкість матиме місце, якщо

$$W(t) = \frac{dV(t)}{dt} < 0. \qquad (2.7)$$

Визначимо допоміжну функцію q(t), яка виходить при почленном відніманні рівняння (2.5) з рівняння (2.8):

$$q(t) = \varepsilon^{(n)}(t) + \sum_{i=1}^{n} c_i \varepsilon^{(i-1)}(t) =$$

$$= y^{(n)}(t) + \sum_{i=1}^{n} a_{oi}(t) y^{(i-1)}(t) - \sum_{i=1}^{m} b_{oi}(t) x^{(i-1)}(t).$$

В отриманому вираженні замінимо

$$a_{oi}(t) = a_i - e_{a_i}(t), \ b_{oi}(t) = b_i - e_{b_i}(t)$$

і після нескладних перетворень отримаємо

$$q(t) = -\sum_{i=1}^{n} e_{a_i}(t) y^{(i-1)}(t) + \sum_{i=1}^{m} e_{b_i}(t) x^{(i-1)}(t) . \qquad (2.8)$$

Тепер умову стійкості (2.7) подаємо у вигляді

$$W(t) = \frac{dV(t)}{dt} < -q^2(t) . \qquad (2.9)$$

Визначимо

$$\frac{dV(t)}{dt} = \sum_{i=1}^{n} K_{a_i} e_{a_i}(t) e_{a_i}^{(1)}(t) + \sum_{i=1}^{m} K_{b_i} e_{b_i}(t) e_{b_i}^{(1)}(t) \qquad (2.10)$$

і

$$-q^2(t) = \sum_{i=1}^{n} e_{a_i}(t) y^{(i-1)}(t) q(t) - \sum_{i=1}^{m} e_{b_i}(t) x^{(i-1)}(t) q(t) . \qquad (2.11)$$

Відповідно до (2.9) прирівняємо у лівій та правій частині виразів (2.10) та (2.11) доданки при однакових помилках e_{ai} (t) та e_{bi} (t). Отримаємо

$$e_{a_i}^{(1)}(t) = \frac{1}{K_{a_i}} y^{(i-1)}(t) q(t) , \; i \in [1, n],$$

$$e_{b_i}^{(1)}(t) = -\frac{1}{K_{b_i}} x^{(i-1)}(t) q(t) , \; i \in [1, m],$$

Звідки, маючи на увазі, що

$$e_{a_i}(t) = a_i - a_{oi}(t), \; i \in [1, n], \quad \text{и} \quad e_{b_i}(t) = b_i - b_{oi}(t), \quad i \in [1, m],$$

а отже,

$$a_{oi}^{(1)}(t) = [a_i - e_{a_i}(t)]^{(1)} = -e_{a_i}^{(1)}(t), \; i \in [1, n],$$

$$b_{oi}^{(1)}(t) = [b_i - e_{b_i}(t)]^{(1)} = -e_{b_i}^{(1)}(t), \; i \in [1, m],$$

отримаємо алгоритм ідентифікації

$$a_{oi}(t) = a_{oi}(0) - \frac{1}{K_{a_i}} \int_0^t y^{(i-1)}(\tau) q(\tau) \, d\tau , \; i \in [1, n],$$

$$b_{oi}(t) = b_{oi}(0) + \frac{1}{K_{b_i}} \int_0^t x^{(i-1)}(\tau) q(\tau) \, d\tau , \; i \in [1, m] .$$

Функцію q(t) можна визначити виразом

$$q(t) = \varepsilon^{(n)}(t) + \sum_{i=1}^{n} c_i \varepsilon^{(i-1)}(t).$$

Перевагою НГСМ є гарантія збіжності оцінок a_{oi} (t) , b_{oi} (t) до параметрів a_i , b_i об'єкта за будь-яких початкових умов при відсутності поміх.

Недоліки

1) НГСМ описується системою нелінійних, нестаціонарних, диференціальних рівнянь, заданих у неявній формі, тому неможливо провести теоретичний аналіз точності та швидкодії алгоритму.

2) У алгоритм ідентифікації входять усі похідні вхідного та вихідного сигналів об'єкта. Виникає необхідність їхнього виміру.

3) Вирішення модельних завдань ілюструє низька швидкодія НГСМ, яка зі збільшенням n або m різко падає.

4) Відсутнє згладжування високочастотних складових поміхи δy (t) через однакові порядків n лівої та правої частини рівняння послідовної моделі.

Зміна параметрів настоюваної моделі здійснюється з допомогою адаптивних пристроїв, що реалізують алгоритми ідентифікації. Наразі запропоновано різні адаптивні алгоритми ідентифікації:

- абсолютно оптимальні алгоритми ідентифікації;
- абсолютно оптимальні на класі алгоритми ідентифікації;
- акселерантні алгоритми ідентифікації;
- модифіковані алгоритми ідентифікації;
- алгоритми ідентифікації нестаціонарних об'єктів;
- структурна та параметрична ідентифікації лінійного стаціонарного об'єкта.

Численність і різноманітність моделей, критеріїв і алгоритмів, що настроюються, природно, ускладнює розв'язання конкретних завдань ідентифікації. Ця обставина втілює до життя спеціальні роботи з експериментального дослідження та порівняння алгоритмів ідентифікації для

типових завдань. На жаль, результати цих робіт, крім констатації окремих фактів не дозволяють встановити будь-які загальні закономірності. Практика застосування адаптивних алгоритмів ідентифікації виявила, що алгоритми найпростішої форми – типу стохастичної апроксимації – часто виявлялися непрацездатними.

2.2 Розпізнання та ідентифікація

Розпізнавання складних об'єктів та явищ вимагає створення спеціальних систем розпізнавання — складних динамічних систем, які складаються в загальному випадку з колективу підготовлених фахівців та сукупності технічних засобів отримання та переробки інформації та призначених для вирішення на основі спеціально сконструйованих алгоритмів задач розпізнавання відповідних об'єктів чи явищ[14].

Системи розпізнавання можна поділити на прості і складні в залежності від того, фізично однорідна або фізично неоднорідна інформація використовується для опису об'єктів, що розпізнаються, чи мають ознаки, на мові яких зроблено опис алфавіту класів, єдину або різну фізичну природу.

Якщо як принцип класифікації використовувати спосіб отримання апостеріорної інформації, то складні системи можна поділити на одноріневі та багаторівневі.

Якщо як принцип класифікації використовувати характер інформації про ознаки об'єктів, що розпізнаються, які підрозділили на детерміновані, імовірнісні, логічні та структурні, то залежно від того, мовою яких ознак проводиться опис цих об'єктів, інакше — залежно від того, який алгоритм розпізнавання реалізований , системи розпізнавання можуть бути поділені на детерміновані, імовірнісні, логічні, структурні та комбіновані.

Процес розпізнавання полягає в тому, що система розпізнавання на підставі зіставлення апостеріорної інформації щодо кожного об'єкта, що надійшов на вхід, або явища з апріорним описом класів приймає рішення про належність цього об'єкта (явлення) до одного з класів. Правило, яке кожному

об'єкту ставить у відповідність певну назву класу, називають вирішальним правилом. У літературі, присвяченій розпізнаванню образів, утвердилася думка, що суть проблеми розпізнавання полягає у визначенні вирішальних правил, знаходженні в ознаковому просторі таких меж (вирішальних кордонів), дотримуючись яких ознакові простори оптимальним чином, наприклад, з точки зору мінімізації помилок розпізнавання, поділяються на області, відповідні класам.

При визначенні вирішальних правил (вирішальних меж у ознаковому просторі) залежно від обсягу вихідної апріорної інформації розглядаються такі ситуації:

1) Кількість вихідної інформації достатньо для того, щоб шляхом її аналізу та безпосередньої обробки визначити вирішальні правила.

2) Кількість вихідної інформації недостатньо для визначення вирішальних правил на основі її безпосередньої обробки, у зв'язку з чим реалізується процедура навчання.

У ситуаціях 1 і 2 завдання відшукання вирішальних правил полягає в тому, що алфавіт класів об'єктів і апріорний словник ознак, призначених їх описів, відомі. Розглядається також така ситуація, коли словник ознак відомий, але невідомий алфавіт класів. При цьому, однак, визначено певний набір правил, відповідно до яких на підставі процедури самонавчання знаходиться алфавіт класів.

До складу алгоритму побудови вирішальних правил входять:

– математична модель системи, яка використовується як на стадії проектування системи розпізнавання, так і під час її експлуатації для уточнення структури та параметрів системи;

– методи та алгоритми обробки вимірювальної інформації, одержуваної технічними засобами системи та призначеної для визначення ознак об'єктів, що розпізнаються;

– методи та алгоритми розпізнавання;

– методи та алгоритми у певному сенсі оптимального управління процесом розпізнавання;

– методи та алгоритми оцінки ефективності системи розпізнавання як на стадії проектування, так і в процесі її функціонування тощо.

Призначення систем розпізнавання — отримати інформацію, необхідну для прийняття певних рішень, про належність невідомого об'єкта до того чи іншого класу. Саме така справа в системах медичної та технічної діагностики, геологічної розвідки, метеорологічного прогнозу, криміналістиці, системах розпізнавання цілей тощо. Тому системи розпізнавання, будучи частиною системи управління (автоматичної або автоматизованої), повинні будуватися з урахуванням забезпечення найбільш ефективного використання всього набору припустимих рішень. Цей факт накладає на побудову систем розпізнавання такі обмеження.

1) За інших рівних умов підвищення ефективності прийнятих рішень слід пов'язувати зі ступенем деталізації визначення або призначення або характеру об'єкта, що розпізнається, або явища. Ступінь деталізації визначається кількістю класів, на яку підрозділено безліч об'єктів чи явищ. Так, якщо система управління має m різні рішення, то в алфавіті класів системи розпізнавання, враховуючи сказане, доцільно передбачити m+1 класів.

Тоді, якщо розпізнаний об'єкт відноситься до класу Ω1 приймається рішення l1, якщо до класу Ω2 - рішення h і т. д., якщо об'єкт відноситься до класу Ωm+1, рішення не приймається.

2) Ефективність прийнятих системою управління рішень за інших рівних умов (зокрема, природно, при заданому алфавіті класів) залежить від точності визначення належності об'єкта, що розпізнається, або явища до відповідного класу.

Точність визначення чи помилка розпізнавання при заданому по точності апріорному описі класів визначається розмірністю та інформативністю ознакового простору, обсягом і якістю апостеріорної

інформації про значення ознак (параметрів), якими характеризується об'єкт, що розпізнається. Інакше висловлюючись, розширення алфавіту класів, що підвищує ступінь деталізації визначення призначення чи характеру розпізнаваного об'єкта (явлення), при постійному словнику ознак підвищує помилку розпізнавання.

Розглянута постановка проблеми розпізнавання дозволяє визначити послідовність завдань, що виникають під час розробки системи розпізнавання, запропонувати їх формулювання та можливі методи розв'язання. Найбільш економним методом вирішення проблеми побудови системи розпізнавання є метод математичного або фізико-математичного моделювання. Основна ідея роботи запропонованої моделі системи розпізнавання — реалізація ітеративної процедури, що забезпечує шляхом послідовних наближень синтез системи, ефективність роботи якої досить близько наближається до потенційно досяжної.

Для побудови моделі потрібні:

1) Безліч можливих рішень, які можуть бути прийняті системою керування на підставі результатів розпізнавання невідомих об'єктів або явищ L = {l1, ..., lk).

2) Апріорний словник ознак xa = {x1 ..., xN}.

3) Вихідна множина об'єктів Ω = {w1 ..., wz}.

4) Розмір ресурсів C0, асигнованих побудова вимірювальної апаратури системи.

5) Значення виграшів, одержуваних системою управління від конкретних рішень з безлічі можливих рішень L= {l1 ..., lk}, що приймаються за результатами розв'язання задачі розпізнавання, тобто величин G(ΩAαi), i=1, ... m; α=1, ..., r.

2.3 Технологія Blockchain – як інструмент захисту ідентичності

Зараз, коли мільярди пристроїв IoT генерують половину всіх нових даних по всьому світу, є необхідність критично оцінювати цілісність та

безпеку даних. Якщо IoT – це технологія, що генерує дані, блокчейн буде тією технологією, яка гарантує довіру до них.

