ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕЮ ІОТ ДЛЯ РОЗУМНОГО ДОМУ»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

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

_____ Владислав ЗАГОРУЙЧЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-62
Владислав ЗАГОРУЙЧЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Катерина ТРЕНЬОВА
PhD *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

ЗАТВЕРДЖУЮ
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Загоруйченко Владиславу Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Розробка інтелектуальної системи управління мережею IoT для розумного дому_____
керівник кваліфікаційної роботи Катерина ТРЕНЬОВА, PhD (доктор філософії)
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « » 2025 р. №

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Архітектура IoT-мереж систем «розумного дому».
   2. Методи моніторингу та управління телекомунікаційними IoT-мережами.
   3. Математичні моделі трафіку та параметрів якості обслуговування (QoS).
   4. Методи машинного навчання для прогнозування стану мережі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
   1. Аналіз існуючих систем моніторингу та управління IoT-мережами.
   2. Моделі управління та прогнозування стану IoT-мережі.
   3. Проєктування інтелектуального контролера управління IoT.

5. Перелік ілюстративного матеріалу: ___презентація на____слайдах_____

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	13.10.2025	Викон.
2	Розробка першого розділу	20.10.2025	Викон.
3	Розробка другого розділу	24.10.2025	Викон.
4	Розробка третього розділу	29.10.2025	Викон.
5	Розробка четвертого розділу	19.11.2025	Викон.
6	Висновки, вступ, реферат	28.11.2025	Викон.
7	Розробка презентації	12.12.2025	Викон.

Здобувач вищої освіти _____ Владислав ЗАГОРУЙЧЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Катерина ТРЕНЬОВА
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Загоруйченко В.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Розробка інтелектуальної системи управління мережею IoT для розумного дому»

Кваліфікаційна робота і рецензія додаються.

Директора ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Загоруйченко Владислав Сергійович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Загоруйченко Владислава Сергійовича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Катерина ТРЕНЬОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Загоруйченко В.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Загоруйченко Владислава Сергійовича
(прізвище, ім'я, по батькові)
на тему «Розробка інтелектуальної системи управління мережею IoT для розумного дому»

Актуальність.
Тема кваліфікаційної роботи є актуальною, оскільки стрімкий розвиток технологій Інтернету речей та зростання кількості IoT-пристроїв зумовлюють необхідність удосконалення підходів до управління телекомунікаційними мережами. Системи «розумного дому» дедалі частіше впроваджуються в житловій, комерційній та інфраструктурній сферах, що висуває підвищені вимоги до надійності, масштабованості та якості обслуговування мережі.
Особливої актуальності набуває перехід від статичних і реактивних методів управління до інтелектуальних систем, здатних прогнозувати стан мережі та приймати проактивні керуючі рішення. З огляду на умови функціонування телекомунікаційних мереж в Україні, де важливими є питання енергоефективності, стабільності зв'язку та оптимального використання ресурсів, обрана тема має як наукове, так і практичне значення.

Позитивні сторони.
1. У роботі комплексно розглянуто IoT-мережу «розумного дому» як телекомунікаційну систему, що дозволило коректно застосувати математичні моделі трафіку та методи теорії масового обслуговування.
2. Обґрунтовано доцільність використання методів машинного навчання для прогнозування стану IoT-мережі.

Недоліки.
1. У роботі доцільно було б більш детально висвітлити питання економічної ефективності впровадження інтелектуальної системи управління IoT-мережею.
2. Окремі експериментальні результати могли б бути доповнені розширеним порівняльним аналізом з існуючими комерційними IoT-рішеннями.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Загоруйченко Владислав Сергійович заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент
науковий ступінь, вчене звання _____ (підпис) _____ *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 70 стор., 12 рис., 2 табл., 17 джерел.

Мета роботи - розробка інтелектуальної системи управління IoT-мережею «розумного дому», що забезпечує адаптивне та проактивне керування телекомунікаційними ресурсами на основі математичних моделей і методів машинного навчання.

Об’єкт дослідження - процеси управління телекомунікаційною IoT мережею в системі «розумного дому», що характеризуються динамічним трафіком, обмеженими ресурсами та вимогами до якості обслуговування.

Предмет дослідження - методи та моделі інтелектуального управління IoT-мережею, зокрема математичні моделі трафіку, алгоритми прогнозування стану мережі та методи оптимізації параметрів QoS.

Короткий зміст роботи: У роботі розглянуто проблеми управління IoT-мережею «розумного дому» в умовах зростання кількості пристроїв і обсягів трафіку. Проаналізовано сучасні IoT-рішення та підходи до моніторингу телекомунікаційних мереж, визначено їхні переваги й обмеження. Розглянуто математичні моделі трафіку та параметрів якості обслуговування, а також підходи до балансування навантаження в IoT-мережі. Обґрунтовано застосування методів машинного навчання для прогнозування стану мережі та переходу до проактивного управління. Сформовано модель прийняття рішень і архітектуру інтелектуального контролера управління IoT-мережею. Проведено практичну реалізацію системи та експериментальні дослідження, результати яких підтверджують доцільність застосування інтелектуального управління в системах «розумного дому».

КЛЮЧОВІ СЛОВА: ІНТЕРНЕТ РЕЧЕЙ, IOT-МЕРЕЖА, РОЗУМНИЙ ДІМ, ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, ІНТЕЛЕКТУАЛЬНЕ УПРАВЛІННЯ, МОНІТОРИНГ МЕРЕЖІ, ПРОГНОЗУВАННЯ СТАНУ МЕРЕЖІ

ABSTRACT

Text part of the master's qualification work: 70 pages, 12 figures, 2 table, 17 sources.

The aim of the work is to develop an intelligent control system for a smart home IoT network that provides adaptive and proactive management of telecommunications resources based on mathematical models and machine learning methods.

The object of the study is the processes of managing a telecommunications IoT network in a smart home system, which are characterised by dynamic traffic, limited resources and service quality requirements.

The subject of the study is methods and models of intelligent IoT network management, in particular mathematical traffic models, network status prediction algorithms, and QoS parameter optimisation methods.

Abstract: The paper considers the problems of managing a smart home IoT network in the context of growing numbers of devices and traffic volumes. It analyses modern IoT solutions and approaches to monitoring telecommunications networks, identifying their advantages and limitations. It considers mathematical models of traffic and quality of service parameters, as well as approaches to load balancing in IoT networks. The use of machine learning methods for predicting network status and transitioning to proactive management is justified. A decision-making model and architecture for an intelligent IoT network management controller are developed. The system is implemented in practice and experimental studies are conducted, the results of which confirm the feasibility of using intelligent management in smart home systems.

KEYWORDS: INTERNET OF THINGS, IOT NETWORK, SMART HOME, TELECOMMUNICATIONS NETWORK, INTELLIGENT MANAGEMENT, NETWORK MONITORING, NETWORK STATUS FORECASTING

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1. АНАЛІЗ СИСТЕМ МОНИТОРИНГУ ТА УПРАВЛІННЯ IoT-МЕРЕЖАМИ 12
1.1. Структура та функції систем моніторингу телекомунікаційних мереж 12
1.2. Аналіз існуючих IoT-рішень для «розумного дому» 15
1.3. Проблеми масштабування, безпеки та інтелектуального управління IoT-мережами 19
РОЗДІЛ 2. МОДЕЛІ УПРАВЛІННЯ IoT-МЕРЕЖЕЮ 23
2.1. Математичні моделі трафіку та балансування навантаження 23
2.2. Методи прогнозування стану мережі на основі машинного навчання 26
2.3. Математичні моделі прийняття рішень та оптимізація параметрів QoS в IoT-мережі 31
РОЗДІЛ 3. ПРОЄКТУВАННЯ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ 36
3.1. Аналіз технічних засобів для побудови IoT-мережі (сенсори, шлюзи, контролери) 36
3.2. Архітектура інтелектуального контролера управління IoT 40
3.3. Алгоритми адаптивного керування та навчання системи 43
3.4. Проєктування бази даних і структури мережевої взаємодії 47
РОЗДІЛ 4. ПРАКТИЧНА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОГО КОНТРОЛЕРА 55
4.1. Реалізація інтелектуальної системи управління IoT-мережею 55
4.2. Інтеграція IoT-пристроїв та організація обміну даними в мережі 60
4.2.1 Загальні принципи інтеграції IoT-пристроїв у систему «розумного дому» 60
4.2.2 Організація обміну даними між IoT-пристроями та контролером 62
4.2.3 Інтеграція сенсорних і виконавчих пристроїв 65
4.2.4 Забезпечення надійності та масштабованості обміну даними 67
4.3. Експериментальні дослідження та оцінка ефективності роботи системи 69
4.3.1. Мета, умови та методика проведення експериментальних досліджень 69
4.3.2. Опис експериментального стенду та програмно-апаратної реалізації 71
4.3.3. Показники ефективності та результати експериментальних досліджень 73
4.3.4. Оцінка ефективності інтелектуального управління IoT-мережею 75
ВИСНОВКИ 78
ПЕРЕЛІК ПОСИЛАНЬ 80
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 82

ВСТУП

Стрімкий розвиток технологій Інтернету речей (Internet of Things, IoT) зумовлює суттєві зміни у підходах до побудови та експлуатації сучасних телекомунікаційних мереж. Однією з найбільш поширених сфер застосування IoT є системи «розумного дому», які поєднують велику кількість сенсорних та виконавчих пристроїв, мережевих шлюзів і програмних компонентів управління. Зі зростанням кількості підключених пристроїв, ускладненням сценаріїв автоматизації та збільшенням обсягів передаваних даних особливої актуальності набувають питання ефективного управління IoT-мережею як телекомунікаційною системою.

Аналіз сучасних IoT-рішень для «розумного дому» свідчить, що більшість комерційних систем орієнтовані на функціональність і зручність користування, однак використовують переважно статичні або реактивні підходи до управління мережею. Такі підходи не забезпечують належної адаптації до динамічних змін мережевого навантаження, не враховують прогнозовані стани мережі та мають обмежені можливості щодо оптимізації параметрів якості обслуговування (QoS). У результаті це призводить до перевантажень окремих вузлів, зростання затримок передавання даних, зниження надійності та збільшення енергоспоживання IoT-пристроїв.

Особливо гостро зазначені проблеми проявляються в умовах України, де системи «розумного дому» все частіше інтегруються в житлові, адміністративні та критично важливі об’єкти, а телекомунікаційна інфраструктура може характеризуватися обмеженою пропускною здатністю, нестабільністю каналів зв’язку та підвищеними вимогами до енергоефективності. У таких умовах актуальною є задача переходу від реактивного до інтелектуального, проактивного управління IoT-мережею, що базується на математичних моделях, методах прогнозування та оптимізації параметрів роботи мережі.

Метою магістерської роботи є розробка інтелектуальної системи управління IoT-мережею «розумного дому», що забезпечує адаптивне та проактивне керування телекомунікаційними ресурсами на основі математичних моделей і методів машинного навчання.

Для досягнення поставленої мети в процесі дослідження вирішувалися такі завдання: проаналізувати сучасні системи моніторингу та управління IoT-мережами; дослідити існуючі IoT-рішення для «розумного дому» та виявити їх обмеження з точки зору телекомунікаційної ефективності; розробити математичні моделі трафіку та балансування навантаження в IoT-мережі; обґрунтувати застосування методів машинного навчання для прогнозування стану мережі; сформалізувати процес прийняття рішень та оптимізації параметрів якості обслуговування; спроєктувати архітектуру інтелектуального контролера управління IoT-мережею.

Об’єктом дослідження є процеси управління телекомунікаційною IoT-мережею в системі «розумного дому», що характеризуються динамічним трафіком, обмеженими ресурсами та вимогами до якості обслуговування.

Предметом дослідження є методи та моделі інтелектуального управління IoT-мережею, зокрема математичні моделі трафіку, алгоритми прогнозування стану мережі та методи оптимізації параметрів QoS.

У роботі використано методи системного аналізу для дослідження існуючих IoT-рішень, математичне моделювання для опису трафіку та процесів управління, методи теорії масового обслуговування для оцінювання затримок і пропускної здатності, а також методи машинного навчання для прогнозування стану мережі. Для оцінювання ефективності запропонованої системи застосовано експериментальні методи та статистичний аналіз результатів.

Наукова новизна роботи полягає в удосконаленні підходу до управління IoT-мережею «розумного дому» шляхом поєднання моделей трафіку, методів прогнозування та оптимізації в межах єдиної інтелектуальної системи. Подальшого розвитку набули методи проактивного управління

телекомунікаційною мережею з урахуванням прогнозованих параметрів її стану.

Практична значущість роботи полягає в можливості використання розробленої системи управління для підвищення ефективності функціонування реальних IoT-мереж «розумного дому», зменшення затримок передавання даних, зниження енергоспоживання та покращення якості обслуговування.

Магістерська робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел. У першому розділі проведено аналіз існуючих IoT-рішень і проблем управління мережами. У другому розділі розглянуто математичні моделі та методи прогнозування. Третій розділ присвячено проєктуванню інтелектуальної системи управління, а в четвертому розділі наведено практичну реалізацію та результати експериментальних досліджень.

РОЗДІЛ 1. АНАЛІЗ СИСТЕМ МОНИТОРИНГУ ТА УПРАВЛІННЯ IoT-МЕРЕЖАМИ

1.1. Структура та функції систем моніторингу телекомунікаційних мереж

Системи моніторингу телекомунікаційних мереж є ключовим компонентом сучасних розподілених інформаційно-комунікаційних систем, оскільки забезпечують спостереження за станом мережевої інфраструктури, контроль параметрів якості обслуговування та своєчасне виявлення відхилень у роботі мережі. У контексті мереж Інтернету речей (IoT) роль таких систем зростає, оскільки кількість підключених пристроїв, гетерогенність протоколів і обмежені ресурси вузлів створюють додаткові вимоги до надійності та адаптивності моніторингу.

Загальна структура системи моніторингу телекомунікаційної мережі (Рис.1.1) має багаторівневу організацію та, як правило, включає рівень збору даних, рівень транспортування інформації та рівень обробки й аналізу. На рівні збору даних функціонують мережеві вузли, сенсори та агенти моніторингу, які здійснюють вимірювання ключових параметрів мережі, таких як затримка передачі пакетів, пропускна здатність каналів, рівень втрат даних, завантаження вузлів і споживання енергії. У мережах IoT ці функції часто реалізуються безпосередньо на кінцевих пристроях або шлюзах доступу, що вимагає мінімізації обчислювальних і енергетичних витрат.

Рівень транспортування даних забезпечує передачу зібраної інформації до центральних або розподілених вузлів обробки. Для цього використовуються стандартні телекомунікаційні протоколи та механізми, адаптовані до умов IoT-мереж, зокрема асинхронна передача повідомлень, агрегування даних та буферизація. Важливою особливістю цього рівня є необхідність забезпечення надійності передачі моніторингової інформації навіть у разі нестабільних каналів зв’язку або обмеженої пропускної здатності.

На рівні обробки та аналізу відбувається централізований або децентралізований аналіз параметрів мережі з метою оцінки її поточного стану та прогнозування подальшої поведінки. Саме на цьому рівні реалізуються алгоритми статистичної обробки, кореляційного аналізу та інтелектуальні методи обробки даних, що дозволяють виявляти аномалії, перевантаження або потенційні відмови мережевих компонентів. Для телекомунікаційних IoT-мереж характерним є поєднання класичних методів моніторингу з елементами машинного навчання, що забезпечує адаптивність системи до змін умов експлуатації.

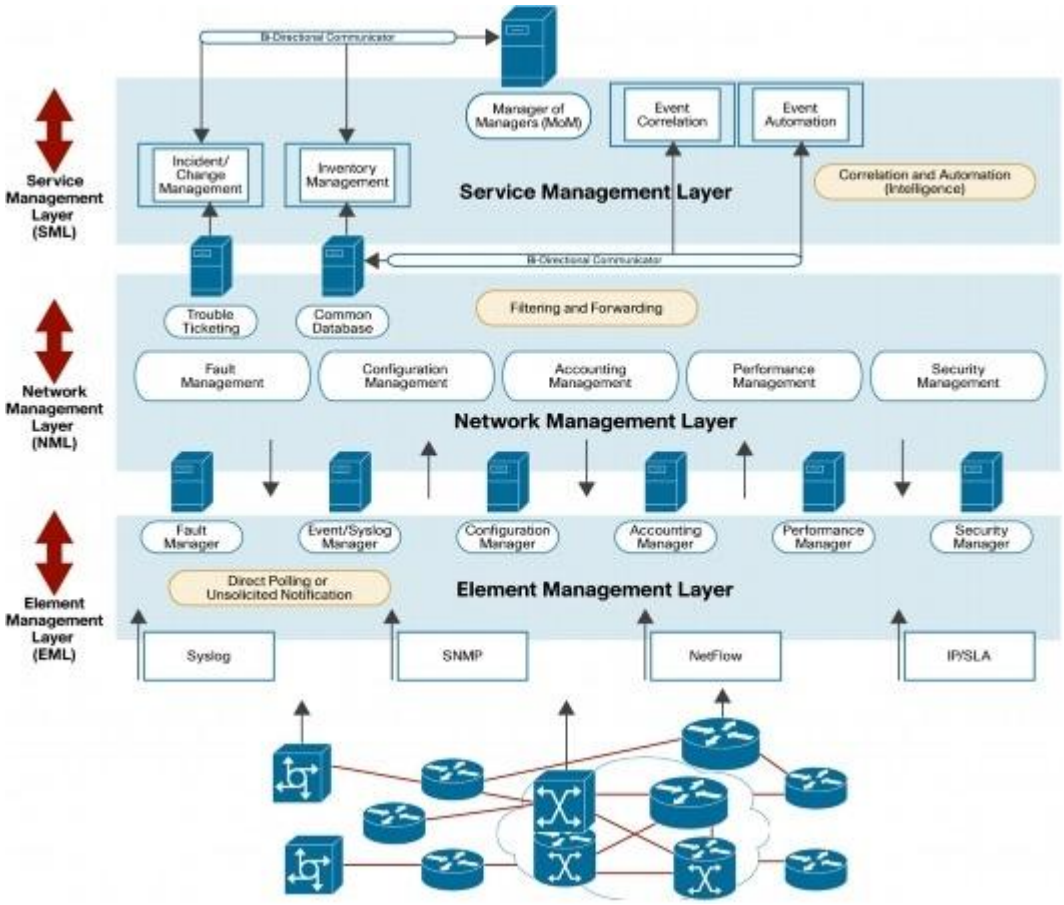


Рис. 1.1. Загальна структура системи моніторингу телекомунікаційної мережі

Функціонально системи моніторингу телекомунікаційних мереж виконують кілька взаємопов’язаних завдань. Першою базовою функцією є збір

і накопичення даних про стан мережі в реальному часі або з заданою періодичністю. Друга функція полягає в аналізі отриманих даних та визначенні відповідності фактичних параметрів мережі заданим нормативам або вимогам якості обслуговування. Третьою важливою функцією є візуалізація результатів моніторингу, що дозволяє оператору або системі управління отримувати узагальнену інформацію про стан мережі у вигляді графіків, таблиць та індикаторів.

Окреме значення для IoT-мереж має функція підтримки процесів управління, яка реалізується через передачу результатів моніторингу до системи прийняття рішень. На основі цих даних можуть виконуватися керуючі дії, спрямовані на зміну параметрів маршрутизації, балансування навантаження або оптимізацію енергоспоживання мережевих вузлів. Таким чином, система моніторингу виступає інформаційною основою для інтелектуального управління телекомунікаційною мережею.

З формальної точки зору основні параметри, що контролюються системою моніторингу, можуть бути представлені у вигляді вектору стану мережі (1.1)

$$\mathbf{S}(t) = \{d(t), b(t), p(t), e(t)\}, \tag{1.1}$$

де $d(t)$— середня затримка передачі даних, $b(t)$— доступна пропускна здатність, $p(t)$— імовірність втрат пакетів, $e(t)$— рівень енергоспоживання мережевих вузлів у момент часу t. Такий опис дозволяє надалі використовувати результати моніторингу для побудови математичних моделей управління та оптимізації роботи IoT-мережі.

Отже, системи моніторингу телекомунікаційних мереж забезпечують комплексне спостереження за параметрами функціонування мережі та створюють інформаційну основу для реалізації інтелектуальних методів управління. У контексті мереж Інтернету речей для «розумного дому» ефективна структура та коректна реалізація функцій моніторингу є

необхідною умовою забезпечення надійності, масштабованості та якості обслуговування всієї системи.

1.2. Аналіз існуючих IoT-рішень для «розумного дому»

Системи «розумного дому», побудовані на основі технологій Інтернету речей, які сьогодні є одним із найпоширеніших прикладів практичного застосування IoT у телекомунікаційних мережах. Вони поєднують в собі сенсорні пристрої, виконавчі модулі, мережеву інфраструктуру та програмні платформи управління, забезпечуючи автоматизацію житлового середовища. Аналіз існуючих IoT-рішень дозволяє визначити типові архітектурні підходи, використовувані телекомунікаційні технології та обмеження, що виникають під час їх експлуатації.

Більшість сучасних IoT-рішень для «розумного дому» реалізуються за ієрархічною архітектурою, у якій кінцеві пристрої з обмеженими ресурсами підключаються до локального шлюзу або контролера. Такий контролер виконує функції агрегації даних, маршрутизації повідомлень та взаємодії з хмарною або локальною серверною інфраструктурою. З телекомунікаційної точки зору ця модель дозволяє зменшити навантаження на сенсорні вузли та забезпечити централізований контроль, однак створює додаткову залежність від працездатності шлюзу.

Для обміну даними в існуючих IoT-системах «розумного дому» застосовується широкий спектр бездротових технологій зв’язку. Найчастіше використовуються протоколи ближнього радіусу дії, орієнтовані на енергоефективність та низьку швидкість передачі даних, а також мережі Wi-Fi для забезпечення доступу до локальної або глобальної мережі. Вибір технології визначається компромісом між пропускною здатністю, енергоспоживанням та дальністю зв’язку, що безпосередньо впливає на якість обслуговування мережі.