Блокчейн — це розподілена база даних, яка використовується спільно між вузлами комп'ютерної мережі. Відрізняється від типової бази даних способом зберігання інформації, а саме способом структурування даних.

Мета блокчейну — дозволити записувати та поширювати цифрову інформацію, але не редагувати. Таким чином, блокчейн є основою для незмінних реєстрів або записів транзакцій, які не можна змінити, видалити або знищити. Ось чому блокчейн також відомий як технологія розподіленої книги (DLT).

IoT потребує блокчейну для розвитку[15]. Навіть стандартні речі, такі як ідентифікація всіх пристроїв у мережі та знання того, що пристрій було зламано, явно відсутні у більшості систем IoT. Це робить пристрої IoT та дані надзвичайно вразливими для атак.

Використання блокчейн вирішує ці проблеми. Будучи децентралізованою, відстежуваною та стійкою до злому структурою даних, блокчейн виступає як «фабрика довіри» для автентифікації пристроїв та забезпечення безпеки[16].

Вплив блокчейну проявляється протягом усього життєвого циклу даних IoT:

1) Реєстрація пристроїв у блокчейні.

2) Відстежуваність даних від периферійного пристрою до шлюзу в блокчейн.

3) Безпечна обробка та передача даних.

Технологія блокчейн була вперше описана в 1991 році Стюартом Хабером і В. Скоттом Сторнеттою, двома математиками, які хотіли реалізувати систему, де не можна було б підробити часові позначки документів. Але лише у 2009 році концепція блокчейну отримала своє перше широке застосування у вигляді біткойну. З тих пір використання блокчейну різко розширилося через створення різних криптовалют, програм

децентралізованого фінансування (DeFi), незмінних токенів (NFT) і смарт-контрактів.

На даний момент ця технологія здебільшого використовується для майнінгу (видобування) цифрових валют. Різні типи інформації можуть зберігатися в блокчейні, але найпоширенішим досі було використання в якості книги для транзакцій.

Крім видобутку віртуальних монет, існує безліч варіантів використання блокчейна. Блокчейн вже намагаються використовувати для зберігання та обробки персональних даних та ідентифікації, у маркетингу та комп'ютерних іграх. Наразі існують десятки тисяч проектів, які намагаються впровадити блокчейни різними способами, щоб допомогти суспільству, крім простого запису транзакцій. Наприклад, використовувати блокчейни як спосіб безпечного голосування на демократичних виборах, інвентаризації товарів, державних ідентифікаційних документів, документів на житло та багато іншого.

Кількість живих блокчейнів зростає з кожним днем і постійно зростаючими темпами. Станом на 2021 рік існує понад 10 000 активних криптовалют, заснованих на блокчейні, і ще кілька сотень некриптовалютних блокчейнів. У бік Blockchain дивляться великі IT-гравці. Слідом за Microsoft і IBM компанія Oracle оголосила в жовтні про новий хмарний сервіс, заснований на блокчейні[17]. У Японії, Азії та на Близькому Сході банки активно впроваджують блокчейн. Технологію оцінили і в Україні. Під час економічного форуму в Давосі Blockchain Research Institute – організація, яка проводить дослідження у сфері блокчейну, представила світову карту технології. На ній зазначено 14 країн включно з Україною, які стали лідерами із застосування Blockchain.

Блокчейн збирає інформацію разом у групи, відомі як «блоки», які містять набори інформації. Блоки мають певну ємність для зберігання і, коли заповнюються, закриваються і пов’язуються з раніше заповненим блоком, утворюючи ланцюжок даних, відомий як «блокчейн».

Вся інформація в базі не належить комусь одному, але кожен користувач має свій індивідуальний ключ до свого блоку даних. Щоб видалити всі дані, потрібно отримати одночасно доступ до всіх комп'ютерів одночасно.

Блоки утворюють ланцюжок даних у міру того, як ресурс переміщається з одного місця до іншого або змінює власників. Блоки підтверджують точний час та порядок виконання транзакцій. Крім того, блоки нерозривно зчеплені один з одним, що виключає можливість зміни блоку або вставки між двома іншими блоками.

Кожен новий блок вважається додатковим підтвердженням справжності попереднього блоку та блокчейну в цілому. Таким чином блокчейн захищений від несанкціонованих змін, і в цьому полягає одна з його головних переваг — незмінність. Оскільки можливість злому з боку зловмисників виключена, створюється надійний реєстр транзакцій, якому учасники мережі можуть довіряти. Кожен блок містить свій власний хеш, а також хеш блоку перед ним, а також позначку часу. Хеш-коди створюються математичною функцією, яка перетворює цифрову інформацію в рядок цифр і букв. Якщо цю інформацію будь-яким чином редагувати, хеш-код також змінюється.

Процес шифрування (хешування) виконується на величезній кількості різних комп'ютерів. Коли результат обчислень на всіх комп'ютерах виходить однаковий, процес вважається завершеним, а сформованому блоку присвоюється цифровий підпис.

Скажімо, зловмистники, який також керує вузлом у мережі блокчейн, хоче змінити блокчейн і вкрасти криптовалюту у всіх інших. Якби вони змінили свою власну єдину копію, вона більше не відповідала б копіям усіх інших. Коли всі інші перехресно посилатимуть свої копії один на одного, вони побачать, що ця копія виділяється, і ця нова версія ланцюга буде відкинута як нелегітимна.

Щоб досягти успіху з таким зломом, зловмистникам потрібно одночасно контролювати та змінювати 51% або більше копій блокчейну, щоб їх нова копія стала основною копією і, таким чином, узгодженим ланцюгом. Для такої атаки також знадобиться величезна кількість грошей та ресурсів, оскільки їм потрібно буде переробити всі блоки, оскільки тепер вони будуть мати інші позначки часу та хеш-коди.

Через розмір багатьох криптовалютних мереж і те, наскільки швидко вони ростуть, витрати на здійснення такого подвигу, ймовірно, були б нездоланними. Це було б не тільки надзвичайно дорого, але й, ймовірно, було б марним. Таке виконання не залишиться непоміченим, оскільки учасники мережі побачать такі кардинальні зміни в блокчейні. Це призведе до того, що вартість атакованої версії токена різко впаде, що в кінцевому підсумку зробить атаку безглуздою.

Мережі блокчейн можуть відрізнятися тим, хто може брати участь і хто має доступ до даних. Мережі зазвичай позначаються як публічні або приватні, що описує, кому дозволено брати участь, і дозволені чи без дозволу, що описує, як учасники отримують доступ до мережі. Існує кілька підходів до створення блокчейн-мережі (див. таб. 2.1)[18].

Таблиця 2.1 – Типи блокчейн-мереж

Назва	Опис
Ексклюзивні блокчейн-мережі	В ексклюзивних блокчейн-мережах накладаються певні обмеження на коло осіб, яким дозволено брати участь у мережі чи лише окремих транзакціях. Учасникам необхідно отримати запрошення чи дозвіл на приєднання. Використовуються зазвичай приватних мережах, але також можуть в загальнодоступних.
Блокчейн-консорціум	Відповідальність за адміністрування блокчейну може лежати на кількох організаціях. Ці заздалегідь обрані організації встановлюють права доступу до транзакцій чи доступу до даних. Блокчейн-консорціум є ідеальним рішенням для компаній, коли всі учасники мають дозволи та несуть колективну відповідальність за блокчейн.

Продовження таблиці 2.1 – Типи блокчейн-мереж

Назва	Опис
Загальнодоступні блокчейн-мережі	До загальнодоступної блокчейн-мережі може приєднатися будь-який користувач. До недоліків такої мережі належать високі вимоги до обчислювальної потужності, низький рівень конфіденційності транзакцій та слабкий захист. Це критерії важливі при використанні блокчейну в корпоративних середовищах.
Приватні блокчейн-мережі	Приватна блокчейн-мережа, як і загальнодоступна блокчейн-мережа, представляє з себе децентралізовану одноранговую мережу. Однак управління такою мережею здійснюється однією організацією, яка відповідає за управління учасниками, виконання протоколу консенсусу та підтримку загального реєстру. Залежно від сценарію використання такий підхід дозволяє істотно підвищити достовірність і надійність інформації, що передається між учасниками. Приватна блокчейн-мережа може перебувати за корпоративним брандмауером або навіть у локальному середовищі.

При всій своїй складності потенціал блокчейну, як децентралізованої форми ведення записів майже безмежний. Від більшої конфіденційності користувачів і підвищеної безпеки до нижчої плати за обробку та меншої кількості помилок.

Серед плюсів технології:

1) Підвищена точність за рахунок виключення участі людини в перевірці. Транзакції в мережі блокчейн схвалюються мережею з тисяч комп'ютерів. Це усуває майже всю людську участь у процесі перевірки, що призводить до менших людських помилок і точного запису інформації. Навіть якби комп'ютер у мережі зробив обчислювальну помилку, помилка була б зроблена лише в одній копії блокчейну. Щоб ця помилка поширилася на решту блокчейну, її мають зробити щонайменше 51% комп'ютерів мережі — майже неможливо для великої та зростаючої мережі розміром з біткойн.

2) Зменшення витрат завдяки виключенню сторонньої перевірки. Як правило, споживачі платять банку за перевірку транзакції, нотаріусу за підписання документа або міністру за укладення шлюбу. Блокчейн усуває потребу в перевірці третьої сторони, а разом з нею — і пов'язаних з ними витрат. Наприклад, власники бізнесу несуть невелику комісію, коли вони приймають платежі за допомогою кредитних карток, оскільки банки та компанії з обробки платежів повинні обробляти ці транзакції. З іншого боку, біткойн не має центрального органу влади і має обмежену комісію за транзакції.

3) Децентралізація ускладнює втручання. Блокчейн не зберігає свою інформацію в центрі. Замість цього блокчейн копіюється і поширюється по мережі комп'ютерів. Щоразу, коли до блокчейну додається новий блок, кожен комп'ютер у мережі оновлює свій блокчейн, щоб відобразити зміни. Поширюючи цю інформацію по мережі, а не зберігаючи її в одній центральній базі даних, блокчейн стає важче підробити. Якщо копія

блокчейну потрапить до рук хакера, буде скомпрометована лише одна копія інформації, а не вся мережа.

4) Трансакції є безпечними, приватними та ефективними.

– ефективні транзакції. Блокчейн працює 24 години на добу, сім днів на тиждень і 365 днів на рік. Трансакції можуть бути завершені всього за десять хвилин і можуть вважатися безпечними вже через кілька годин. Це особливо корисно для транскордонних торгів, які зазвичай займають набагато більше часу через проблеми з часовим поясом і той факт, що всі сторони повинні підтвердити обробку платежу.

– приватні транзакції. Багато мереж блокчейн працюють як загальнодоступні бази даних, а це означає, що будь-хто, хто має підключення до Інтернету, може переглянути список історії транзакцій мережі. Хоча користувачі можуть отримати доступ до інформації про транзакції, вони не можуть отримати доступ до ідентифікаційної інформації про користувачів, які здійснюють ці транзакції. Якщо людина здійснила покупку біткойн на біржі, яка вимагає ідентифікації, то особистість особи все ще пов’язана з її адресою в блокчейні, але транзакція, навіть якщо вона прив’язана до імені людини, не розкриває жодної особистої інформації.

– безпечні транзакції. Після запису транзакції її автентичність повинна бути перевірена мережею блокчейн. Тисячі комп’ютерів на блокчейні поспішають підтвердити, що деталі покупки правильні. Після того, як комп’ютер підтвердив транзакцію, вона додається до блокчейну. Кожен блок в блокчейні містить свій унікальний хеш разом з унікальним хешем блоку перед ним. Коли інформація про блок редагується будь-яким чином, хеш-код цього блоку змінюється, але хеш-код у

блоці після нього не змінюється. Ця невідповідність надзвичайно ускладнює зміну інформації про блокчейн без попередження.

5) Прозора технологія. Більшість блокчейнів є програмним забезпеченням з відкритим вихідним кодом. Це означає, що кожен може переглянути його код. Це дає аудиторам можливість переглядати криптовалюти, такі як біткойн, на предмет безпеки. Це також означає, що немає реальних повноважень щодо того, хто контролює код Bitcoin або як він редагується. Через це будь-хто може запропонувати зміни або оновлення системи. Якщо більшість користувачів мережі згодні з тим, що нова версія коду з оновленням є надійною та гідною, тоді біткойн можна оновити.

Серед мінусів технології:

- значна вартість технології, пов'язана з майнінгом криптовалют;
- низька кількість транзакцій в секунду;
- приклади використання в незаконній діяльності;
- регулювання залежить від юрисдикції і залишається невизначеним;
- обмеження зберігання даних.

Оскільки багато практичних застосувань для цієї технології вже впроваджуються та досліджуються, блокчейн нарешті робить собі ім’я, багато в чому завдяки біткойн та криптовалюті.

Інтернет речей (IoT) став одним із найбільш перспективних варіантів використання блокчейну. Є низка сфер застосування, де блокчейн може підтримувати зростання та розвиток IoT. Серед них: протидія шахрайству, керування ідентифікацією, проведення транзакцій, верифікація стану елементів різних систем, забезпечення цілісності даних тощо. Однією із основних областей застосування блокчейну в IoT стануть ідентифікація пристроїв та забезпечення цілісності даних.

Однією з багатьох компаній, яка займається даною сферою є Factom. Ця компанія створює рішення на базі блокчейну, що дозволяють організаціям захистити найважливішу інформацію. Рішення, що

розробляються компанією на базі блокчейну, відкривають широкі можливості для прозорого аудиту бізнес-процесів та фінансових послуг, реєстрації прав власності, забезпечення цілісності, достовірності медичних записів та займається розробкою рішень щодо забезпечення безпеки цифрової ідентифікації у додатках Інтернету речей (IoT).

2.4 Технологія eSim

При покупці нового смартфону новий власник, насамперед вставляє у нього SIM-карту, саме вона дозволяє повною мірою користуватися спектром послуг, що надаються мобільним оператором.

Абревіатура SIM (Subscriber Identity Module) розшифровується як модуль ідентифікації абонента[19]. Завдяки появі цього стандарту вперше розділилася ідентифікація абонента та апарату - так, як перші мобільні телефони зовсім не мали ніяких карт: їх програмував оператор і потім номер зберігався у внутрішній пам'яті пристрою.

Саме в 1991 році з появою мереж 2G вирішили вводити сім-карти, які дозволили б використовувати свій телефон в мережі будь-якого оператора, а свій «облік» (тобто сам номер) залишати з собою, спокійно змінюючи пристрої. Перші сім-картки були розміром майже з банківську карту (див. рис. 2.3), але так як з часом телефони і модеми ставали все компактнішими, то і сімки зменшувалися разом з ними.

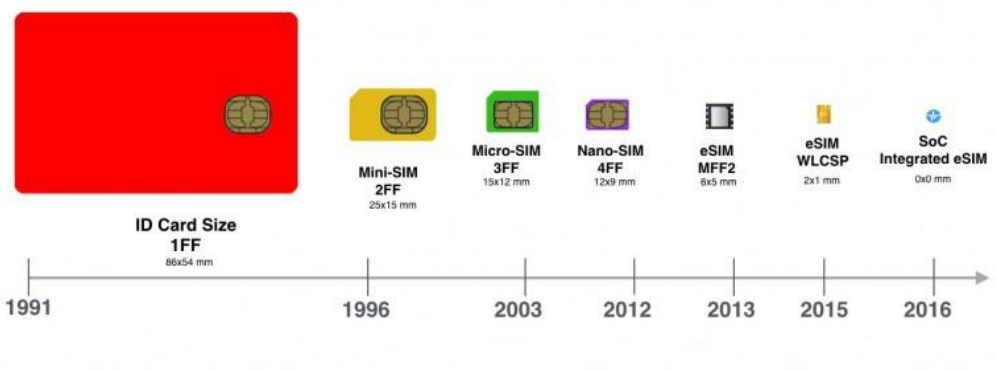


Рисунок 2.3 - Історія eSim

Вперше зменшення сім-карти розміром з банківську картку (85×54 мм) зменшили до формату mini SIM (25×15 мм) у 1996 році. Цей стандарт використовувався на ринку довгий час, але його поступово витісняли Micro SIM та Nano SIM.

Здебільшого нові формати SIM-карток з'явилися завдяки компанії Apple. Сім-карта формату Micro SIM (15×12 мм) вперше була встановлена в iPhone 4 у 2010 році, а через два роки з'явився формат nano SIM (12,3×8,8 мм), який використовувався в iPhone 5. На сьогоднішній день формат Nano SIM є світовим стандартом та використовується в більшості сучасних пристроїв.

Приблизно в цей же час, коли було прийнято рішення вводити SIM-картки, почався перший сплеск буму «інтернету-речей»: і якщо в той же холодильник чи котел можна було вставити SIM-карту, то зі смарт-годинами і подібною дрібною технікою цього не виходило. Тому виробники вигадали вбудовану SIM-карту eSim: і якщо 35 років тому подібні чіпи були прив'язані лише до одного оператора, то зараз їх можна міняти по клацанню пальця. Сьогоднішні вбудовані SIM-карти підтримують віддалене завантаження: це суттєво економить час та гроші для тих, хто використовує розумні пристрої у великих кількостях для бізнесу.

Очікується, що в найближчому майбутньому SIM-картки замінять технологією eSIM (embedded SIM) - це стандарт, розроблений асоціацією GSMA, який дозволяє зберігати кілька профілів операторів зв'язку на одному інтегрованому електронному пристрої (чіпі) та дозволяє підключати пристрої до стільникового зв'язку без фізичних SIM-карток[20]. При цьому абонентські профілі конкретних операторів зв'язку можуть завантажуватись у eSIM через мережу (Інтернет). eSIM походить від англійського слова “embedded SIM”, що означає “інтегрована SIM”. Впровадження стандарту eSIM спрощує процес підключення таких пристроїв, як планшети, смарт-годинник, фітнес-браслети, переносні системи охорони здоров'я та інші пристрої до мережі.

Дані пакета певного оператора вносяться до гаджету через спеціальний QR-код. При цьому важливо, щоб і пристрій, і мобільний постачальник підтримували функцію eSIM. Налаштування параметрів зв'язку здійснюється онлайн. Як і у випадку з класичною сім-картою, дані eSIM (номери, PIN-коди та тарифні плани) можна перенести на інший гаджет, якщо, наприклад, користувач змінює телефон. Але для цього знадобляться нові QR-коди.

Якщо ви видалили обліковий запис eSIM з пристрою, його можна відновити, ввівши QR-код, виданий користувачеві раніше. Процедуру з тим самим гаджетом і QR-кодом можна здійснити не більше 10 разів. eSIM в Україні та інших країнах може працювати як у зв'язку з фізичною сім-карткою, так і самостійно.

Відмова від SIM-карт на користь інтегрованих чіпів суттєво полегшить налаштування телефону, допоможе за лічені хвилини змінити оператора та швидко знайти втрачений гаджет.

Серед переваг технології eSIM[21]:

1) eSIM спрощує процес зміни оператора мобільного зв'язку. Сьогодні для зміни оператора потрібно йти до салону зв'язку, купувати стартовий пакет та вибирати тариф. eSIM дає змогу придбати потрібний тариф, використовуючи програмне забезпечення. Таку можливість насамперед оцінять ті, хто часто буває за кордоном і завжди хоче залишатися на зв'язку з близькими. Не доведеться шукати магазин, де купити сім-карту, достатньо просто поміняти налаштування у смартфоні.

2) Більше не буде проблем через неправильно вставлену сім-карту. Деякі власники сучасних гаджетів не завжди правильно вставляють SIM-карту в пристрій, така необережність призводить до того, що карта псується. З появою eSIM таких проблем не буде.

3) Більш ефективний захист смартфона та іншої техніки від крадіжки. У разі крадіжки грабіжник не зможе викинути сім-карту, тому приховати місцезнаходження теж не вийде. Більше того, щоб внести дані нового eSIM-акаунта, йому знадобиться ввести пароль видаленого облікового запису.

4) Нові гаджети стануть тоншими. За рахунок економії простору майбутні планшети, смартфони та інші гаджети стануть тоншими. Надалі можна буде відмовитися від лотка для сім-карти, відповідно, зменшиться кількість місць, куди може просочитися вода або проникнути пил - гаджети стануть ще герметичнішими. Також eSIM легше переносить удари, протистоїть вібраціям, пилу, на відміну від звичайних сім-карток.

5) На одній картці можна зберігати до 5 віртуальних номерів одночасно, що дуже сподобається людям, яким за обов'язком служби потрібно мати кілька номерів;

6) Можливість активувати eSIM-профіль на кількох пристроях одночасно, наприклад, на смартфоні та робочому планшеті. Це дозволяє завжди бути на зв'язку, незалежно від того, який гаджет використовується в конкретний момент. Головне, знати, які телефони підтримують eSIM і на яких ще девайсах вона доступна.

7) eSim дозволяє віддалено налаштувати будь-який пристрій. Наприклад, якщо ви їдете на довгий час в іншу країну, то можете укласти контракт з одним із місцевих операторів і почати користуватися новим номером, перебуваючи вдома.

До основних недоліків eSim можна зарахувати:

1) Неможливість поставити таку SIM-картку в будь-який телефон: новий гаджет також має підтримувати цю технологію. При цьому, близько години ви перебуватимете поза мережею, оскільки оператору потрібен час, щоб перенести номер на інший пристрій.

2) Поки що eSim використовується далеко не скрізь. Станом на початок 2020 року технологію підтримують лише кілька топових флагманів: до повного впровадження технології у звичайне життя пройде ще мінімум 3-5 років.

Архітектура системи віддаленого програмування інтегрованого пристрою (чіпа) та внутрішня високорівнева архітектура інтегрованого

пристрою embedded універсальний integrated circuit card (eUICC)[22], на базі якого реалізує функціонал стандарту eSIM (див. рис. 2.4 – 2.5).

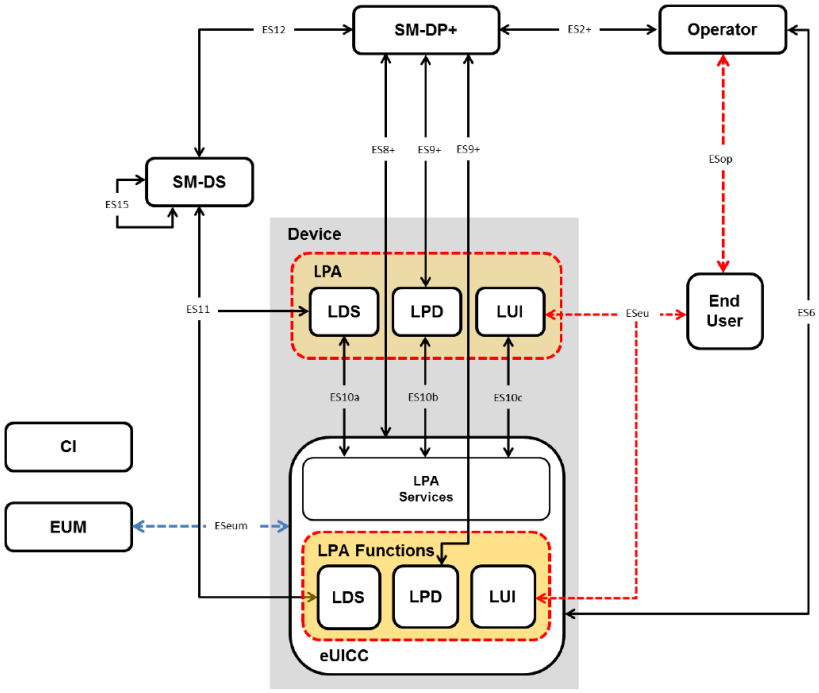


Рисунок 2.4 - Архітектура стандарту eSIM та його інтерфейси взаємодії

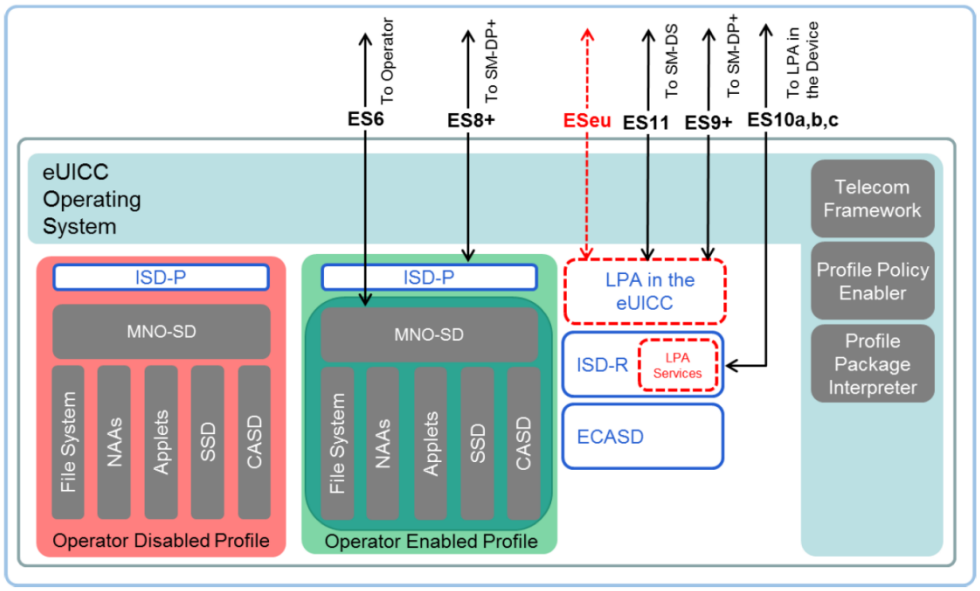


Рисунок 2.5 - Архітектура інтегрованого електронного пристрою eUICC

Опис основних елементів архітектури. ECASD (англ. Embedded UICC Controlling Authority Security Domain) – інтегрований домен безпеки eUICC.