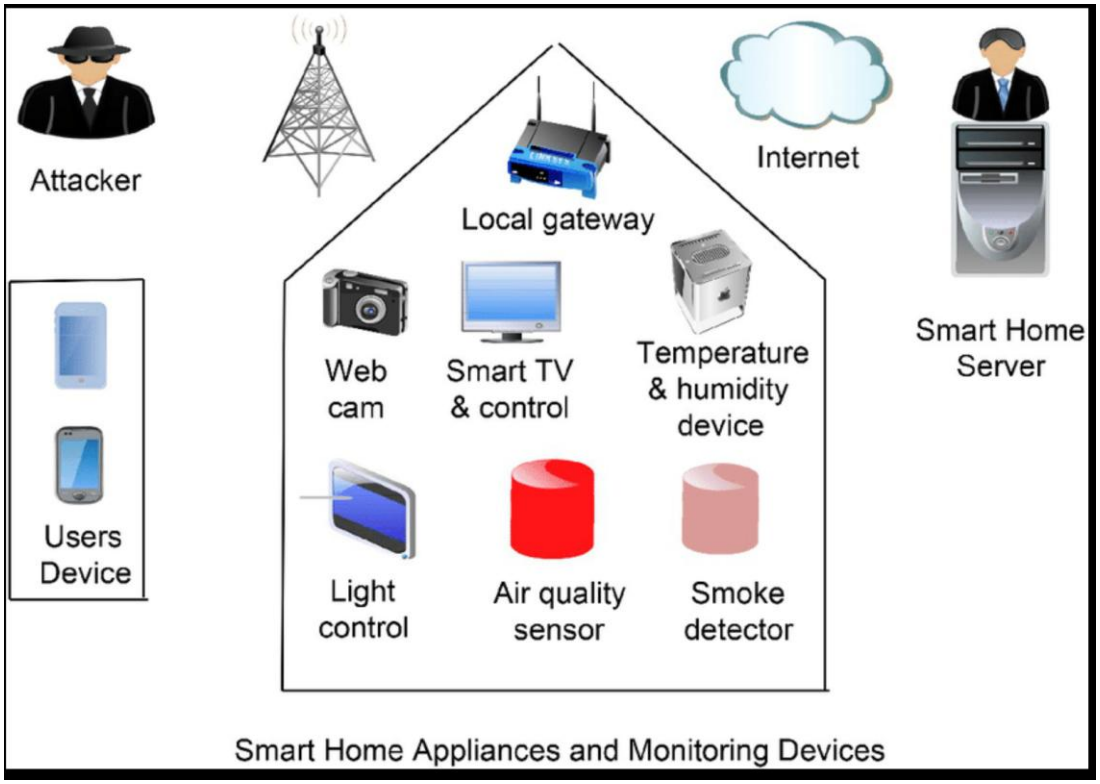


Рис. 1.2 Розумна побутова техніка та пристрої моніторингу

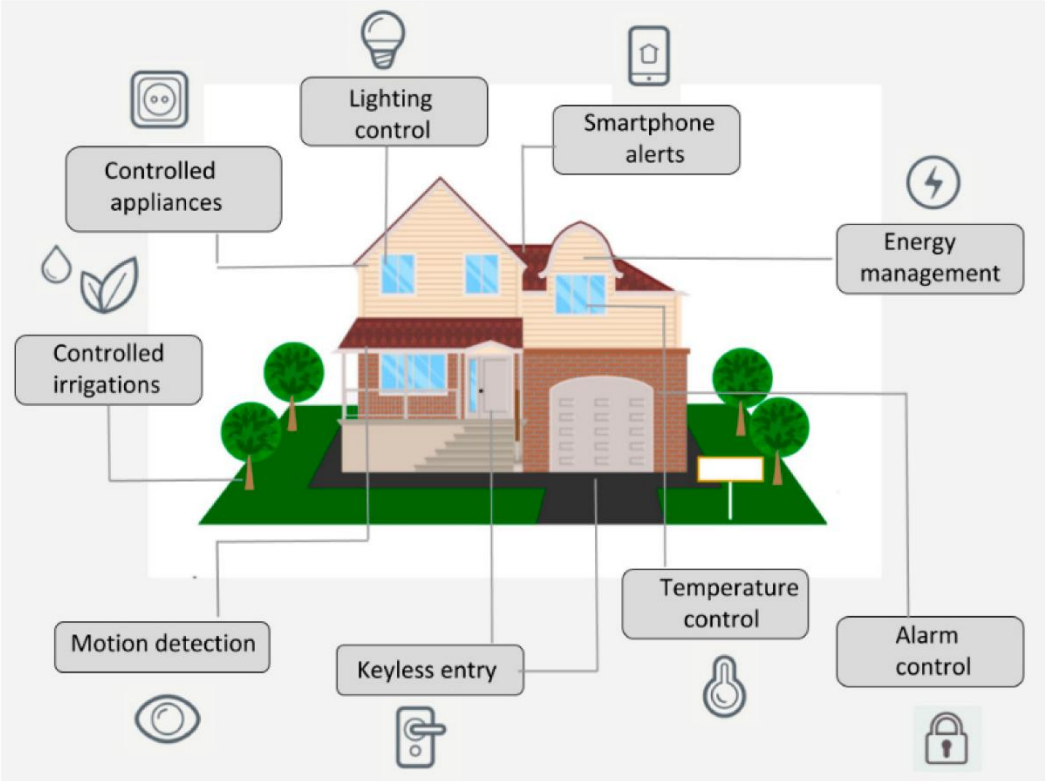


Рис. 1.3. Приклад автоматизації системи розумного дому на основі IoT

З функціональної точки зору більшість існуючих IoT-рішень орієнтовані на моніторинг параметрів середовища та дистанційне керування виконавчими пристроями. До типових функцій належать контроль температури, вологості, освітлення, енергоспоживання, а також автоматизоване керування системами опалення, вентиляції, безпеки та доступу. При цьому алгоритми управління у багатьох комерційних рішеннях мають переважно статичний характер і базуються на заздалегідь визначених сценаріях або простих правилах.

З точки зору телекомунікаційних систем важливим аспектом є спосіб обробки та передачі даних у таких IoT-рішеннях. Частина систем використовує централізовану модель із передачею даних у хмарну інфраструктуру, що спрощує масштабування та доступ користувачів, але водночас збільшує затримки та залежність від зовнішніх каналів зв’язку. Альтернативою є локальні рішення з обмеженим виходом у глобальну мережу, які характеризуються меншими затримками, проте мають обмежені можливості аналітики та прогнозування.

Для узагальнення результатів аналізу існуючих IoT-рішень виділимо їх основні характеристики. У таблиці 1.1 наведено узагальнену характеристику основних підходів до побудови IoT-рішень для «розумного дому», які відрізняються архітектурою, способом обробки даних та рівнем залежності від телекомунікаційної інфраструктури. Виділення централізованих, локальних та гібридних рішень дозволяє систематизувати існуючі підходи та оцінити їх придатність для реалізації інтелектуального управління IoT-мережею.

Таблиця 1.1

Узагальнена характеристика IoT-рішень для «розумного дому»

Характеристика	**Централізовані рішення**	**Локальні рішення**	**Гібридні рішення**
Архітектура	Хмарна	Локальна	Комбінована
Затримка передачі даних	Висока	Низька	Середня

Продовження таблиці 1.1

Узагальнена характеристика IoT-рішень для «розумного дому»

Масштабованість	Висока	Обмежена	Висока
Залежність від мережі Інтернет	Значна	Мінімальна	Часткова
Гнучкість управління	Середня	Обмежена	Висока

Централізовані IoT-рішення базуються на використанні хмарної інфраструктури як основного вузла обробки та управління. У таких системах більшість даних, зібраних сенсорними пристроями, передається через телекомунікаційну мережу до віддалених серверів, де виконується їх аналіз, зберігання та формування керуючих впливів. Основною перевагою цього підходу є висока масштабованість, оскільки обчислювальні ресурси хмари дозволяють обслуговувати значну кількість пристроїв без суттєвих змін у локальній інфраструктурі. Водночас централізована архітектура характеризується підвищеними затримками передачі даних та значною залежністю від стабільності доступу до мережі Інтернет, що є критичним для телекомунікаційних систем реального часу.

Локальні IoT-рішення орієнтовані на обробку та управління даними безпосередньо в межах локальної мережі «розумного дому». У таких системах основні функції моніторингу та прийняття рішень реалізуються на локальному контролері або шлюзі, що зменшує затримки передачі та знижує навантаження на зовнішні канали зв’язку. З телекомунікаційної точки зору цей підхід є ефективним для забезпечення мінімальної затримки та підвищеної надійності, однак він обмежений за масштабованістю та обчислювальними можливостями. Крім того, відсутність централізованої аналітики ускладнює реалізацію складних алгоритмів прогнозування та інтелектуального управління мережею.

Гібридні IoT-рішення поєднують переваги централізованих і локальних підходів, використовуючи розподілену архітектуру управління. У таких

системах частина обробки даних і прийняття рішень виконується локально, тоді як складні аналітичні та оптимізаційні задачі передаються до серверної або хмарної інфраструктури. Такий підхід дозволяє зменшити затримки для критичних керуючих операцій і водночас забезпечити масштабованість та гнучкість системи. З позиції телекомунікаційних систем гібридна архітектура є найбільш перспективною, оскільки дозволяє адаптувати управління IoT-мережею до змін навантаження та умов зв’язку.

Порівняльний аналіз, наведений у таблиці 1.1, свідчить про те, що жоден із розглянутих підходів не є універсальним. Централізовані рішення забезпечують зручність і масштабованість, але страждають від затримок і залежності від мережі Інтернет. Локальні системи характеризуються високою оперативністю, проте обмежені з точки зору інтелектуальної обробки та розширення. Гібридні рішення, хоча й є складнішими в реалізації, створюють передумови для побудови адаптивних та інтелектуальних систем управління IoT-мережами.

Таким чином, результати аналізу підтверджують доцільність переходу від простих сценарних або централізованих підходів до інтелектуальних систем управління, здатних динамічно адаптуватися до змін параметрів телекомунікаційної мережі. Саме ці обмеження існуючих підходів зумовлюють актуальність подальшого дослідження проблем масштабування, безпеки та інтелектуального управління IoT-мережами.

1.3. Проблеми масштабування, безпеки та інтелектуального управління IoT-мережами

Проведений у попередньому підрозділі аналіз існуючих IoT-рішень для «розумного дому» показав, що більшість сучасних систем орієнтовані на функціональність і зручність використання, однак мають суттєві обмеження з точки зору телекомунікаційної ефективності. Зі зростанням кількості підключених пристроїв, обсягу переданих даних і складності сценаріїв

взаємодії ці обмеження проявляються у вигляді проблем масштабування, забезпечення безпеки та недостатнього рівня інтелектуальності управління мережею.

Однією з ключових проблем IoT-мереж є масштабування телекомунікаційної інфраструктури. Зі збільшенням кількості сенсорних та виконавчих пристроїв різко зростає навантаження на мережеві вузли, канали зв'язку та контролери управління. Для багатьох існуючих рішень характерна статична конфігурація мережі, яка не передбачає динамічної адаптації до змін топології або інтенсивності трафіку. Це призводить до перевантаження окремих вузлів, зростання затримок передачі даних та зниження якості обслуговування, що є критичним для телекомунікаційних систем реального часу.

Проблема масштабування тісно пов'язана з обмеженими ресурсами IoT-пристроїв. Більшість сенсорних вузлів мають обмежену обчислювальну потужність, обсяг пам'яті та запас енергії, що ускладнює реалізацію складних мережевих протоколів і алгоритмів управління. У результаті значна частина логіки управління переноситься на шлюзи або сервери, що, з одного боку, спрощує кінцеві пристрої, а з іншого — створює централізовані точки перевантаження та відмови.

Ще одним критичним аспектом є безпека телекомунікаційних IoT-мереж. Велика кількість вузлів, гетерогенність протоколів і відкритий характер середовища зв'язку створюють сприятливі умови для реалізації атак, спрямованих на порушення конфіденційності, цілісності та доступності даних. Типовими загрозами для IoT-мереж є несанкціонований доступ до пристроїв, перехоплення або підміна даних, а також атаки типу відмови в обслуговуванні. У багатьох комерційних рішеннях механізми захисту реалізуються на базовому рівні та не враховують динамічну зміну стану мережі, що знижує їх ефективність у складних телекомунікаційних середовищах.

Забезпечення безпеки в IoT-мережах ускладнюється необхідністю дотримання балансу між рівнем захисту та енергоспоживанням. Використання

складних криптографічних алгоритмів і частих процедур автентифікації може суттєво збільшувати навантаження на ресурси пристроїв, що негативно впливає на їх автономність. Таким чином, виникає задача пошуку адаптивних механізмів безпеки, які враховують поточний стан мережі та можливості її вузлів.

Окрему групу проблем становить відсутність інтелектуального управління IoT-мережею. Більшість наявних систем використовує заздалегідь визначені правила або сценарії, які не здатні ефективно реагувати на зміну умов функціонування мережі. Такий підхід є прийнятним для простих конфігурацій, проте стає неефективним у разі збільшення кількості пристроїв, появи непередбачуваних навантажень або відмов окремих вузлів. Відсутність механізмів прогнозування стану мережі призводить до запізнілого реагування на проблеми та зниження загальної ефективності системи.

З позиції телекомунікаційних систем актуальною є задача переходу від реактивного до проактивного управління мережею, яке ґрунтується на аналізі поточних і прогнозованих параметрів її стану. Формально це може бути представлено як задача оптимізації, у якій необхідно мінімізувати функцію втрат, що залежить від затримки передачі даних, рівня втрат пакетів і енергоспоживання вузлів:

$$J = \alpha \cdot D + \beta \cdot P + \gamma \cdot E, \tag{1.2}$$

де D— середня затримка в мережі, P— імовірність втрат пакетів, E— сумарне енергоспоживання, а коефіцієнти α, β, γвизначають пріоритети управління. Така постановка задачі підкреслює необхідність використання математичних моделей і інтелектуальних алгоритмів для прийняття рішень у складних IoT-мережах.

Таким чином, проблеми масштабування, безпеки та інтелектуального управління є взаємопов’язаними та визначають основні обмеження існуючих

IoT-рішень для «розумного дому». Їх вирішення потребує застосування формалізованих математичних моделей, методів прогнозування та оптимізації параметрів телекомунікаційної мережі.

РОЗДІЛ 2. МОДЕЛІ УПРАВЛІННЯ IoT-МЕРЕЖЕЮ

У першому розділі роботи було визначено основні обмеження та проблеми функціонування IoT-мереж у системах «розумного дому», зокрема питання масштабування, безпеки та недостатнього рівня інтелектуального управління телекомунікаційною інфраструктурою. Аналіз існуючих рішень показав необхідність переходу від статичних і реактивних підходів до формалізованих моделей управління, здатних враховувати динамічний характер трафіку та змінні умови функціонування мережі.

У цьому розділі розглядаються математичні та алгоритмічні основи управління IoT-мережею як телекомунікаційною системою. Основну увагу приділено моделюванню мережевого трафіку, методам балансування навантаження, прогнозуванню стану мережі та формалізації задач прийняття рішень з урахуванням параметрів якості обслуговування. Викладені теоретичні положення створюють основу для подальшого проєктування та практичної реалізації інтелектуальної системи управління IoT-мережею, що розглядається в наступних розділах роботи.

2.1. Математичні моделі трафіку та балансування навантаження

Ефективне управління IoT-мережею як телекомунікаційною системою неможливе без формалізованого опису процесів передавання даних. У мережах Інтернету речей трафік формується великою кількістю розподілених вузлів, які генерують пакети даних з різною інтенсивністю та вимогами до якості обслуговування. Такий характер трафіку зумовлює необхідність використання математичних моделей, що дозволяють оцінити навантаження на мережу, затримки передачі та ймовірність втрат пакетів.

Однією з базових моделей для опису телекомунікаційного трафіку є модель потоків заявок, у якій процес надходження пакетів описується випадковим процесом з певною інтенсивністю. Для IoT-мереж у багатьох випадках

припустимо використовувати пуассонівський потік заявок, що характеризується параметром інтенсивності λ, який визначає середню кількість пакетів, що надходять за одиницю часу. Така модель є зручною для аналітичних оцінок і широко застосовується при дослідженні сенсорних та телекомунікаційних мереж.