ECASD відповідає за безпечне зберігання облікових даних, необхідних для забезпечення необхідного рівня безпеки.

Лише один елемент ECASD може існувати на eUICC. ECASD має бути встановлений та персоналізований виробником eUICC.

ECASD повинен містити таку інформацію:

– закриті ключі eUICC для створення електронних підписів;

– пов'язані з eUICC сертифікати безпеки для її автентифікації;

– кореневі публічні ключі для перевірки сертифікатів безпеки елементів SM-DP+ та SM-DS;

– набір секретних ключів виробника eUICC, необхідних для оновлення ключів/сертифікатів.

Крім того, ECASD відповідає за аутентифікацію eUICC з використанням необхідних ключів безпеки.

ISD-R (англ. Issuer Security Domain – Root) – кореневий домен безпеки. ISD-R відповідає за створення нових та керування життєвим циклом доменів безпеки профілів (ISD-P).

ISD-P (англ. Issuer Security Domain – Profile) – домен безпеки профілю. ISD-P забезпечує завантаження, встановлення та зберігання профілів SIM карт. ISD-P – це подання даних SM-DP+ на чіпі.

MNO-SD (англ. Mobile Network Operator - Security Domain) - подання даних оператора зв'язку. MNO-SD містить ключі OTA і забезпечує безпековий канал обміну даних через OTA.

Profile Policy Enabler – сервіс операційної системи eUICC, що виконує перевірку та застосування політик безпеки.

Telecom Framework – сервіс операційної системи eUICC, який забезпечує роботу алгоритмів автентифікації, які розміщені на ISD-Ps. Додатково сервіс пропонує конфігурувати алгоритми необхідними параметрами.

Profile Package Interpreter – сервіс операційної системи eUICC, який перетворює отримані дані профілю у внутрішній формат eUICC.

LPA Services (Local Profile Assistant Services) - локальні сервіси, що реалізують доступ до даних, необхідних LPA функцій, для:

- отримання кореневої адреси SM-DS;
- отримання адреси SM-DP+, що опціонально зберігається;
- спрощення прийому профілю SIM під час передачі від LPA;
- отримання інформації про встановлений профіль;
- забезпечення управління профілями;
- забезпечення функціоналу аутентифікації та взаємодії з SM-DS;
- забезпечення доступу до ідентифікатора eUICC (EID) лише з LPA.

LPA включає три функції:

1) Local Discovery Service (LDS) – відповідає за отримання відкладених подій від SM-DS

2) Local Profile Download (LPD) – виконує роль посередника для більш ефективного завантаження пакета профілю із SM-DP+.

3) Local User Interface (LUI) – дозволяє кінцевому користувачеві керувати профілями на пристрої.

Передбачено два режими роботи LPA. Перший: LPA функції надаються пристроєм, другий: LPA функції надаються eUICC.

SM-DP+ (англ. Subscription Manager Data Preparation +) – елемент архітектури стандарту eSIM, який відповідає за створення, керування та захист профілів SIM на підставі запиту Оператора зв'язку. Він також відповідає за доставку профілю та запит ISD-P у створенні профілю на eUICC. SM-DP+ також керуватиме життєвим циклом профілю ISD-P, який був створений на його запит.

SM-DS (англ. Subscription Manager - Discovery Service) - сервер виявлення, що реалізує механізм, який дозволяє SM-DP+ інформувати LDS будь-якого пристрою про те, що SM-DP+ хоче встановити з ним зв'язок.

CI (англ. Certificate Issuer) – центр сертифікації, що здійснює випуск сертифікатів для аутентифікації об'єктів стистеми.

EUM (англ. eUICC Manufacturer) – виробник електронних чіпів eUICC.

Одним із основних завдань стандарту eSIM є організація процедури безпечного завантаження профілю в чіп eSIM. Верхньорівнева процедура виглядає так:

1) Виробник абонентських пристроїв виготовляє гаджет із вбудованим eSIM модулем. На eSIM мають бути записані у т.ч. адреса кореневого сервера виявлення (SM-DS), ідентифікатор модуля (EID - eUICC-ID) та сертифікати безпеки.

2) Користувач купує гаджет із встановленим модулем eSIM та укладає договір з оператором на надання послуг мобільного зв'язку.

3) Оператор зв'язку створює на SM-DP+ абонентський профіль та прив'язує його до сертифікатів безпеки eSIM модуля, встановленого у гаджеті клієнта. Абонентський профіль містить у т.ч. міжнародний ідентифікатор мобільного користувача (IMSI), параметри алгоритму автентифікації та особисті ключі (OP, OPc, KI), коди захисту PIN, PUK.

4) Оператор створює абонентський профіль у мережевих базах даних та платформах - HLR/HSS, BSS,...

5) Далі в рамках процедури виявлення SM-DP+ завантажує абонентський профіль до eSIM.

У 2012 перша версія eSIM була вмонтована в автомобілі як функцію екстреного дзвінка (eCall) у разі аварії. У смартфонах, планшетах та інших гаджетах технологію почали застосовувати у 2016-2017 роках. Першопрохідником, який вдало впроваджує eSIM у свої гаджети, була південнокорейська компанія Samsung, яка представила в 2016 році smart-вотч Gear S2 Classic 3G. Крім цього і далі продовжує активно впроваджувати нову технологію з їхніми Galaxy Fold, S20, S20+, S20 Ultra, Z Flip.

Слідом пішла і компанія Google, реалізувавши eSIM у телефонах Pixel 2/2 XL та Pixel 3/3 XL, але з невеликою умовою: технологія реалізується

через спеціальну службу Google Fi (віртуальний оператор мобільного зв'язку). Станом на початок березня 2020 року, цю технологію підтримують Pixel 2 і 2 XL, 3, 3A XL, 3 XL і 4, 4 XL.

Також eSIM підтримується в смарт-годинниках Huawei Watch 2 та планшеті-трансформаторі Microsoft Surface Pro 5-го покоління. Віртуальні SIM-карти також сподобалися Motorola, тому ми всі можемо побачити eSim в її новому смартфоні Motorolla Razr, що «згинається».

Активним просуванням технології eSIM у маси займається компанія Apple. Яблучна корпорація створила фірмовий сервіс Apple SIM, який є сім-картою, незалежною від мобільних операторів. Він може змінювати мобільного оператора та тарифний план через налаштування пристрою. Спершу для таких сімок використовувався стандартний слот, але через деякий час випустили iPad з технологією Apple SIM, а в смарт-годиннику Apple Watch третього покоління була вперше використана технологія eSIM.
Сьогодні, eSim є у таких моделях:

- iPhone Xs, Xs Max, Xr (iOS 12.1 та вище);
- iPhone 11, 11 Pro, 11 Pro Max;
- iPad 2019, iPad Pro 11 та 12,9, iPad Air 2019, iPad Mini 5;
- Apple Watch з підтримкою LTE.

Сьогодні eSIM активно запроваджують за кордоном оператори Verizon, T-Mobile, Truphone. Останній пропонує тарифні плани у 80 країнах. Технологію Україна почала вводити наприкінці 2019 року. Першим оператором, який пропонує електронну сім-карту, став «ТріМоб». За тиждень про впровадження послуги оголосив провайдер lifecell.

3 РОЗРОБКА МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ МЕРЕЖІ

3.1 Функціональні характеристики мережі

Концепція розумних міст випливає з необхідності вирішення кількох проблем, спричинених нестримним зростанням населення в міських центрах, які безпосередньо впливають на декілька послуг, таких як транспорт, безпека, водо- та електро- постачання/споживання, санітарія, використання природних ресурсів, управління катастрофами.

У спрощеному розумінні, керівництво кожної служби пропонує постійний моніторинг, оснащений механізмами збору даних. Ці дані необхідно обробляти та аналізувати, повертаючи у відповідь певні дії для забезпечення надання послуг на задовільному рівні якості та ефективності. З більш складної точки зору, розповсюдження та інтеграція необхідні, як від контролюваних елементів, так і від застосування необхідних дій; дані повинні бути пов'язані, а обробка й аналіз повинні враховувати існуючий вплив зовнішніх агентів та інших служб.

Складне уявлення про програму керування послугами - розподілене та інтегроване - вимагає масового використання певного роду датчиків у цільових об'єктах. Саме з цього унітарного механізму моніторингу будується цілісне уявлення про місто, спрямоване на ефективне обслуговування його послуг з метою покращення якості пропонованих послуг.

Багато проблем, з якими сьогодні стикаються великі міста, можна уникнути або навіть пом'якшити, якщо застосувати бачення «розумних міст» до управління послугами, використовуючи інформаційно-комунікаційні технології. Серед таких послуг:

Безпека – ця сервіс виконується різноманітними приватними комунікаціями, відеоспостереженням, і виконує функції командування та диспетчеризації для всіх видів державних і приватних об'єктів, від урядових

служб та служб екстреної допомоги до енергетичних управлінь та медичних працівників.

(Водо- /газо-) постачання - розумні системи водо- та газопостачання, як і розумні енергетичні системи, використовують датчики з підтримкою IoT для збору даних у реальному часі. Це дозволяє оптимізувати об’єкти, виявляючи витоки або відстежуючи, як вода або газ розподіляється по мережі, і дозволяє людям приймати більш обґрунтовані рішення щодо управління ресурсами. Наприклад, ці розумні датчики можуть виявляти витік у трубах і негайно сповіщати інженерів про вжиття заходів та пом’якшення наслідків.

Забруднення повітря спрямоване на моніторинг рівня забруднення, особливо рівнів у містах, за допомогою кількох пристроїв IoT та підключених датчиків. Ідея передбачає розміщення кількох станцій у кількох районах міст. Ці станції періодично завантажують та надсилають дані в хмару IoT. Зв'язок між пристроями здійснюється через глобальну мережу великого радіусу дії (LoRaWAN). Друга версія рішення має на меті використовувати мережу IoT-NB 5G GSM (NarowBand IoT) у гібридному підході з Wi-Fi, SigFox і LoRaWAN і підвищити безпеку за допомогою елемента захисту Java Card в межах промислового шлюзу IoT.

Менеджмент відходів Сучасні смітники оснащені датчиками для визначення рівня їх заповнення, а шлюзи додатків пов’язують платформи IoT. Вони також мають датчики, які надсилають дані зі сміттєвих контейнерів на сервери в хмарі. Платформи IoT обробляють необроблені дані в інформацію, яка може діяти. Такими датчиками можуть бути GPS, датчики руху, світла або вібрації, які відстежують фізичні зміни, температуру та зміни місця розташування.

Розумне освітлення вулиць Інтернет речей (IoT) насамперед забезпечує концепцію розумних вуличних ліхтарів, збираючи різні типи електронних даних з різних фізичних пристроїв за допомогою датчиків і надаючи інформацію на пристрої. Таким чином можна значно скоротити

витрати на вуличне освітлення, а заощаджену суму можна інвестувати в інший розвиток нації.