Для аналізу затримок і пропускної здатності IoT-мережі доцільно використовувати апарат теорії масового обслуговування. Найпростішою є модель одноканальної системи масового обслуговування типу $M/M/1$, у якій час обслуговування заявок має експоненційний розподіл з інтенсивністю μ. У такій моделі середній час перебування пакета в системі визначається співвідношенням

$$T = \frac{1}{\mu - \lambda}, \tag{2.1}$$

де $\lambda < \mu$є умовою стійкості системи. Хоча дана модель є спрощеною, вона дозволяє отримати початкові оцінки затримок і виявити вплив зростання інтенсивності трафіку на продуктивність мережі.

У реальних IoT-мережах «розумного дому» часто має місце багатоканальне обслуговування та ієрархічна структура передачі даних, що потребує використання більш складних моделей, зокрема $M/M/n$або мереж черг. У таких моделях кожен вузол або шлюз може розглядатися як окрема система масового обслуговування, а загальний час затримки визначається сумою затримок на окремих етапах маршруту. Формально середня затримка передачі даних у мережі може бути представлена у вигляді

$$D = \sum_{i=1}^{N} T_i, \tag{2.2}$$

де T_i— середній час обслуговування на i-му вузлі маршруту, N— кількість вузлів, через які проходить пакет.

Зі збільшенням кількості IoT-пристроїв у мережі виникає проблема нерівномірного розподілу навантаження, коли окремі вузли або канали зв’язку стають перевантаженими, тоді як інші використовуються неефективно. Для

розв’язання цієї проблеми застосовуються методи балансування навантаження, метою яких є рівномірний розподіл трафіку між доступними ресурсами мережі. У телекомунікаційних системах балансування навантаження часто формулюється як задача мінімізації максимального навантаження на вузли мережі.

Нехай мережа описується графом $G = (V, E)$, де V— множина вузлів, E— множина каналів зв’язку. Інтенсивність трафіку, що проходить через вузол v_i, позначимо як λ_i. Тоді задача балансування навантаження може бути сформульована у вигляді оптимізаційної задачі $\min\left(\max_i \lambda_i\right)$, за умови дотримання обмежень на пропускну здатність каналів і вимоги до якості обслуговування. Така постановка дозволяє формалізувати вибір маршрутів і розподіл потоків даних у мережі.

Особливістю IoT-мереж є також різнорідність трафіку, оскільки різні типи пристроїв генерують пакети з різною періодичністю та пріоритетами. Наприклад, події безпеки потребують мінімальної затримки, тоді як дані моніторингу можуть передаватися з менш жорсткими часовими вимогами. У математичних моделях це враховується шляхом введення вагових коефіцієнтів або класів обслуговування, що дозволяє оцінювати вплив пріоритетів на затримки та пропускну здатність мережі.

Таким чином, математичні моделі трафіку та балансування навантаження створюють теоретичну основу для аналізу продуктивності IoT-мережі та оцінки її здатності забезпечувати задані параметри якості обслуговування. Отримані в цьому підпункті формалізовані залежності є базою для подальшого розгляду методів прогнозування стану мережі та інтелектуального прийняття рішень, які дозволяють адаптивно керувати трафіком у динамічному телекомунікаційному середовищі.

2.2. Методи прогнозування стану мережі на основі машинного навчання

Управління IoT-мережею як телекомунікаційною системою ускладнюється динамічним характером трафіку, змінною кількістю активних пристроїв та нестабільністю параметрів зв'язку. Класичні аналітичні моделі, розглянуті вище, дозволяють оцінювати стан мережі за фіксованих умов, однак вони не забезпечують достатньої гнучкості в ситуаціях, коли параметри мережі змінюються у часі. У зв'язку з цим актуальним є застосування методів машинного навчання для прогнозування стану IoT-мережі та підтримки процесів інтелектуального управління.

Прогнозування стану мережі передбачає оцінювання майбутніх значень ключових телекомунікаційних параметрів на основі історичних даних моніторингу. До таких параметрів належать інтенсивність трафіку, середня затримка передачі даних, імовірність втрат пакетів, завантаження мережевих вузлів і рівень енергоспоживання. Формально стан мережі в момент часу t може бути представлений вектором

$$\mathbf{S}(t) = \{\lambda(t), D(t), P(t), E(t)\}, \tag{2.3}$$

де $\lambda(t)$— інтенсивність надходження пакетів, $D(t)$— середня затримка, $P(t)$— імовірність втрат, $E(t)$— енергоспоживання. Завдання прогнозування полягає у визначенні оцінки вектора $\mathbf{S}(t + \Delta t)$на деякому часовому горизонті Δt.

Методи машинного навчання дозволяють формувати прогностичні моделі без необхідності жорсткого аналітичного опису всіх процесів у мережі. Найпростішим підходом є використання методів регресійного аналізу, у яких майбутні значення параметрів мережі визначаються як функція їх попередніх значень. Лінійні та поліноміальні регресійні моделі є обчислювально простими та придатними для використання на вузлах з обмеженими ресурсами, проте їх

точність знижується у випадку складних нелінійних залежностей, характерних для IoT-мереж.

Більш ефективними для прогнозування телекомунікаційного трафіку є методи машинного навчання, що враховують часову залежність даних. До таких методів належать моделі часових рядів, зокрема авторегресійні моделі та рекурентні нейронні мережі. Вони дозволяють враховувати кореляції між значеннями параметрів мережі в різні моменти часу та адаптуватися до змін умов функціонування. Застосування таких моделей є доцільним у мережах «розумного дому», де характер трафіку часто залежить від добових циклів, поведінки користувачів та сценаріїв автоматизації.

Для задач прогнозування стану телекомунікаційної IoT-мережі широко застосовуються методи *навчання з учителем*, у яких модель навчається на попередньо розмічених даних моніторингу. Такі методи дозволяють встановити залежність між вхідними параметрами мережі та її функціональним станом, що є особливо важливим для автоматизованих систем управління. До найбільш поширених моделей цього класу належать дерева рішень, ансамблеві методи та їх комбінації, які забезпечують баланс між точністю прогнозування та інтерпретованістю результатів.

Дерева рішень є одним із найпростіших і водночас ефективних методів навчання з учителем, що широко використовуються в задачах аналізу телекомунікаційних мереж. У таких моделях процес прийняття рішення представлений у вигляді ієрархічної структури, де кожен внутрішній вузол відповідає перевірці певного параметра мережі, а листові вузли — прогнозованому стану. Для IoT-мереж параметрами розгалуження можуть бути значення затримки передачі, інтенсивності трафіку, рівня втрат пакетів або завантаження вузлів. Основною перевагою дерев рішень є їх наочність і можливість прямої інтерпретації отриманих правил, що спрощує інтеграцію таких моделей у системи управління телекомунікаційною мережею. Водночас дерева рішень можуть бути чутливими до шуму в даних і схильними до перенавчання за великої кількості параметрів.

Для підвищення точності прогнозування та зменшення впливу випадкових факторів у практиці управління IoT-мережами широко застосовуються *ансамблеві методи*, які базуються на поєднанні декількох моделей навчання. Найбільш відомим прикладом є метод *випадкового лісу*, у якому використовується сукупність дерев рішень, навчання яких виконується на різних підмножинах даних і параметрів. Такий підхід дозволяє зменшити дисперсію прогнозу та підвищити стійкість моделі до змін у мережевому середовищі. Для телекомунікаційних IoT-мереж ансамблеві моделі є особливо корисними в умовах нерівномірного трафіку та динамічної зміни топології мережі.

Окрему групу ансамблевих методів становлять *методи підсилення*, у яких послідовно формуються моделі, що компенсують помилки попередніх. Такі підходи дозволяють більш точно прогнозувати складні стани мережі, наприклад наближення до перевантаження або нестабільний режим роботи окремих сегментів. У задачах управління IoT-мережею це дає змогу своєчасно виявляти критичні ситуації та ініціювати коригуючі дії ще до фактичного погіршення параметрів якості обслуговування.

Важливою особливістю методів навчання з учителем є можливість *класифікації станів мережі,* а не лише прогнозування числових значень параметрів. Наприклад, на основі вхідного вектора параметрів мережі модель може визначати, чи перебуває мережа в нормальному режимі функціонування, режимі підвищеного навантаження або аварійному стані. Така класифікація значно спрощує подальший етап прийняття рішень у системі управління, оскільки дозволяє застосовувати заздалегідь визначені стратегії керування для кожного класу станів.

Таким чином, дерева рішень і ансамблеві методи навчання з учителем є ефективним інструментом прогнозування та класифікації станів IoT-мережі. Їх застосування забезпечує формування структурованої інформації про стан телекомунікаційної системи, що створює основу для реалізації

інтелектуальних алгоритмів управління та оптимізації параметрів якості обслуговування в умовах динамічного функціонування мережі.

Особливу увагу в IoT-мережах слід приділяти обчислювальній складності моделей машинного навчання. Багато сенсорних вузлів і шлюзів мають обмежені ресурси, тому використання складних моделей безпосередньо на периферійних пристроях є недоцільним. У таких випадках застосовується розподілений підхід, за якого попередня обробка та агрегація даних виконується локально, а навчання і прогнозування — на більш потужних обчислювальних вузлах або сервері управління.

Інтеграція результатів прогнозування в систему управління IoT-мережею дозволяє реалізувати проактивні механізми керування. Наприклад, у разі прогнозованого зростання інтенсивності трафіку система може заздалегідь змінити маршрути передачі даних або перерозподілити ресурси між вузлами мережі. З формальної точки зору прогнозовані значення параметрів використовуються як вхідні дані для задач оптимізації, що дозволяє мінімізувати затримки та втрати пакетів ще до виникнення критичних ситуацій.

Важливим аспектом застосування методів машинного навчання в управлінні IoT-мережею є оцінка точності прогнозування телекомунікаційних параметрів, оскільки саме від неї залежить ефективність подальших керуючих рішень. Некоректні або нестабільні прогнози можуть призводити до помилкового перерозподілу ресурсів мережі, збільшення затримок передачі даних або нераціонального використання енергетичних ресурсів вузлів. Тому оцінювання якості моделей прогнозування є обов’язковим етапом їх впровадження в систему управління IoT-мережею.

Для кількісної оцінки точності прогнозування широко використовуються стандартні метрики помилки, які порівнюють прогнозовані значення параметрів мережі з фактичними вимірюваннями, отриманими в результаті моніторингу. Однією з найпоширеніших метрик є середньоквадратична помилка, яка визначається як

$$\mathrm{MSE} = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2, \tag{2.4}$$

де y_i— фактичне значення прогнозованого параметра мережі, $\hat{y}_i$— відповідне прогнозоване значення, N— кількість спостережень. Дана метрика є чутливою до великих відхилень прогнозу, що дозволяє виявляти ситуації, у яких модель суттєво помиляється при різких змінах стану мережі.

Ще однією важливою метрикою є середня абсолютна похибка, яка визначається співвідношенням

$$\mathrm{MAE} = \frac{1}{N}\sum_{i=1}^{N} \mid y_i - \hat{y}_i \mid, \tag{2.5}$$

та характеризує середнє абсолютне відхилення прогнозу від реальних значень. На відміну від середньоквадратичної помилки, дана метрика менш чутлива до поодиноких великих помилок і дозволяє отримати більш стабільну оцінку якості прогнозування в умовах шумних телекомунікаційних даних, що є типовим для IoT-мереж.

Використання зазначених метрик дозволяє не лише порівнювати різні моделі машинного навчання між собою, а й оптимізувати їх параметри з урахуванням специфіки телекомунікаційної мережі. Наприклад, для задач прогнозування затримки передачі даних доцільно мінімізувати середньоквадратичну помилку, тоді як для оцінювання енергоспоживання або рівня втрат пакетів більш інформативною може бути середня абсолютна похибка. Таким чином, результати оцінювання точності прогнозування є важливим критерієм вибору конкретного методу машинного навчання та налаштування його параметрів у системі інтелектуального управління IoT-мережею.

Таким чином, методи машинного навчання створюють ефективний інструментарій для прогнозування стану IoT-мережі в умовах динамічного трафіку та обмежених ресурсів. Їх використання дозволяє перейти від реактивного управління до проактивного, що є необхідною умовою

забезпечення стабільної роботи телекомунікаційної мережі «розумного дому». Результати прогнозування стану мережі є основою для формалізації задач прийняття рішень та оптимізації параметрів якості обслуговування, які розглядаються в наступному підпункті.

2.3. Математичні моделі прийняття рішень та оптимізація параметрів QoS в IoT-мережі

Інтелектуальне управління IoT-мережею як телекомунікаційною системою передбачає формалізований процес прийняття рішень на основі інформації про поточний і прогнозований стан мережі. На відміну від реактивних підходів, які реагують лише на вже виниклі перевантаження або відмови, інтелектуальні методи управління орієнтовані на оптимізацію параметрів якості обслуговування з урахуванням динаміки трафіку, обмежень ресурсів і прогнозованих змін мережевого стану.