Системи керування трафіком у реальному часі керують поведінкою на дорогах у режимі реального часу, використовуючи мережу технологій, включаючи датчики, розумні камери, GPS та Bluetooth/Wi-Fi. Це можна використовувати, щоб ефективно зменшити затори, вузькі місця та інші проблеми з трафіком. Дані в режимі реального часу можна використовувати, щоб запропонувати водіям альтернативні маршрути, коли маршрути перевантажені, і вказати операторам громадського транспорту та особам, які приймають рішення, де знаходиться попит і пропозиція користувачів. Удосконалення технологій дозволило розробити складні послуги для управління мережами для вирішення суперечливих запитів усіх користувачів доріг і транспорту.

Розширені системи керування дорожнім рухом покращують якість та продуктивність дорожніх послуг, оскільки вони надають точні дані в режимі реального часу з багатьох джерел, таких як датчики, GPS, розумні камери, динамічні повідомлені знаки, світлофори та системи інформації про погоду. Без цієї інформації про трафік покращення мережі, інтеграція нових видів транспорту та розвиток інфраструктури не будуть придатними для поточних і майбутніх транспортних потреб (тобто не забезпечать гнучкості та адаптивності, необхідні від нової транспортної інфраструктури, щоб реагувати на мінливий попит).

Розумні послуги керування трафіком дозволяють інтегровано оптимізувати дорожні та транспортні мережі для відповідності попиту та пропозиції інфраструктури майже в режимі реального часу, керуючи швидкістю, частотою та пріоритетом транспортних засобів, дотримуючись правил та вимог безпеки.

Розумне паркування — це рішення для паркування, яке може включати в себе наземні датчики або камери виявлення/підрахунку Smart Parking. Ці пристрої зазвичай вбудовуються в місця для паркування або

розміщуються поруч з ними, щоб визначити, вільні місця для паркування чи зайняті. Це відбувається шляхом збору даних в режимі реального часу. Потім дані передаються на мобільний додаток або веб-сайт Smart Parking, який повідомляє про доступність своїм користувачам. Деякі компанії також пропонують іншу інформацію в додатку, як-от ціни та місця паркування.

Враховуючи зрівняння технічних характеристик технологій(див. рис. 3.1-3.2)[24] та їх специфікацій стає можливим сформулювати вимоги (див. табл. 3.1) необхідних інформаційним системам для забезпечення ідентифікації пристроям та забезпечення безперебійної роботи систем.

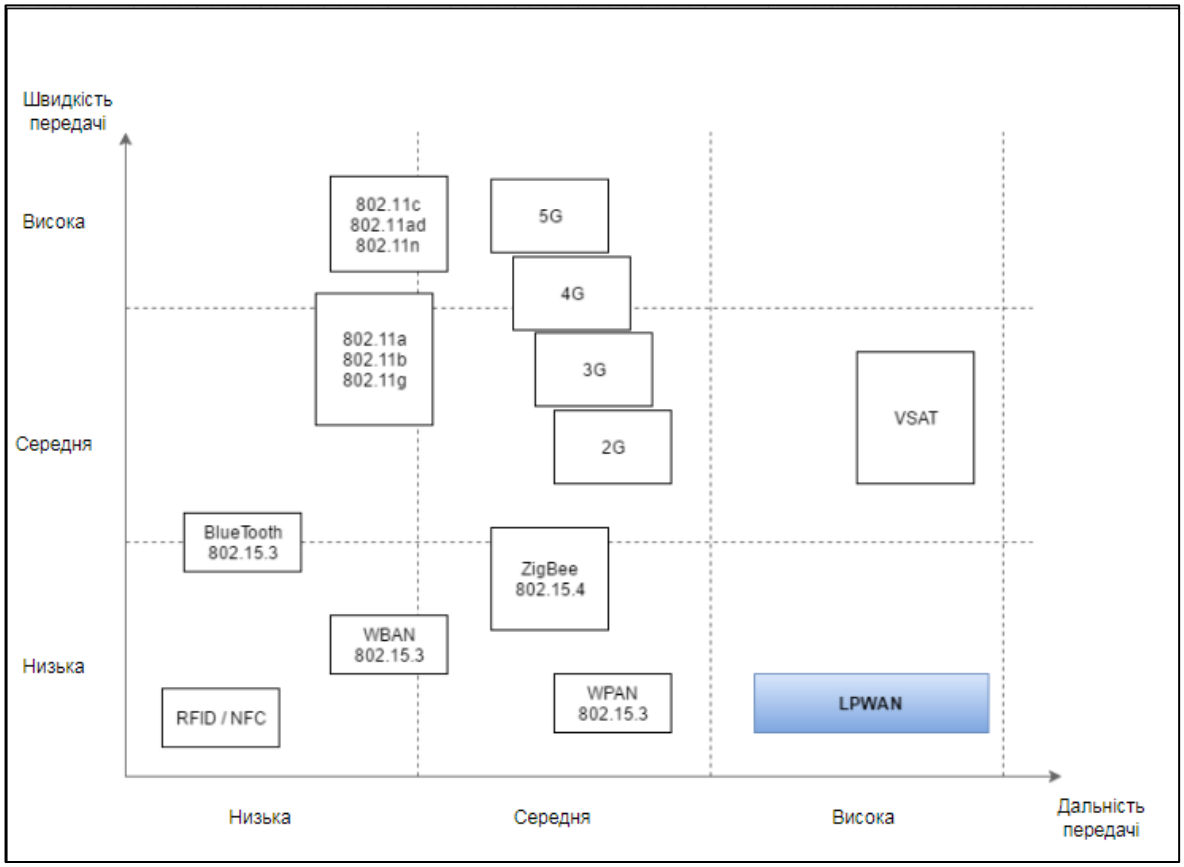


Рисунок 3.1- Порівняння технологій по швидкості та дальності

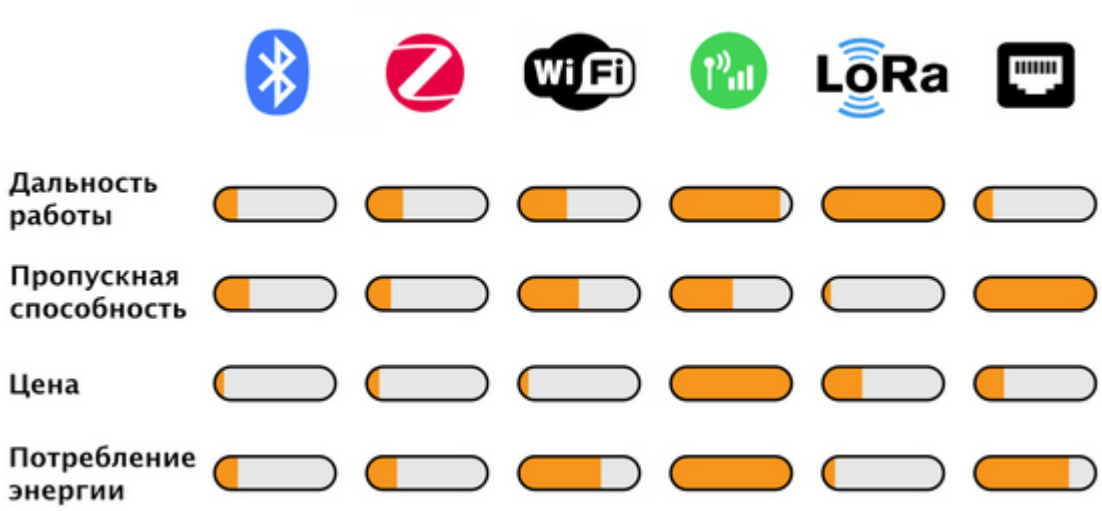


Рисунок 3.2- Порівняння технологій по ціні та енергоефективності

Таблиця 3.1 – Вимоги до систем ідентифікації та параметри забезпечення безперебійної роботи Smart City

№	Система «послуга»	Технологія ідентифікації	Параметри безперебійної роботи
1	Ідентифікація мережі, підмереж	Blockchain / IPv6	LoRaWAN
2	Транспорт (автономні автомобілі)	Blockchain / IPv6	LTE-V / DSRC
3	(Водо- /газо- /електро-) системи (Датчики, сенсори)	eSim, Blockchain	NB-IoT 5G, LoRaWAN

Продовження таблиці 3.1 – Вимоги до систем ідентифікації та параметри забезпечення безперебійної роботи Smart City

№	Система «послуга»	Технологія ідентифікації	Параметри безперебійної роботи
4	Забруднення повітря	eSim	IoT-NB 5G GSM у гібридному підході з Wi-Fi, SigFox і LoRaWAN
5	Менеджмент відходами	eSim,	LoRaWAN
6	Освітлення вулиць	eSim, Blockchain	LoRaWAN

3.2 Системи управління ідентифікації

Система управління відповідає за конфігурацію, оновлення програмного забезпечення та моніторинг роботи обладнання. При цьому можливості керувати об’єктами набагато менше в порівнянні з «класичним» пристроєм (маршрутизатором, комп'ютером, серверами ...) і мають свою специфіку. Також системи управління класифікуються на основі того скільки елементів цієї системи мають повноваження та можливості виконувати керуючу функцію. Серед видів систем управління є централізована, децентралізована та розподільна[24].

Централізовані системи. Усі центральні системи мають лише одну точку управління, якою здійснюється контроль за системою (див. рис. 3.3). Усі процеси проводяться лише у цій точці, у ній приймаються рішення. Тому

система дуже вразлива до збоїв, які можуть призвести до її обвалення: будь-який збій – і вся система обвалиться.

Особливості: єдина точка управління, усі процеси виконуються в одному місці, дуже чуттєве до збоїв.

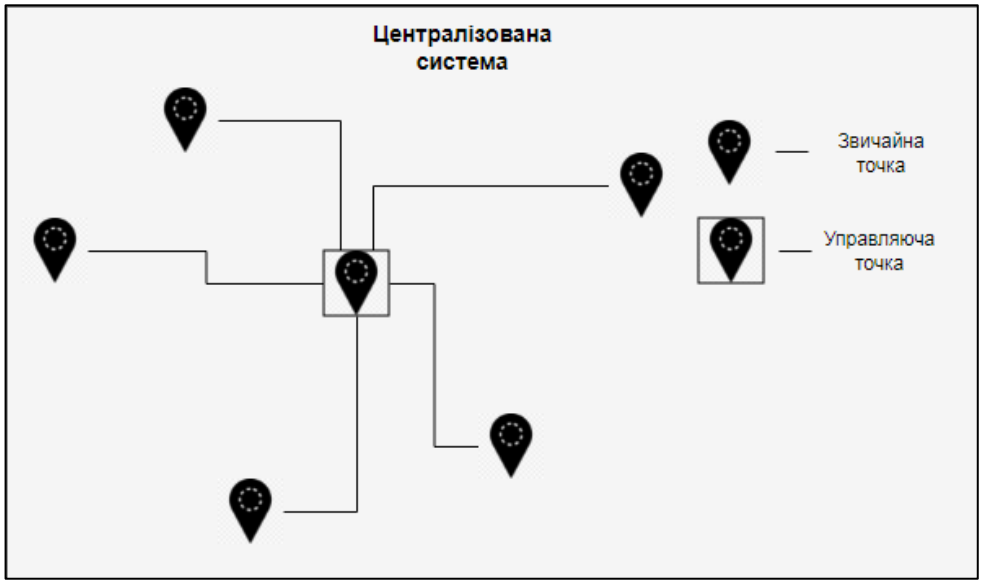


Рисунок 3.3 - Схема централізованої системи

Плюси використання централізованої системи:

1) Вона легко реалізується і всі рішення приймаються набагато швидше, аніж у інших системах управління. Оскільки в ній лише одна точка управління, в якій зосереджений весь контроль за системою.

2) Економія на масштабі позбавляє необхідності подвійної роботи, яка іноді робиться за наявності кількох точок управління. Так, як в системі тільки одна точка управління, то не потрібно змушувати безліч точок виконувати одні й самі функції, що і дає економію на масштабі.