Основою математичної моделі прийняття рішень в інтелектуальній системі управління IoT-мережею є представлення телекомунікаційної мережі у вигляді керованої динамічної системи, стан якої змінюється у часі під впливом як зовнішніх факторів, так і керуючих дій. На відміну від статичних моделей, такий підхід дозволяє враховувати часову еволюцію параметрів мережі та використовувати результати моніторингу й прогнозування для формування проактивних рішень.

Стан IoT-мережі в дискретні моменти часу доцільно описувати узагальненим вектором телекомунікаційних параметрів

$$\mathrm{S}(t) = [s_1(t), s_2(t), s_3(t), s_4(t)], \tag{2.6}$$

де компоненти вектора відповідають основним характеристикам якості обслуговування мережі. З урахуванням специфіки IoT-систем ці параметри інтерпретуються як інтенсивність трафіку, затримка передачі даних, рівень

втрат пакетів та енергоспоживання мережевих вузлів. Таке узагальнене подання дозволяє уникнути жорсткої прив’язки до конкретних фізичних величин і надалі розширювати модель додатковими параметрами без зміни її структури.

Керуючі впливи, що формуються системою управління, задаються вектором

$$\mathrm{U}(t) = [u_1(t), u_2(t), u_3(t)], \tag{2.7}$$

елементи якого відповідають керованим параметрам телекомунікаційної мережі. До таких параметрів належать вибір маршрутів передачі даних, правила розподілу пропускної здатності між потоками та режими функціонування мережевих вузлів. Саме через зміну цих керуючих змінних система управління може впливати на динаміку мережі та досягати заданих показників якості обслуговування.

Динаміка IoT-мережі в умовах керування описується рівнянням переходу станів

$$\mathrm{S}(t+1) = F(\mathrm{S}(t), \mathrm{U}(t), \xi(t)), \tag{2.8}$$

де функція $F(\cdot)$відображає поведінку телекомунікаційної системи, а $\xi(t)$характеризує вплив випадкових факторів, зокрема нерівномірність трафіку, завади в каналах зв’язку та зміну активності IoT-пристроїв. Така модель є узагальненою та придатною для використання в умовах неповної визначеності, що є характерним для мереж Інтернету речей.

Процес прийняття рішень у системі управління формалізується як задача вибору оптимальної керуючої дії на кожному часовому кроці з урахуванням поточного та прогнозованого стану мережі. Замість фіксованої цільової функції доцільно використовувати узагальнений критерій ефективності, який оцінює якість майбутнього стану мережі:

$$\mathcal{J}(t) = \Phi(\mathrm{S}(t+1)), \tag{2.9}$$

де функціонал $\Phi(x)$відображає сукупний вплив затримки, втрат пакетів і енергоспоживання на якість обслуговування. Мінімізація цього критерію забезпечує досягнення компромісу між швидкодією мережі та її енергоефективністю без необхідності жорстко фіксувати вагові коефіцієнти для кожного параметра.

Таким чином, задача управління IoT-мережею зводиться до послідовного вибору керуючих дій

$$\mathrm{U}^*(t) = \arg \min_{\mathrm{U}(t)\in\Omega} \Phi(F(\mathrm{S}(t), \mathrm{U}(t))), \tag{2.10}$$

де Ω— множина допустимих керуючих стратегій, визначена обмеженнями телекомунікаційної інфраструктури. Такий підхід дозволяє реалізувати адаптивне та інтелектуальне управління IoT-мережею, яке враховує динамічний характер трафіку та обмежені ресурси мережевих вузлів, що є критичним для систем «розумного дому».

Оптимізаційна задача прийняття рішень розв’язується за наявності ряду обмежень, які відображають фізичні та телекомунікаційні характеристики мережі. До таких обмежень належать умови пропускної здатності каналів зв’язку

$$\lambda_i \le C_i, \tag{2.11}$$

де λ_i— інтенсивність трафіку на i-му каналі, C_i— його пропускна здатність, а також вимоги до допустимих значень затримки та втрат пакетів, що задаються нормативами якості обслуговування. Наявність цих обмежень зумовлює необхідність використання адаптивних алгоритмів управління, здатних змінювати керуючі параметри в реальному часі.

Особливістю інтелектуальних систем управління IoT-мережею є використання результатів прогнозування стану мережі, отриманих методами машинного навчання. Прогнозовані значення параметрів $\mathrm{S}(t + \Delta t)$дозволяють формувати керуючі рішення не лише на основі поточного стану, а й з

урахуванням очікуваних змін. Це забезпечує реалізацію проактивного управління, за якого система може заздалегідь змінювати маршрути, перерозподіляти навантаження або переводити окремі вузли в енергозберігаючі режими.

З точки зору телекомунікаційних систем важливим є також врахування різних класів трафіку та пріоритетів обслуговування. Для цього у математичній моделі вводяться вагові коефіцієнти або окремі цільові функції для різних типів даних. Наприклад, для критичних повідомлень систем безпеки пріоритет надається мінімізації затримки, тоді як для періодичних даних моніторингу більш важливим є зменшення енергоспоживання. Такий підхід дозволяє реалізувати диференційоване управління трафіком у межах єдиної IoT-мережі.

Таким чином, математичні моделі прийняття рішень та оптимізації параметрів QoS забезпечують формалізовану основу для інтелектуального управління IoT-мережею. Поєднання аналітичних моделей трафіку, методів прогнозування стану мережі та оптимізаційних алгоритмів дозволяє підвищити ефективність використання телекомунікаційних ресурсів, зменшити затримки передачі даних і забезпечити стабільну роботу системи «розумного дому» в умовах зростаючої складності мережевої інфраструктури.

Отже, У другому розділі магістерської роботи розглянуто теоретичні основи управління IoT-мережею як телекомунікаційною системою. На основі математичних моделей трафіку та балансування навантаження проаналізовано вплив інтенсивності передавання даних на затримки та використання мережевих ресурсів. Показано, що класичні аналітичні підходи дозволяють оцінювати продуктивність мережі, однак мають обмежені можливості в умовах динамічної зміни трафіку та масштабування IoT-інфраструктури.

Також обґрунтовано доцільність застосування методів машинного навчання для прогнозування стану IoT-мережі та формалізовано процес прийняття рішень у вигляді керованої динамічної системи. Запропонований підхід до оптимізації параметрів якості обслуговування створює теоретичну

основу для реалізації адаптивного та проактивного управління телекомунікаційною мережею. Отримані результати слугують базою для подальшого проєктування та практичної реалізації інтелектуальної системи управління IoT-мережею, що розглядається в наступному розділі.

РОЗДІЛ 3. ПРОЄКТУВАННЯ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ

3.1. Аналіз технічних засобів для побудови IoT-мережі (сенсори, шлюзи, контролери)

Побудова IoT-мережі для системи «розумного дому» як телекомунікаційної системи потребує комплексного вибору технічних засобів, які забезпечують збір, передавання, обробку та управління даними. До таких засобів належать сенсорні пристрої, виконавчі модулі, мережеві шлюзи та контролери управління. Кожен з цих компонентів виконує визначені функції та має свої обмеження, що необхідно враховувати під час проєктування інтелектуальної системи управління IoT-мережею.

Сенсорні пристрої є базовими елементами IoT-мережі, оскільки саме вони забезпечують первинний збір інформації про стан навколишнього середовища та об’єктів управління.



Рис. 3.1 Датчики та сенсори розумного будинку

У системах «розумного дому» сенсори використовуються для вимірювання температури, вологості, освітленості, рівня газів, руху, споживання електроенергії та інших параметрів. З телекомунікаційної точки зору важливими характеристиками сенсорів є точність вимірювань, частота генерації даних, енергоспоживання та підтримка бездротових інтерфейсів зв’язку. Обмежені ресурси сенсорних вузлів зумовлюють необхідність використання енергоефективних протоколів передавання даних і мінімізації обсягу переданої інформації.

Окрім сенсорів, важливу роль у IoT-мережі відіграють виконавчі пристрої, які реалізують керуючі впливи на фізичні об’єкти. До таких пристроїв належать реле, електроприводи, клапани, освітлювальні модулі та інші компоненти, що реагують на команди системи управління. З позиції телекомунікаційних систем ці пристрої висувають підвищені вимоги до затримки передавання даних і надійності зв’язку, оскільки керуючі сигнали часто мають виконуватися в режимі, близькому до реального часу.

Мережеві шлюзи виконують функцію проміжної ланки між локальною IoT-мережею та зовнішніми телекомунікаційними мережами або серверною інфраструктурою. Вони забезпечують агрегацію даних від сенсорних вузлів, перетворення протоколів, маршрутизацію повідомлень і первинну обробку інформації. У контексті інтелектуального управління шлюзи також можуть виконувати роль локальних обчислювальних вузлів, на яких реалізуються елементи аналітики або фільтрації даних. Вибір шлюзу визначається його обчислювальними можливостями, підтримуваними протоколами зв’язку та здатністю працювати в умовах обмеженої пропускної здатності каналів.

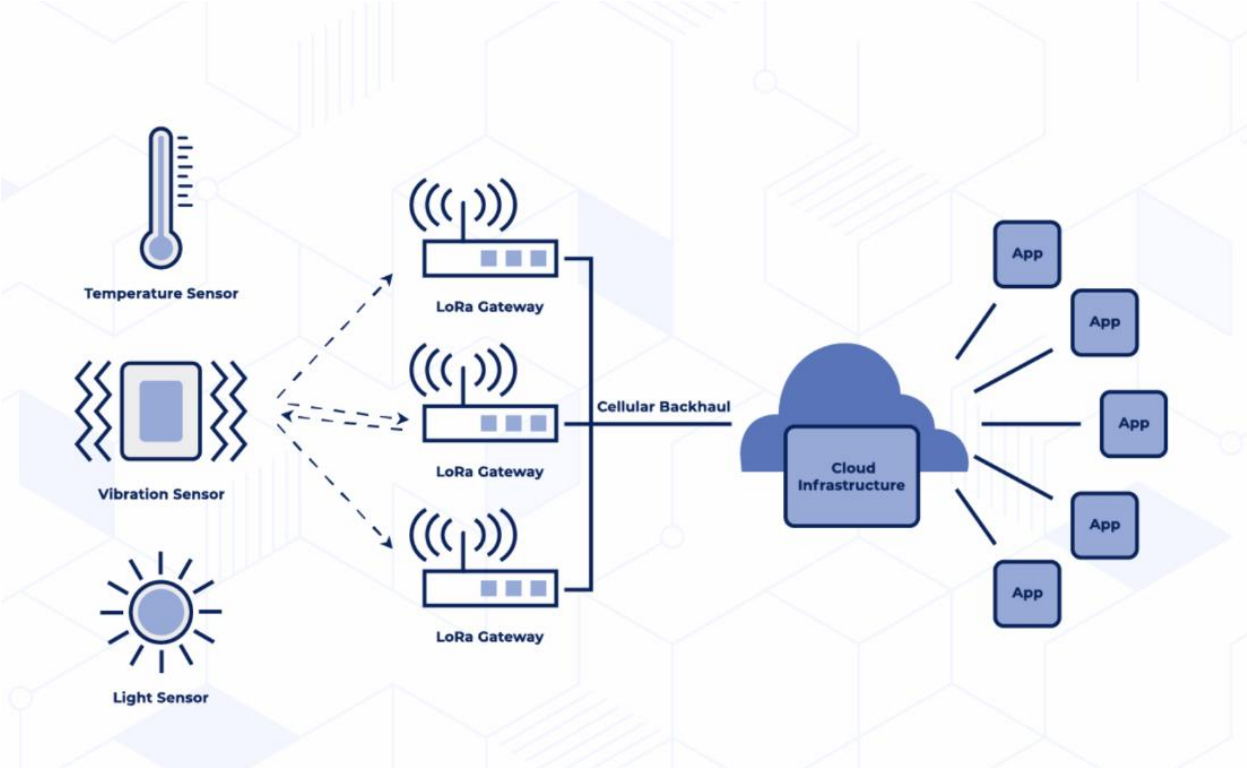


Рис. 3.2. Схема роботи IoT шлюза

Контролери управління є центральними елементами системи, що реалізують логіку прийняття рішень та взаємодіють з усіма компонентами IoT-мережі. У телекомунікаційних системах «розумного дому» контролер може бути реалізований у вигляді окремого серверного модуля, вбудованої системи або програмного компонента, розгорнутого в локальній або хмарній інфраструктурі. Основними функціями контролера є аналіз даних моніторингу, формування керуючих впливів, управління маршрутизацією трафіку та забезпечення взаємодії між різними сегментами мережі.