Мінуси використання централізованої системи:

1) Залежність від однієї точки управління. Наявність лише однієї точки управління робить систему беззахисною, оскільки будь-яка атака на цю єдину точку управління дестабілізує всю систему.

2) Можлива необхідність у посередниках.

Децентралізовані системи – це системи, що мають кілька точок управління та повноваження диверсифіковані (див. рис. 3.4). Це дозволяє знизити ймовірність виникнення неполадок у роботі системи, оскільки вихід з ладу однієї точки управління не призводить до падіння всієї системи. У порівнянні з централізованою системою, ієрархія такої системи ближча до горизонтальної.

Особливості: Багато точок управління, менша схильність до падінь, більш горизонтальна ієрархія.

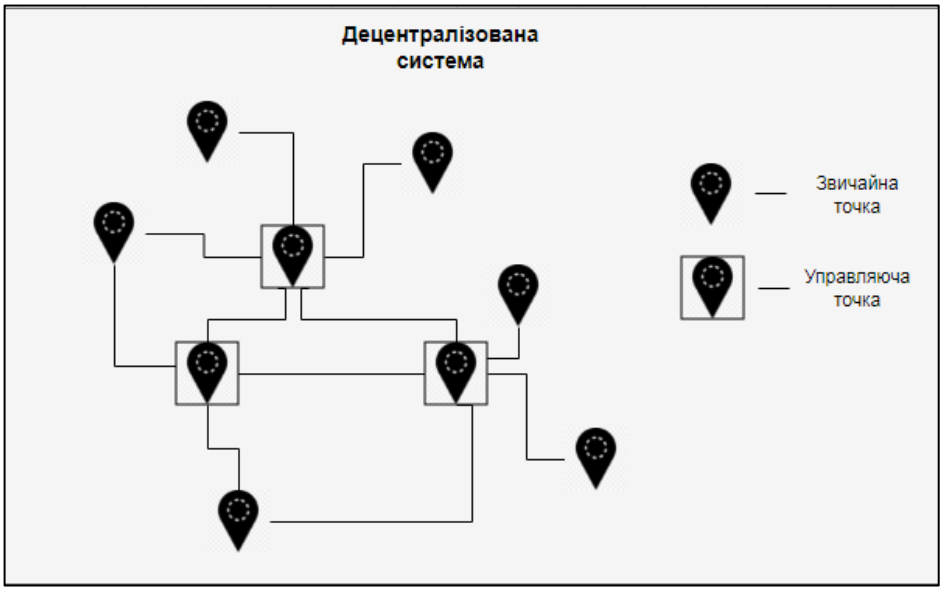


Рисунок 3.4 - Схема децентралізованої системи

Плюси використання децентралізованої системи:

1) Рішення в ній приймаються на рівні, більш наближеному до користувача. Таким чином у точок, що приймають рішення, набагато більше інформації про кінцевого користувача (якщо йдеться про продукт).

2) Ця система менше схильна до відмов і збоїв, оскільки тепер у ній кілька точок управління. Збій в одній точці не призведе до дестабілізації всієї системи, як у випадку з централізованою системою.

Мінуси використання децентралізованої системи:

1) Негативний економічний ефект, пов'язаний із збільшенням масштабів системи. У такій системі через збільшення кількості точок управління можна отримати проблему дублювання завдань.

2) Незважаючи на те, що децентралізовані системи надійніші за централізовані, вони все одно схильні до збоїв, тому їх не можна назвати повністю надійними.

Розподілені системи – це системи у яких будь-яка точка – є керуючою (див. рис. 3.5). Завдяки цьому такі системи майже повністю падіння стійкі, хоча це не означає, що вони є повністю захищені від зломів. Якщо узяти під контроль більше 50% точок управління, то систему можливо узяти під контроль або вивести із ладу. Але на це піде більшість прибутку і зробить економічно недоцільним таку діяльність.

Особливості: Усі ці системи мають горизонтальну ієрархію. Усі точки керування рівні одна одній, і будь-яка точка системи може бути точкою управління. Отже всі рівні, що призводить до горизонтальної ієрархії.

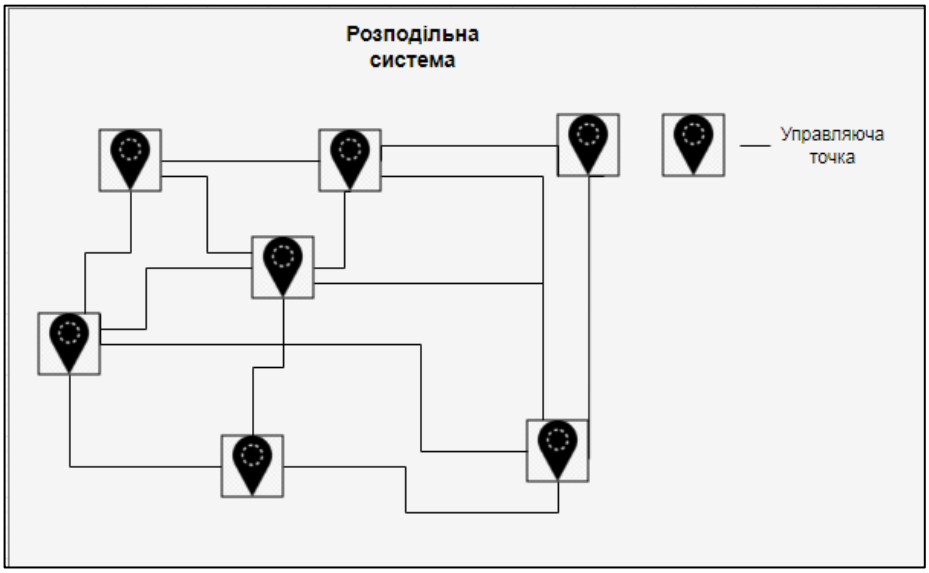


Рисунок 3.5 - Схема розподіленої системи

Плюси використання розподіленої системи:

1) Використання розподіленої системи усуває потребу у посередниках.

2) Зламування цих систем економічно недоцільно, що робить їх надзвичайно надійною та найбезпечнішою із трьох розглянутих систем.

Мінуси використання розподіленої системи:

1) Такі системи досі вважаються новими, та їх технології перебувають у процесі зародження.

2) Для стабілізації таких систем знадобиться багато часу та суттєві вкладення. Згодом вдасться заощадити на масштабі, але спочатку ці системи досить дорогі.

Системи, що самоорганізуються(self-organization system)[25]:

Ключовою особливістю систем, що самоорганізуються, є відсутність центрального контролю для координації дій компонентів у системі. Система часто розподілена в тому сенсі, що окремі компоненти діють як однорангові, а кожен компонент взаємодіє лише зі своїми сусідами. Ці взаємодії разом призводять систему до впорядкованого стану. Таким чином, система за своєю суттю масштабована, а основні принципи добре підходять для дуже складних і великомасштабних динамічних систем. Крім того, принципи самоорганізації успішно застосовуються для вирішення складних завдань електротехніки та інформатики. Ця популярність пов’язана з тим, що забезпечується розподілені рішення з обмеженим зв’язком, обчисленнями та споживанням енергії на системному рівні. Системи, що самоорганізуються, повинні передбачати локальну та обмежену координацію між компонентами системи.

Автоматизація мережі з використанням самоорганізованої мережі (SON) може вирішити проблеми забезпечення безперебійного покриття та ємності, масштабованості, ефективного управління радіоресурсами, енергоефективності, відмовостійкості та швидкого відновлення. Основна мета SON у стільникових мережах полягає в тому, щоб мінімізувати втручання людини в проектування та роботу мережі. Крім того, автоматизація мережі за допомогою підходів, які здатні адаптуватися до різної топології мережі, умов каналу та вимог до якості обслуговування користувачів. SON забезпечує кращу продуктивність мережі, більшу масштабованість та надійність.

Випадки використання SON, пов’язані з розгортанням і роботою мережі, зазвичай класифікуються на три основні категорії: самоналаштування, самооптимізація та самовідновлення. Самостійна конфігурація мережевих вузлів передбачає автоматичне завантаження та встановлення програмного забезпечення з наступним налаштуванням основних параметрів мережі. Ця функція «підключи і працюй» особливо важлива для гетерогенних мереж (HetNets), які складаються із випадкового та некоординованого розгортання вузлів з низьким енергоспоживанням, де традиційні підходи до планування мережі неможливі. З іншого боку, самооптимізація передбачає вимірювання стану мережі та ключових показників продуктивності, які згодом використовуються для оптимізації параметрів мережі. Приклади включають оптимізацію покриття та ємності (CCO), координацію міжстільникових перешкод та оптимізацію параметрів мобільності та балансування навантаження. Функції самовідновлення, спрямовані на мінімізацію погіршення продуктивності, запускаються, коли мережа виявляє погіршення продуктивності, наприклад перебої через збої вузлів.

У діяльності зі стандартизації 3GPP мереж стільникового зв'язку розглядалися як централізовані, так і розподілені SON. Тому алгоритми SON можуть бути повністю розподіленими, які не передбачають передачу повідомлень, розподілені підходи з передачею повідомлень або навіть централізовані механізми роботи мережі. Централізований SON означає, що всі алгоритми та функції SON розташовані в операційній системі та системі управління на високому ієрархічному рівні. У розподіленому SON усі алгоритми та функції розташовані на відносно нижчому рівні, тобто на рівні розвиненого вузла B. Архітектура, що складається з комбінації набору функцій SON, розташованих на різних ієрархічних рівнях, називається гібридною SON.

Причини, чому слід керувати пристроями IoT за допомогою системи управління:

Автоматизація. Очевидно, що суто ручної системи управління недостатньо для роботи з рішенням IoT, яке включає безліч пристроїв. Щоб безперешкодно інтегрувати рішення IoT у існуючі системи, необхідна автоматизація. Кожен інструмент або процес, необхідний для підтримки та керування рішеннями IoT, повинний функціонувати в автоматизованому режимі. Починаючи від безпечного підключення нових пристроїв до виявлення проблем, класифікації пристроїв та виведення з експлуатації старих пристроїв, система управління автоматизує кожен процес і робить усі рішення IoT більш ефективними.

Оптимізація роботи пристроїв. Розглядаючи пристрій Інтернету речей як будь-який інший розумний пристрій таким же чином, як і смартфони, планшети та комп'ютери. Стає очевидним, що оновлення мікропрограм та програмного забезпечення необхідні для інших розумних пристроїв, так же як і у випадку з пристроями IoT. Використання системи управління пристроями IoT забезпечує своєчасне оновлення, що гарантує, що помилки в пристроях IoT успішно виправляються. Системи управління дозволяють не лише віддалено оновлювати програми, мікропрограмне забезпечення та файли конфігурації для кожного пристрою; це також можна зробити на партії пристроїв. Таким чином забезпечується розгортання тисяч пристроїв у різних місцях. Система управління пристроями IoT допомагає розробникам IoT скоротити час на розробку та тестування. У поєднанні з пропозицією підключення також надається все, що потрібно для негайного запуску мережі. Крім того, архітектура, що забезпечує майбутнє, дозволяє здійснювати масштабні розгортання та сприяти майбутньому розвитку рішень IoT. Оскільки розгортання Інтернету речей може масштабуватися до сотень або тисяч територіально розкиданих вузлів, усунення несправностей за допомогою ручного підходу є дорогим або неефективним. З іншого боку, якщо тримати вузли без нагляду, існує ризик не отримати критично важливі дані, коли це найбільше потрібно. Розгортання рішення IoT надає можливість перегляд мережевого трафіку, зареєстрованих вузлів і стану в реальному часі.

Це дає змогу в режимі реального часу відстежувати вхідні дані, повідомлення та статус акумулятора з окремих вузлів.

Спрощена інтеграція: дані пристрою часто потрібно передавати в різні місця та аналізувати іншим програмним забезпеченням. Використовуючи програмне забезпечення для керування пристроями, забезпечується взаємодія між пристроями, що розгорнуті у системі.

3.3 Архітектура інформаційної системи мережі міста

Нарешті визначається архітектура інформаційної системи (див. рис. 3.6).