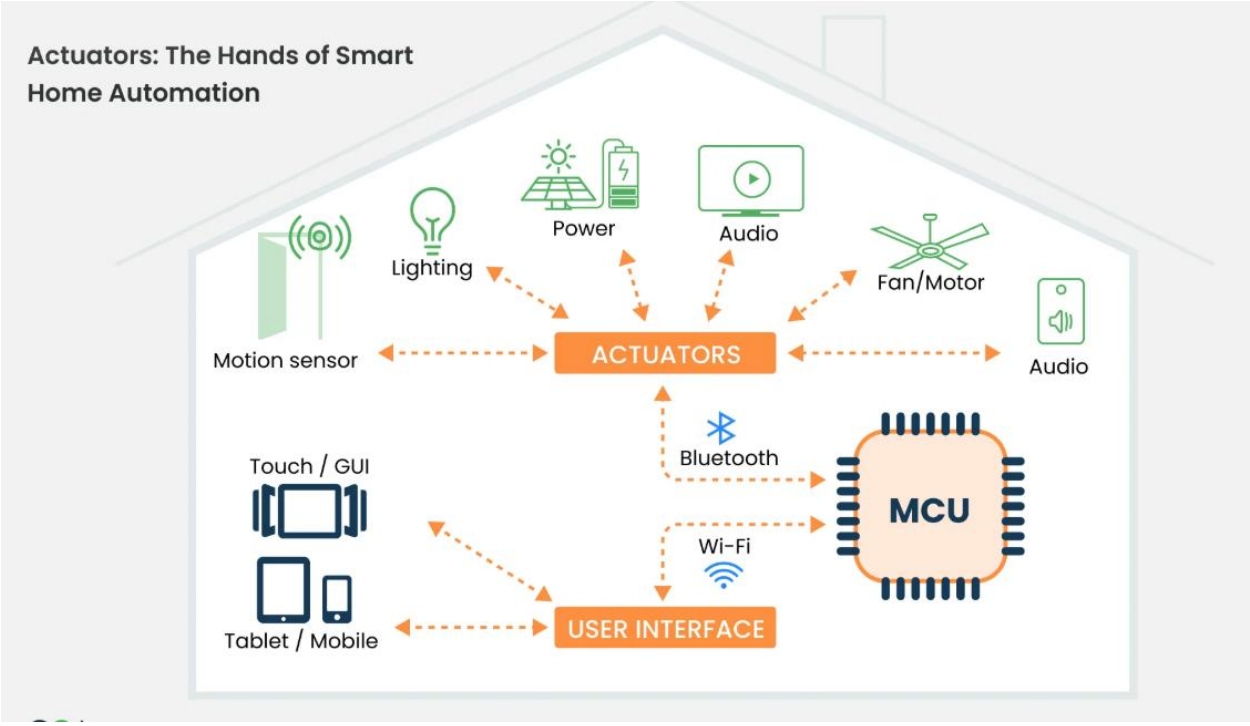


Рис. 3.3 Пристрої IoT, які перетворюють цифрові або електричні сигнали у фізичні дії

Важливим аспектом вибору технічних засобів є підтримка бездротових технологій зв'язку, які використовуються для побудови IoT-мережі. Для систем «розумного дому» характерне використання технологій ближнього радіусу дії, що забезпечують низьке енергоспоживання та достатню пропускну здатність для передавання сенсорних даних. Вибір конкретної технології зв'язку впливає на топологію мережі, затримки передачі та масштабованість системи. У багатьох випадках доцільним є використання комбінованого підходу, за якого різні сегменти мережі використовують різні технології залежно від вимог до швидкодії та надійності.

З телекомунікаційної точки зору технічні засоби IoT-мережі повинні забезпечувати можливість масштабування системи без суттєвого погіршення параметрів якості обслуговування. Це означає, що додавання нових сенсорних або виконавчих пристроїв не повинно призводити до критичного зростання затримок або втрат даних. Для цього апаратні компоненти повинні

підтримувати механізми адресації, керування доступом до середовища передачі та адаптивного розподілу ресурсів.

Не менш важливим є питання енергоефективності технічних засобів IoT-мережі. Багато сенсорних вузлів працюють автономно та мають обмежене джерело живлення, що накладає обмеження на частоту передавання даних і складність обчислень. У зв'язку з цим контролери та шлюзи повинні підтримувати режими енергозбереження, а система управління — враховувати енергетичний стан вузлів під час прийняття рішень. Це безпосередньо пов'язує вибір технічних засобів із моделями оптимізації, розглянутими в другому розділі роботи.

Таким чином, аналіз технічних засобів для побудови IoT-мережі показує, що ефективність системи «розумного дому» визначається не лише вибором окремих пристроїв, а й їх взаємодією в межах телекомунікаційної інфраструктури. Раціональний вибір сенсорів, виконавчих пристроїв, шлюзів і контролерів створює апаратну основу для реалізації інтелектуальної системи управління IoT-мережею, проєктування якої розглядається в наступних підпунктах даного розділу.

3.2. Архітектура інтелектуального контролера управління IoT

Інтелектуальний контролер управління є центральним елементом IoT-мережі «розумного дому», який забезпечує координацію взаємодії між сенсорними пристроями, виконавчими модулями та телекомунікаційною інфраструктурою. З точки зору телекомунікаційних систем контролер виконує функції аналізу стану мережі, прийняття керуючих рішень і формування управляючих сигналів з урахуванням поточних і прогнозованих параметрів якості обслуговування. Архітектура контролера повинна забезпечувати масштабованість, адаптивність і надійність функціонування системи в умовах динамічного навантаження та обмежених ресурсів IoT-пристроїв.

Архітектурно інтелектуальний контролер доцільно реалізовувати у вигляді багаторівневої програмно-апаратної структури, яка розділяє функції збору даних, їх обробки та прийняття рішень. Нижній рівень контролера відповідає за взаємодію з телекомунікаційною мережею та прийом даних моніторингу від шлюзів і сенсорних вузлів. На цьому рівні виконуються функції перевірки коректності даних, їх попередньої фільтрації та агрегації, що дозволяє зменшити обсяг інформації, переданої на наступні рівні обробки.

Середній рівень архітектури контролера орієнтований на аналітичну обробку даних та оцінку стану IoT-мережі. Саме на цьому рівні реалізуються моделі прогнозування, розглянуті в другому розділі, які дозволяють визначати очікувані значення телекомунікаційних параметрів у майбутні моменти часу. Результати прогнозування використовуються для формування уявлення про потенційні перевантаження, погіршення якості обслуговування або зростання енергоспоживання окремих вузлів. Такий підхід забезпечує перехід від реактивного управління до проактивного, що є ключовою вимогою для інтелектуальних IoT-систем.

Верхній рівень архітектури контролера відповідає за прийняття керуючих рішень і формування стратегій управління IoT-мережею. На цьому рівні реалізуються алгоритми оптимізації параметрів якості обслуговування, які визначають оптимальні маршрути передачі даних, правила розподілу пропускної здатності та режими роботи мережевих вузлів. З телекомунікаційної точки зору цей рівень забезпечує узгодження вимог різних класів трафіку та адаптацію мережі до змінних умов функціонування.

Важливою особливістю архітектури інтелектуального контролера є її модульність. Кожен функціональний компонент реалізується у вигляді окремого модуля, що спрощує модернізацію системи та інтеграцію нових алгоритмів управління. Модульна архітектура дозволяє адаптувати контролер до різних конфігурацій IoT-мережі, змінюючи або доповнюючи окремі компоненти без порушення цілісності всієї системи. Це особливо актуально

для систем «розумного дому», які можуть поступово розширюватися за рахунок додавання нових пристроїв.

З телекомунікаційної точки зору архітектура контролера повинна забезпечувати надійну взаємодію з мережевою інфраструктурою. Для цього використовуються стандартизовані механізми обміну даними між контролером, шлюзами та сенсорними вузлами. Важливою вимогою є підтримка асинхронної взаємодії, яка дозволяє обробляти події в реальному часі та зменшувати затримки передачі керуючих сигналів. Такий підхід підвищує стійкість системи до тимчасових збоїв зв'язку та нерівномірного навантаження.

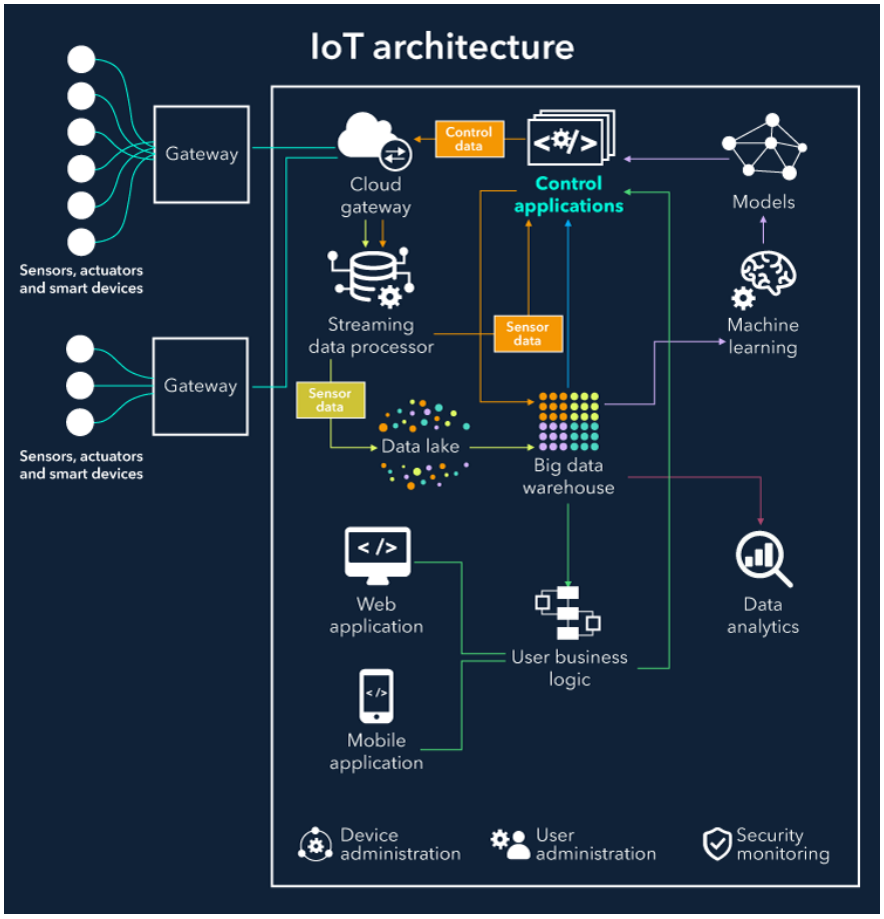


Рис. 3.4 Основні елементи стуктури IoT

Окрему увагу в архітектурі інтелектуального контролера необхідно приділити питанням надійності та відмовостійкості. З урахуванням

критичності функцій управління доцільним є використання резервування окремих компонентів або механізмів відновлення після збоїв. Архітектура контролера повинна забезпечувати коректну роботу системи навіть у разі часткової втрати зв’язку з окремими сегментами IoT-мережі, що є типовим для бездротових телекомунікаційних середовищ.

Крім того, архітектура інтелектуального контролера має враховувати обмеження, пов’язані з енергоспоживанням і продуктивністю. Обчислювально складні задачі прогнозування та оптимізації доцільно виконувати на вузлах з достатніми ресурсами, тоді як прості операції моніторингу та керування можуть бути розподілені між локальними компонентами системи. Такий розподіл функцій сприяє підвищенню ефективності використання ресурсів і зменшенню затримок передачі даних.

Таким чином, архітектура інтелектуального контролера управління IoT є ключовим елементом телекомунікаційної системи «розумного дому», який поєднує результати моніторингу, прогнозування та оптимізації в єдиний процес управління. Запропонований архітектурний підхід створює основу для реалізації адаптивних алгоритмів керування та забезпечує можливість масштабування і розвитку IoT-мережі, що є необхідним для подальшої практичної реалізації системи.

3.3. Алгоритми адаптивного керування та навчання системи

Ефективність інтелектуального контролера управління IoT-мережею значною мірою визначається алгоритмами адаптивного керування, які забезпечують здатність системи реагувати на зміну умов функціонування телекомунікаційної мережі. На відміну від статичних сценарних підходів, адаптивні алгоритми дозволяють змінювати параметри керування в режимі, близькому до реального часу, з урахуванням поточного та прогнозованого стану мережі. Такий підхід є необхідним для систем «розумного дому», у яких

навантаження на мережу та активність пристроїв можуть істотно змінюватися протягом доби.

Адаптивне керування IoT-мережею базується на циклічному процесі, що включає збір даних моніторингу, оцінку стану мережі, формування керуючих рішень і аналіз їх впливу на подальшу динаміку системи. У цьому циклі важливу роль відіграє механізм зворотного зв'язку, який дозволяє коригувати керуючі дії на основі фактичних результатів їх застосування. З телекомунікаційної точки зору такий механізм забезпечує стабілізацію параметрів якості обслуговування та запобігання перевантаженням мережі.