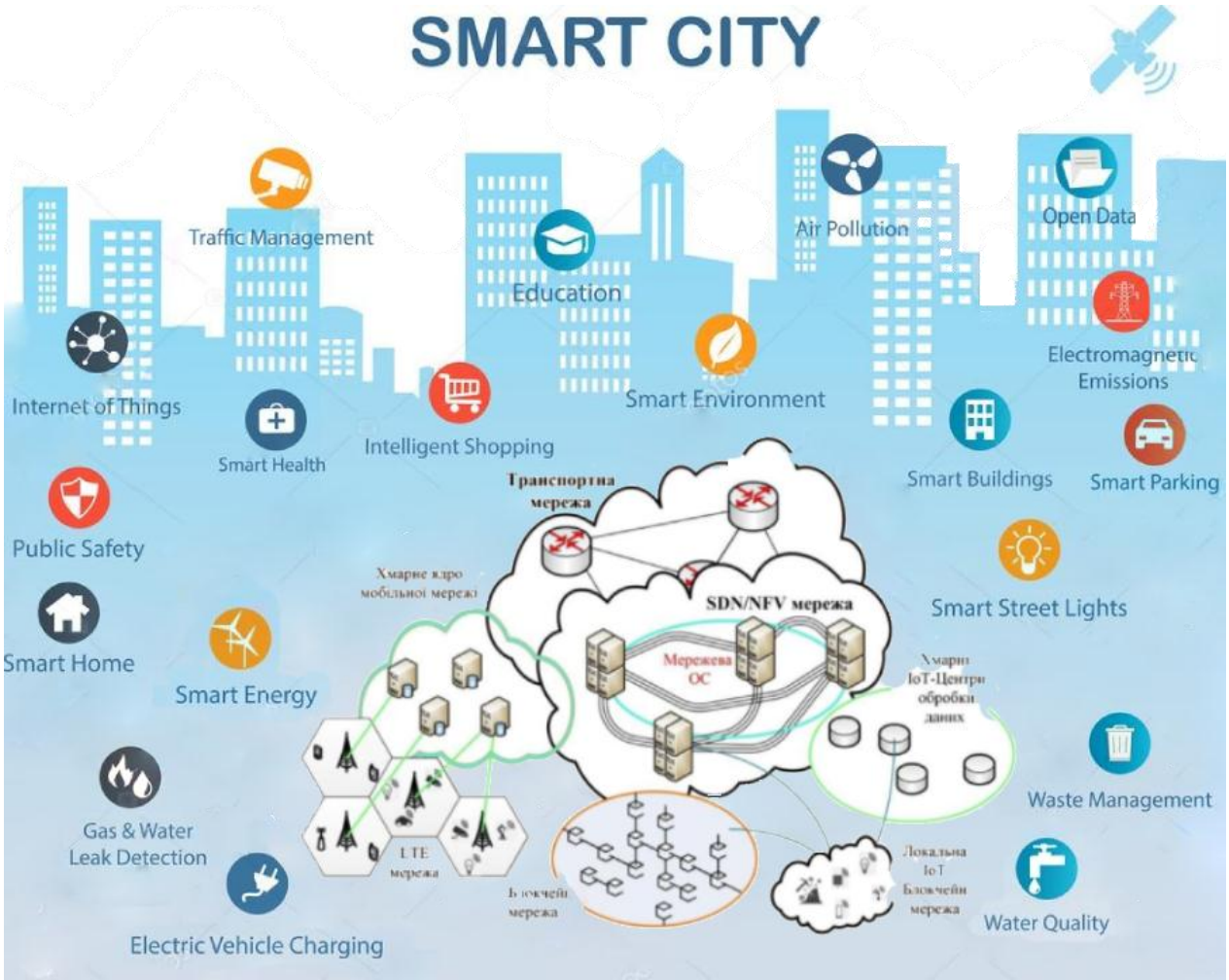


Рисунок 3.6 - Архітектура ІС Smart city

Що складається із таких компонентів:

Ядро (CORE) – технології 40 Gigabite Ethernet (40GbE) та 100 Gigabite Ethernet (100GbE). Ці стандарти є наступним етапом розвитку групи стандартів, що мали до 2010 найбільшу швидкість 10 Гбіт/с. У новому стандарті (IEEE 802.3ba-2010) забезпечуються швидкості передачі даних 40 Гбіт/с та 100 Гбіт/с при спільному використанні кількох ліній зв'язку (lane) по 10 Гбіт/с або 25 Гбіт/с кожна. Цей стандарт описує єдину архітектуру, здатну підтримувати 40 GbE та 100 GbE, визначає технічні особливості високошвидкісної передачі інформації, а також вимоги до фізичного рівня мережі: міжплатних з'єднань в активному обладнанні, мідножильних та волоконно-оптичних кабельних ліній. Стандарт 802.3Ьа підтримує лише дуплексний режим роботи.

Середовищем передачі для 40CBASE-SR4 та 100CBASE-SR10 є одномодові ОВ кабелі та багатомодові ОВ кабелі категорії ОМ-3 та ОМ-4. Ряд компаній вже пропонують рішення щодо роботи 40GbE та 100GbE, включаючи комплектуючі, комутатори та тестери. Стандарт 802.3ba розроблений на базі добре відомого та широко поширеного формату кадрів Ethernet та контролера мережного доступу та включає новий рівень середовища для 40 та 100 Гбіт/с. Робота додатків передбачена з коефіцієнтом помилок трохи більше 10-12. Середовище передачі включає одномодове (ОМВ) та багатомодове (ММВ) волокно, кручену пару і шину.

Без проводові глобальні мережі на базі технології LTE. Мережа LTE складається з удосконаленої універсальної наземної підсистеми радіодоступу (Evolved Packet Core, EPC). Вузли eNodeB здійснюють радіообмін з пристроями користувача (User Equipment, UE), реалізуючи ефективні технології OFDMA і SCFDMA і сучасні способи радіозв'язку із застосуванням більш ніж однієї антени (MIMO і формування променя). У смузі частот шириною 20 МГц швидкість передачі даних користувачам становить до 150 Мбіт/с (у разі застосування MIMO 2×2), а у зворотному напрямку – до 75 Мбіт/с. Основними функціональними елементами EPC є:

вузол управління мобільністю (Mobility Management Entity, MME), обслуговуючий шлюз (Serving Gateway, SGW), пакетний шлюз (Packet Data Network Gateway, PGW), а також вузол для виставлення рахунків користувачам та реалізації правил системної політики (Policy and Charging Rules Function, PCRF). Інформація про користувачів зберігається на сервері Home Subscriber Server (HSS). Елементи мережі взаємодіють між собою через стандартизовані інтерфейси.

SDN/NFV – віртуалізація мережних функцій. Ще одна нова парадигма Software-DefinedNetworking (SDN) використовується для організації та контролю великої кількості даних, що виробляються пристроями IoT. Вона відокремлює площину даних від площини керування мережевими пристроями, що дозволяє легко конфігурувати ці пристрої та керувати ними. Крім того, для оптимізації та безпеки мережі SDN є віртуалізація мережевих функцій (NFV). Вона дозволяє розгортати мережеві пристрої як віртуалізовані компоненти за допомогою програмного забезпечення. Інтеграція NFV в мережу SDN покращує продуктивність мережі за рахунок збільшення пропускної здатності та послідовності часу, а також скорочує час передачі.

Крім того рішення, поєднання мереж 5G з NFV і SDN робить його дуже потужним для автономних автомобілів. Підходи на основі SDN можуть забезпечити можливість взаємодії між різнорідними даними, що генеруються електронними модулями керування автономних автомобілів. Взаємодія між цими джерелами даних може принести інновації та нові інтелектуальні функції, які можуть значно покращити безпеку та зручність для пасажирів.

ЦОД (технології хмарних обчислень – Iaas, SaaS, PaaS). Для обробки та зберігання інформації існують центри обробки даних (ЦОД). Вони є спеціалізованими приміщеннями або цілими будівлями, де встановлюється серверне та мережеве обладнання, а також вибудовується відповідна інфраструктура.

Виділяють три найпоширеніші моделі хмарних послуг[26]:

– Infrastructure as a Service (IaaS) – інфраструктура як послуга – це надання обчислювальних ресурсів через хмару. Як готове рішення клієнт може вибрати: сховище даних, віртуальний сервер, операційну систему та кількість ресурсів. IaaS часто використовують ті, хто хоче позбавитися необхідності підтримувати власні локальні центри обробки даних.

– Platform as a Service (PaaS) — це платформа як послуга. Платформа як послуга (PaaS) надає середовище для розробників. Клієнти отримують доступ до платформи або набору інструментів для створення програм через інтернет. За допомогою послуг PaaS розробники можуть створювати все від простих мобільних додатків до складного програмного забезпечення для бізнесу.

– Software as a Service (SaaS) — програмне забезпечення як послуга. Програмне забезпечення як послуга (SaaS) – це надання клієнтам вже налаштованих програм для різноманітних бізнес-завдань через інтернет. Як SaaS-рішень можуть надаватися CRM, ERP, ITSM-системи, таск-трекери та інше програмне забезпечення.

ВИСНОВКИ

По перше проаналізовано технології побудови інтелектуальних інформаційних мереж. Протягом роботи досліджувались такі технології, як: LoRaWAN, 5G(NB-IoT).

По друге досліджено методи ідентифікації та розпізнавання об`єктів інформаційних мереж. Серед яких різноманітні алгоритми, математичні моделі та технології(eSim, Blockchain).

По третє визначені сервіси, що надаються інтелектуальною мережею міста. Розумне місто надає такі послуги, як:

- контроль освітлення вулиць;
- менеджмент відходами;
- забезпечує безпеку;
- контролює (електро-, водо-, газо-) постачання та відстежує можливі витіки;
- контроль транспортного трафіку.

Та сформована таблиця з вимогами для забезпечення найоптимальнішого надання цих послуг.

По четверте визначена класифікація систем управління ідентифікацією об`єктів мережі. Вона полягає розділяє системи управління ідентифікації на наступні види:

1) Централізована – управління мережею здійснюється з головної станції, а інші об’єкти лише є її «підлеглими».

2) Децентралізована – управління мережею здійснюється кількома станціями, що вважаються головними.

3) Розподільна – кожен об’єкт вважається головним, також для захисту ідентичності використовуються технологія Blockchain.

Ідентифікація об’єктів здійснюється завдяки технології eSim.

По п’яте побудована архітектура інформаційної системи інтелектуальної мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. John Smith. IoT Tutorial: Introduction to Internet of Things (IoT Basics) [Електронний ресурс] – Режим доступу до ресурсу: https://www.guru99.com/iot-tutorial.html

2. Alexander S. Gillis. What is internet of things (IoT)? [Електронний ресурс] – Режим доступу до ресурсу: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

3. Технічні характеристики 5G. Порівняння 4G та 5G. [Електронний ресурс] – Режим доступу до ресурсу: http://1234g.ru/5g/tekhnicheskie-kharakteristiki-5g

4. 5G and IoT in 2021. [Електронний ресурс] – Режим доступу до ресурсу: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/innovation-technology/5G-iot

5. Brian McGlynn, Davra, COO. The Impact of 5G on the Internet of Things [Електронний ресурс] – Режим доступу до ресурсу: https://davra.com/5g-internet-of-things/

6. LoRaWAN [Електронний ресурс] – Режим доступу до ресурсу: https://www.trendmicro.com/vinfo/us/security/definition/lorawan

7. Технологія LoRaWAN [Електронний ресурс] – Режим доступу до ресурсу: https://deps.ua/knowegable-base-ru/spravochnaya-informatsiya/66633.html

8. Що таке LoRaWan [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/nag/blog/371067/

9. WHAT IS A SMART CITY? – DEFINITION AND EXAMPLES [Електронний ресурс] – Режим доступу до ресурсу: https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city

10. SMART-ІНФРАСТРУКТУРА У СТАЛОМУ РОЗВИТКУ МІСТ: СВІТОВИЙ ДОСВІД ТА ПЕРСПЕКТИВИ УКРАЇНИ [Електронний ресурс] –

Режим доступу до ресурсу: https://razumkov.org.ua/uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf

11. Модели идентификации цифровых объектов в интернете: стандарты и перспективы / [Д. М. Белявский, С. С. Дарбинян, И. И. Засурский та ін.] // Цифровая идентификация объектов: технология и не только / [Д. М. Белявский, С. С. Дарбинян, И. И. Засурский та ін.]. – Москва: Фонд содействия развитию интернета, 2016. – С. 5–72

12. ЦЫПКИН Я.З. ИНФОРМАЦИОННАЯ ТЕОРИЯ ИДЕНТИФИКАЦИИ. [Електронний ресурс] / Я.З. ЦЫПКИН. – 1995. – Режим доступу до ресурсу: https://obuchalka.org/20191022114828/informacionnaya-teoriya-identifikacii-cipkin-ya-z-1995.html

13. ЧИКИЛЬДИН Г. П. ИДЕНТИФИКАЦИЯ ДИНАМИЧЕСКИХ ОБЪЕКТОВ. [Електронний ресурс] / Г. П. ЧИКИЛЬДИН. – 2017. – Режим доступу до ресурсу: https://ua1lib.org/book/6151511/09ddb2.