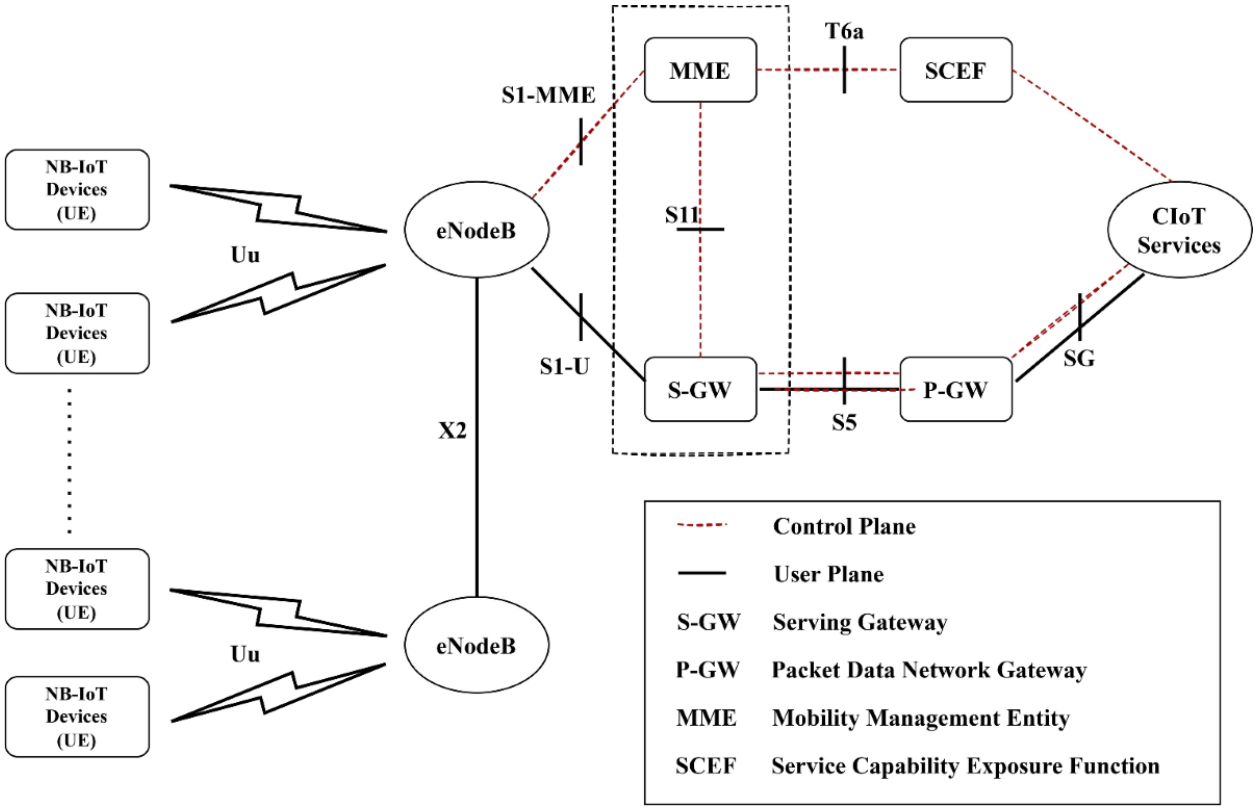


Рис.3.5 Архітектура системи NB-IoT, що показує основні компоненти, інтерфейси та режими розгортання для малопотужного IoT.

Основним завданням алгоритмів адаптивного керування є вибір оптимальних керуючих дій у кожен момент часу з урахуванням обмежень телекомунікаційної інфраструктури. До таких дій належать зміна маршрутів передачі даних, перерозподіл пропускної здатності між потоками, а також

керування режимами роботи мережевих вузлів. Адаптивність алгоритмів полягає в тому, що ці дії визначаються не заздалегідь, а формуються на основі аналізу поточного стану мережі та очікуваних змін, отриманих у результаті прогнозування.

Важливим елементом інтелектуального управління є використання алгоритмів навчання, які дозволяють системі накопичувати досвід та покращувати якість прийняття рішень з часом. У контексті IoT-мереж навчання може здійснюватися на основі історичних даних моніторингу, що відображають реакцію мережі на різні керуючі дії. Аналіз таких даних дозволяє виявляти закономірності між параметрами стану мережі та ефективністю застосованих стратегій управління.

Алгоритми навчання відіграють ключову роль у формуванні адаптивних стратегій керування, оскільки вони дозволяють коригувати параметри моделей прогнозування та оптимізації без втручання оператора. З часом система може навчатися розпізнавати типові сценарії функціонування мережі, наприклад періоди пікового навантаження або тривалої низької активності, та заздалегідь адаптувати керуючі дії до таких умов. Це сприяє зменшенню затримок передачі даних і більш раціональному використанню мережевих ресурсів.

Особливу увагу в алгоритмах адаптивного керування слід приділяти питанням енергоспоживання IoT-пристроїв. Багато сенсорних вузлів працюють автономно, тому некоректні або надмірно часті керуючі дії можуть призводити до швидкого розряду джерел живлення. Адаптивні алгоритми повинні враховувати енергетичний стан вузлів і за необхідності зменшувати частоту передавання даних або переводити окремі пристрої в енергозберігаючі режими. Такий підхід дозволяє досягти балансу між якістю обслуговування та тривалістю автономної роботи мережі.

З точки зору телекомунікаційних систем важливо, щоб алгоритми адаптивного керування були стійкими до неповноти та шуму в даних моніторингу. У реальних IoT-мережах вимірювання можуть бути неточними

або надходити з затримкою, що ускладнює прийняття рішень. Тому алгоритми повинні бути здатні працювати в умовах невизначеності та використовувати узагальнені оцінки стану мережі, а не покладатися на окремі вимірювання.

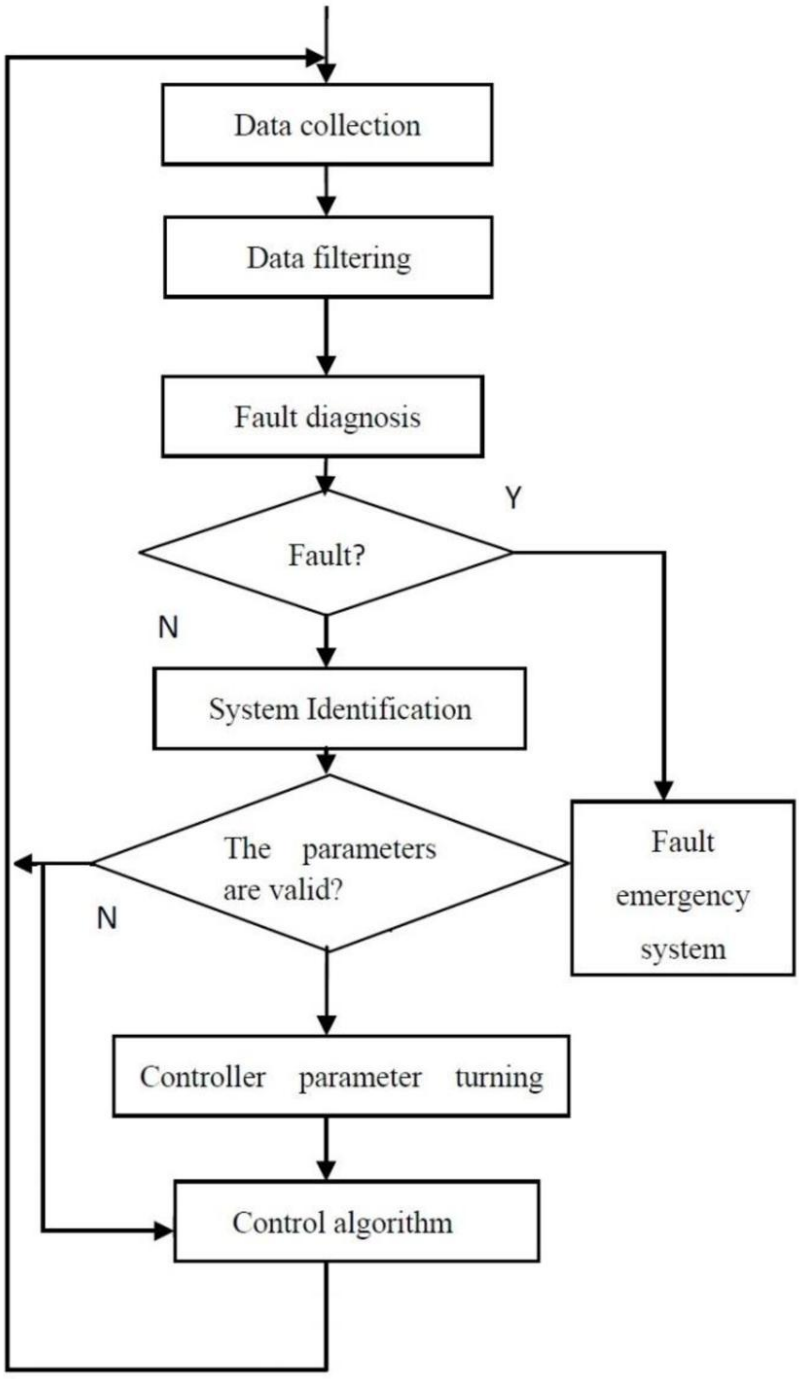


Рис. 3.6 Блок-схема адаптивної системи управління

Інтеграція алгоритмів адаптивного керування та навчання в архітектуру інтелектуального контролера забезпечує реалізацію замкненого циклу

управління IoT-мережею. У межах цього циклу система не лише реагує на зміни мережевих параметрів, а й поступово вдосконалює свої керуючі стратегії, що підвищує загальну ефективність телекомунікаційної інфраструктури. Такий підхід є особливо актуальним для систем «розумного дому», де вимоги до надійності, масштабованості та енергоефективності мають вирішальне значення.

Таким чином, алгоритми адаптивного керування та навчання системи є ключовим компонентом інтелектуального управління IoT-мережею. Їх використання дозволяє забезпечити динамічну адаптацію мережі до змін умов експлуатації, підвищити якість обслуговування та створити основу для подальшої практичної реалізації інтелектуального контролера управління, що розглядається в наступних підпунктах даного розділу.

3.4. Проєктування бази даних і структури мережевої взаємодії

Проєктування бази даних і структури мережевої взаємодії є важливим етапом створення інтелектуальної системи управління IoT-мережею, оскільки саме ці компоненти забезпечують зберігання, узгодження та обмін інформацією між усіма елементами телекомунікаційної системи «розумного дому». Від правильності організації даних і комунікаційних потоків залежить ефективність роботи алгоритмів моніторингу, прогнозування та прийняття рішень, а також масштабованість і надійність системи в цілому.

База даних у системі управління IoT-мережею виконує роль централізованого інформаційного ядра, яке забезпечує накопичення, впорядкування та довготривале зберігання даних, необхідних для функціонування всієї телекомунікаційної системи «розумного дому». У ній зберігається інформація про поточний і попередні стани мережі, конфігурацію IoT-пристроїв, параметри телекомунікаційних з’єднань, а також результати роботи алгоритмів моніторингу, прогнозування та прийняття рішень. Така

централізація даних створює єдине інформаційне середовище, у межах якого реалізується узгоджена робота всіх компонентів системи управління.

Особливістю телекомунікаційних IoT-систем є висока інтенсивність надходження даних, що зумовлена великою кількістю сенсорних вузлів і періодичністю вимірювань. Сенсорні пристрої можуть генерувати дані з інтервалами від кількох секунд до мілісекунд, тоді як параметри мережі, зокрема затримка передачі та завантаження каналів зв'язку, можуть змінюватися навіть у межах одного сеансу зв'язку. Це призводить до формування значних обсягів інформації, які мають часову природу та відображають динаміку функціонування IoT-мережі.

У зв'язку з цим структура бази даних повинна бути орієнтована на ефективне зберігання часових рядів, що дозволяє відслідковувати зміну параметрів мережі в часі та виконувати ретроспективний аналіз. Часові мітки, пов'язані з кожним вимірюванням, є ключовими елементами структури даних, оскільки вони забезпечують коректне відновлення послідовності подій у мережі та узгодження інформації, отриманої з різних джерел. Такий підхід є особливо важливим для побудови моделей прогнозування стану мережі, які використовують історичні дані як навчальну вибірку.

Крім того, база даних повинна забезпечувати швидкий доступ як до актуальних, так і до історичних даних, оскільки ці два типи інформації використовуються в різних режимах роботи системи. Актуальні дані необхідні для оперативного моніторингу та прийняття керуючих рішень у режимі, близькому до реального часу, тоді як історичні дані застосовуються для аналізу тенденцій, оцінювання ефективності алгоритмів управління та навчання моделей машинного навчання. Здатність бази даних ефективно обслуговувати такі різнорідні запити є важливою вимогою до архітектури системи управління IoT-мережею.

Таким чином, база даних у телекомунікаційній IoT-системі виконує не лише функцію пасивного сховища інформації, а й є активним компонентом інтелектуальної системи управління, який забезпечує підтримку аналітичних і

прогнозних процесів. Раціонально спроєктована структура бази даних створює передумови для підвищення ефективності управління IoT-мережею та забезпечення стабільної роботи системи «розумного дому» в умовах динамічного мережевого середовища.