14. Горелік А. Л., Скрипкін В. А. Методи розпізнавання: Підручник для вузів, 1977.

15. Alina Burya. Как Blockchain трансформирует Интернет вещей (IoT)? [Електронний ресурс] – Режим доступу до ресурсу: https://vc.ru/crypto/75080-kak-blockchain-transformiruet-internet-veshchey-iot

16. ADAM HAYES. Blockchain Explained [Електронний ресурс] – Режим доступу до ресурсу: https://www.investopedia.com/terms/b/blockchain.asp

17. Алекс Кондратюк. Блокчейн и IoT: перспективы взаимодействия и проблемы на пути развития [Електронний ресурс] – Режим доступу до ресурсу: https://forklog.com/blokchejn-i-iot-perspektivy-vzaimodejstviya-i-problemy-na-puti-razvitiya/

18. Что такое технология блокчейна? [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/ru-ru/topics/what-is-blockchain

19. Что такое технология eSim? [Електронний ресурс] – Режим доступу до ресурсу: https://stylus.ua/articles/449.html

20. Что такое eSIM: суть технологии и особенности ее использования [Електронний ресурс] – Режим доступу до ресурсу: https://teztele.com/chto-takoe-esim-sut-tehnologii-i-osobennosti-ee-ispolzovaniya/

21. Наталья Супрунюк. eSim в Украине: что это такое и как им воспользоваться? [Електронний ресурс] – Режим доступу до ресурсу: https://itc.ua/articles/esim-v-ukraine-chto-eto-takoe-i-kak-im-vospolzovatsya/

22. Технология eSIM [Електронний ресурс] – Режим доступу до ресурсу: https://itechinfo.ru/content/esim

23. Порівняння різних мереж на основі швидкості та дальності [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/436708/

24. Види систем управління [Електронний ресурс] – Режим доступу до ресурсу: https://intuit.ru/studies/courses/3443/685/lecture/32363

25. Furqan Ahmed. Self-Organization: A Perspective on Applications in the Internet of Things [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/328673216_Self-Organization_A_Perspective_on_Applications_in_the_Internet_of_Things

26. Моделі хмарних послуг [Електронний ресурс] – Режим доступу до ресурсу: https://itglobal.com/ru-ru/company/blog/iaas-paas-saas/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

РОЗРОБКА МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ДАТЧИКІВ ТА СЕНСОРІВ В ІНТЕЛЕКТУАЛЬНІЙ МЕРЕЖІ МІСТА

Виконав: студент групи ІСДМ-61
Воїнов Юрій Юрійович
Науковий керівник:
професор, д.т.н.
Бондарчук А.П.

1) Мета роботи – дослідження та розробка інформаційних систем ідентифікації датчиків і сенсорів у інтелектуальній мережі міста
2) Об`єкт дослідження – технології інтелектуальної мережі міста.
3) Предмет дослідження – ідентифікація об`єктів інтелектуальної мережі міста.
4) Наукова новизна магістерської роботи – полягає у створеній моделі інформаційної системи.

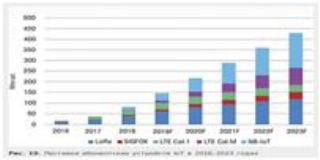
Тенденції та потреби

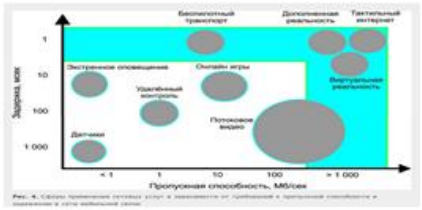
Источник: http://smart-energy.mdt.ru/

Рис. 3.8. Структура диспетчерского управления инфраструктурными объектами на территории района

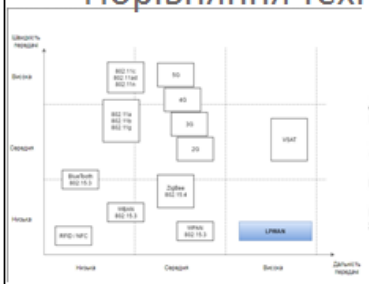
Решения Smart City

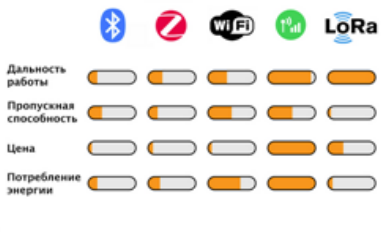
Тенденції та потреби





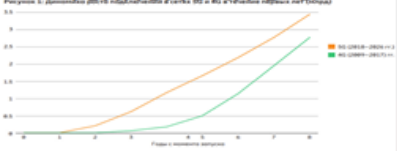
Порівняння технологій

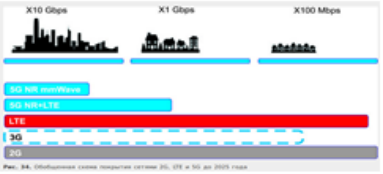




Local Area Network Short Range Communication	Low Power Wide Area (LPWAN) Internet of Things	Cellular Network Traditional M2M
Well established standards In building	Low power consumption Low cost Positioning	Existing coverage High data rate
Battery Live Provisioning Network cost & dependencies	High data rate Emerging standards	Autonomy Total cost of ownership
Bluetooth 4.0 · Wi Fi	LoRa	3G / H+ / 4G

Технологія 5 G

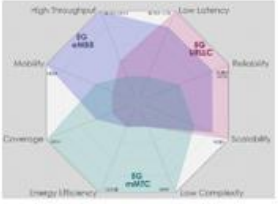




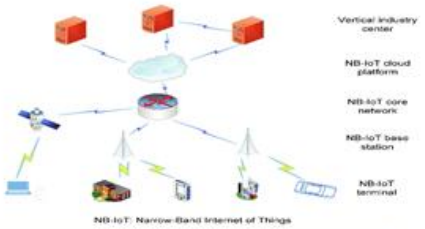
Характеристики 5 G

ТАБЛИЦА 3. СЦЕНАРИИ ПРИМЕНЕНИЯ В РАЗНЫХ ЧАСТОТНЫХ ДИАПАЗОНАХ 5G

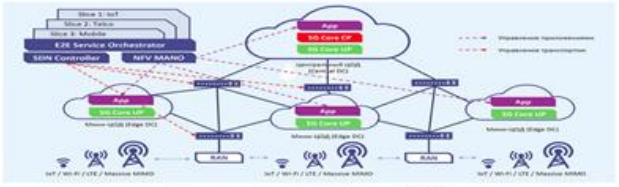
Частоты	Ширина полосы	Сценарии	Характеристика
Выше 7 ГГц (FR2)	800 МГц	eMBB	Сверхвысокая скорость, маленькое покрытие, только на улицах
2-7 ГГц (FR1)	100 МГц	eMBB, URLLC, mMTC	Высокая скорость, широкое покрытие на улицах, удовлетворительное покрытие в помещениях
< 2 ГГц (FR1)	20 МГц	eMBB, URLLC, mMTC	Средняя скорость, вездесущее покрытие на улицах и в помещениях



Архітектура мережі 5 G (NB-IoT)



NB-IoT: Narrow-Band Internet of Things



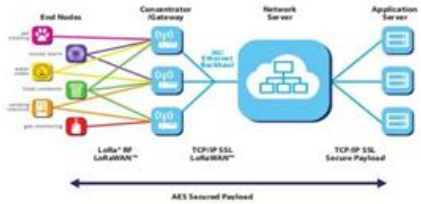
Общая архитектура сети 5G. Источник: ЦПИКС

Технічні характеристики LPWAN

Характеристика	Числова оцінка LPWAN технології
Велика дальність (Ling Range)	5 – 40 км на відкритій місцевості
Ультра низька потужність	Термін роботи батареї близько 10 років
Пропускна спроможність	Залежить від додатку, але близько декількох сотень на секунду
Витрати на мікросхеми радіоприймача	До $2
Вартість обслуговування	$1 за пристрій на рік
Затримка передачі	Не є основною вимогою для LPWAN. Додатки IoT зазвичай нечутливі до затримок
Необхідна кількість базових станцій для покриття	Дуже мала. Базові станції LPWAN спроможні обслуговувати тисячі пристроїв
Географічне покриття, проникність	Відмінне покриття в віддалених сільських місцевостях. Хороша проникність крізь будинки.

Характеристики, коректні лише для Європи	
Frequency band (частотний діапазон)	867-868 МГц
Channels	10
Channel BW Up	125/250 кГц
Channel BW Dn	125 кГц
TX Power Up/Dn	+14 дБм
SF Up	7-12
Data rate (швидкість передачі даних)	250біт/с – 50 кбіт/с
Link Budget Up/Dn	155дБ

Архітектура мережі LoRaWAN



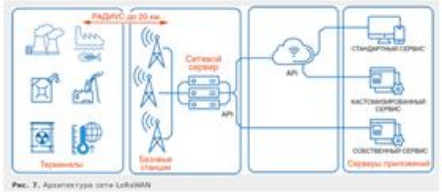
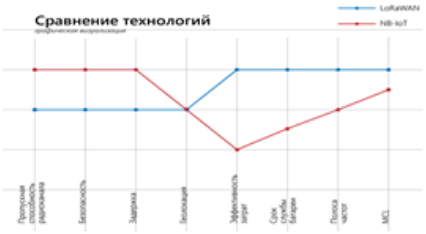


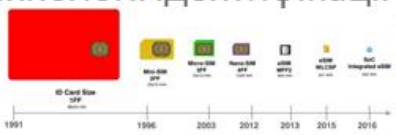
Рис. 7. Архитектура сети LoRaWAN

Порівняння 5 G і LoRaWAN мереж

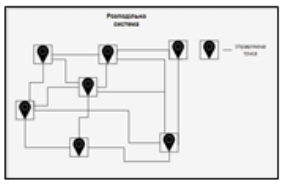
Параметры	LoRaWAN	NB-IoT
Полоса частот	125 кГц	180 кГц
Величина MCL	165 дБ	164 дБ
Срок службы батареи	15+ лет	10+ лет
Пиковый ток	32 мА	120 мА
Ток в спящем режиме	1мкА	5 мкА
Пропускная способность радиоканала	50 Кб/с	60 Кб/с
Задержка	Зависит от класса устройства	Меньше 10 с
Безопасность	AES 128 бит	3GPP 128-256 бит
Геолокация	Да, метод TDOA	Да, метод 3GPP Rel 14
Эффективность затрат (устройства и сеть)	Высокая	Средняя



Технології ідентифікації



Системи управління ідентифікацією



АРХІТЕКТУРА ІС МЕРЕЖІ SMART CITY

ВИСНОВКИ

- Визначені сервіси, що надаються інтелектуальною мережею міста
- Проаналізовано технології побудови інтелектуальних інформаційних мереж
- Досліджено методи ідентифікації об`єктів інформаційних мереж
- Визначена класифікація систем управління ідентифікацією об`єктів мережі
- Побудована архітектура інформаційної системи інтелектуальної мережі

АПРОБАЦІЯ

1. Воїнов Ю.Ю. КОНЦЕПЦІЯ SMART CITY. XIII Міжнародна науково-технічна конференція студентства та молоді «СВІТ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЙ». Збірник тез. – К.: ДУТ, 2021, с. 142-143.

2. Опубліковано статтю «ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ АВТОНОМНИХ ТРАНСПОРТНИХ ЗАСОБІВ ДЛЯ ВИКОРИСТАННЯ В МЕРЕЖАХ SMART CITY » у фаховому виданні «ЗВ'ЯЗОК» № 4 (2021) (готується до друку)