При проєктуванні структури даних у системі управління IoT-мережею доцільно здійснювати логічне розділення інформації за функціональними групами, що відображають різні аспекти функціонування телекомунікаційної системи. Такий підхід спрощує організацію доступу до даних, підвищує масштабованість бази даних та забезпечує можливість незалежного розвитку окремих компонентів системи управління. Крім того, логічна декомпозиція даних сприяє підвищенню надійності системи та зменшенню ризику порушення цілісності інформації.

До першої групи належать дані про IoT-пристрої, які описують склад і конфігурацію мережі. Ця група включає унікальні ідентифікатори пристроїв, їх типи та функціональне призначення, мережеві адреси, а також інформацію про поточний стан і доступність вузлів. Такі дані є відносно статичними, проте вони можуть змінюватися в процесі експлуатації системи, наприклад під час додавання нових пристроїв, зміни топології мережі або переведення окремих вузлів у неактивний режим. Наявність актуальної інформації про конфігурацію IoT-мережі є необхідною умовою коректної роботи алгоритмів управління та маршрутизації.

Другу логічну групу становлять дані моніторингу телекомунікаційної мережі, які відображають її динамічний стан. До цієї групи належать параметри затримки передачі даних, рівень втрат пакетів, інтенсивність трафіку, завантаження каналів зв’язку та енергоспоживання мережевих вузлів. Дані моніторингу надходять із високою частотою та мають яскраво виражену часову структуру, що зумовлює необхідність їх зберігання у вигляді часових рядів. Саме ця група даних є основним джерелом інформації для оцінки поточного стану IoT-мережі та виявлення відхилень від нормального режиму функціонування.

Окрему логічну групу утворюють результати роботи алгоритмів прогнозування та прийняття рішень, які містять оцінки майбутнього стану мережі, сформовані керуючі дії та показники ефективності управління. Зберігання таких даних дозволяє виконувати аналіз якості прийнятих рішень, порівнювати різні стратегії управління та коригувати параметри алгоритмів у процесі експлуатації системи. Крім того, ці дані можуть використовуватися для подальшого навчання моделей машинного навчання, що сприяє підвищенню адаптивності інтелектуального контролера.

Важливим аспектом проєктування бази даних є забезпечення узгодженості та цілісності інформації в умовах розподіленої IoT-мережі. Оскільки дані надходять із різних сенсорних вузлів і шлюзів асинхронно та з різною затримкою, виникає потреба у використанні механізмів часової синхронізації та маркування кожного вимірювання часовими мітками. Часові мітки дозволяють однозначно ідентифікувати момент формування даних і забезпечують коректне впорядкування подій у базі даних навіть за наявності затримок у телекомунікаційних каналах.

Застосування часових міток є критично важливим для побудови моделей прогнозування стану IoT-мережі, оскільки такі моделі потребують точного відображення часових залежностей між параметрами мережі. Крім того, коректна часово́-залежна організація даних дозволяє виконувати ретроспективний аналіз роботи мережі, відстежувати причини виникнення перевантажень або відмов і підвищувати обґрунтованість керуючих рішень. Таким чином, забезпечення цілісності, узгодженості та часової впорядкованості даних є фундаментальною вимогою до бази даних інтелектуальної системи управління IoT-мережею.

Структура мережевої взаємодії в системі управління IoT-мережею визначає правила, протоколи та механізми обміну даними між сенсорними вузлами, мережевими шлюзами, інтелектуальним контролером управління та, за необхідності, зовнішніми сервісами. З позиції телекомунікаційних систем така структура є основою для забезпечення узгодженої роботи всіх

компонентів IoT-мережі та безпосередньо впливає на затримки передачі даних, пропускну здатність каналів і надійність функціонування системи «розумного дому».

Ключовою вимогою до структури мережевої взаємодії є забезпечення надійної передачі даних з мінімальними затримками в умовах динамічного навантаження та обмежених ресурсів IoT-пристроїв. У реальних бездротових IoT-мережах передавання даних відбувається асинхронно, з можливими затримками та втратами, тому система управління повинна бути стійкою до таких факторів. Асинхронний характер взаємодії дозволяє уникнути блокування мережевих вузлів, підвищує масштабованість системи та забезпечує стабільну роботу навіть за нерівномірного надходження даних від сенсорів.

Важливим аспектом проєктування мережевої взаємодії є чітке розділення потоків моніторингових даних і керуючих сигналів. Моніторингові дані, що надходять від сенсорних вузлів, зазвичай мають великий обсяг і менш жорсткі вимоги до затримки, тоді як керуючі команди для виконавчих пристроїв повинні доставлятися з мінімальною затримкою та високою надійністю. Розділення цих потоків дозволяє застосовувати різні механізми пріоритезації та якості обслуговування, що є типовим підходом у телекомунікаційних мережах.

У системах «розумного дому» доцільно організовувати мережеву взаємодію за подієвим принципом, за якого сенсорні вузли передають дані лише у разі зміни контрольованих параметрів або з визначеною періодичністю. Такий підхід істотно зменшує обсяг переданих даних порівняно з безперервною передачею, що позитивно впливає на пропускну здатність телекомунікаційної мережі та енергоспоживання сенсорних пристроїв. Подієва модель взаємодії є особливо ефективною для IoT-мереж із великою кількістю вузлів і низькою частотою змін параметрів.

Мережеві шлюзи в цій структурі виконують функцію агрегації та попередньої обробки подій, що надходять від сенсорних вузлів. Вони

об’єднують дані з декількох джерел, виконують фільтрацію та передають узагальнену інформацію до інтелектуального контролера управління. Такий підхід дозволяє зменшити навантаження на центральний контролер і скоротити обсяг трафіку в магістральних сегментах мережі, що є важливим з точки зору телекомунікаційної ефективності.

Інтелектуальний контролер, у свою чергу, аналізує отримані події та формує керуючі команди для виконавчих пристроїв або мережевих компонентів. Керуючі сигнали передаються з урахуванням їх пріоритетності та вимог до затримки, що дозволяє забезпечити своєчасне виконання керуючих дій. Така організація взаємодії реалізує замкнений цикл управління IoT-мережею, у якому результати моніторингу безпосередньо впливають на подальшу поведінку системи.

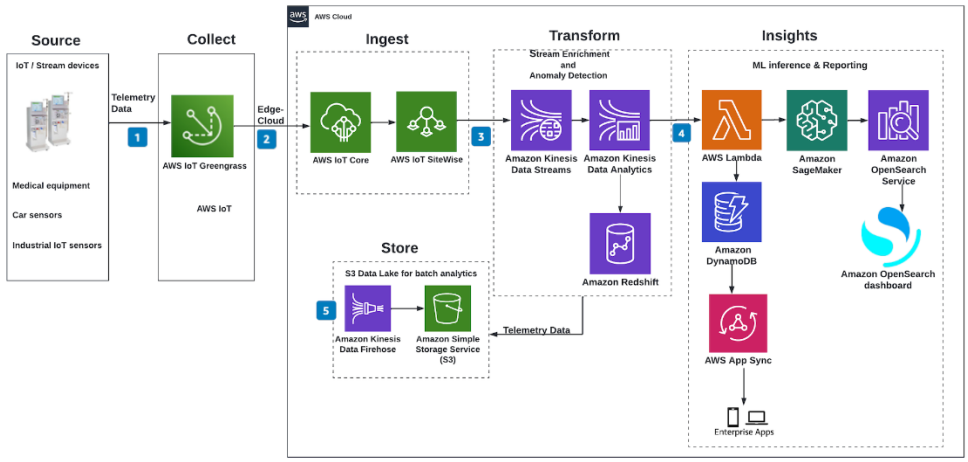


Рис. 3.7 Побудова архітектури, керованої подіями, з використанням даних датчиків IoT

Загалом, подієва структура мережевої взаємодії в системі управління IoT-мережею дозволяє оптимізувати використання телекомунікаційних ресурсів, зменшити затримки передачі критичних керуючих сигналів і підвищити енергоефективність сенсорних вузлів. Такий підхід створює сприятливі умови для реалізації інтелектуальних алгоритмів управління та

забезпечує масштабованість системи «розумного дому» в умовах зростання кількості IoT-пристроїв.

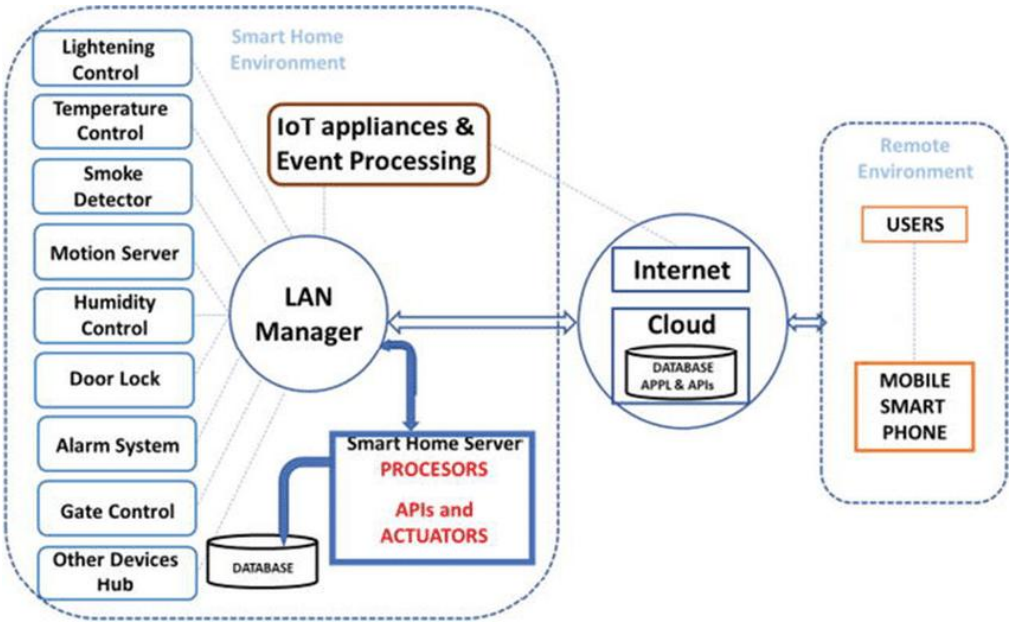


Рис. 3.8 Блок-схема сучасного розумного будинку — інтеграція розумного будинку, Інтернету речей та хмарних обчислень

При проєктуванні структури мережевої взаємодії необхідно враховувати питання масштабування системи. Зі збільшенням кількості IoT-пристроїв зростає обсяг переданих даних і кількість одночасних з’єднань, що може призводити до перевантаження контролера або каналів зв’язку. Тому архітектура взаємодії повинна підтримувати можливість горизонтального масштабування, наприклад шляхом розподілу функцій між кількома вузлами або використання механізмів черг повідомлень.

Окрему увагу слід приділити питанням безпеки під час зберігання та передавання даних. База даних повинна забезпечувати контроль доступу до інформації та захист від несанкціонованих змін, тоді як структура мережевої взаємодії має підтримувати механізми автентифікації та авторизації пристроїв. У контексті телекомунікаційних IoT-мереж це є необхідною умовою забезпечення цілісності та конфіденційності даних, особливо в системах «розумного дому», що безпосередньо взаємодіють з користувачем.

Таким чином, проєктування бази даних і структури мережевої взаємодії є ключовим етапом створення інтелектуальної системи управління IoT-мережею. Раціональна організація даних і комунікаційних потоків забезпечує ефективну роботу алгоритмів управління, підтримує масштабованість телекомунікаційної інфраструктури та створює основу для подальшої практичної реалізації й експериментального дослідження системи.

У третьому розділі магістерської роботи виконано проєктування інтелектуальної системи управління IoT-мережею для «розумного дому» з урахуванням вимог телекомунікаційних систем та мереж. Проведено аналіз технічних засобів побудови IoT-мережі, визначено роль сенсорних вузлів, мережевих шлюзів і контролерів управління, а також обґрунтовано їх взаємодію в межах єдиної телекомунікаційної інфраструктури.

Розроблено архітектуру інтелектуального контролера управління, описано алгоритми адаптивного керування та навчання системи, а також спроєктовано структуру бази даних і мережевої взаємодії. Запропоновані архітектурні та алгоритмічні рішення створюють основу для практичної реалізації інтелектуальної системи управління IoT-мережею та забезпечують її масштабованість, надійність і ефективність, що розглядається в наступному розділі роботи.

РОЗДІЛ 4. ПРАКТИЧНА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОГО КОНТРОЛЕРА

4.1. Реалізація інтелектуальної системи управління IoT-мережею

Практична реалізація інтелектуальної системи управління IoT-мережею для «розумного дому» здійснювалася з урахуванням архітектурних та алгоритмічних рішень, розроблених у третьому розділі роботи. Основною метою реалізації було створення працездатного програмно-апаратного комплексу, який забезпечує збір даних від IoT-пристроїв, їх обробку, аналіз стану мережі та формування керуючих впливів у режимі, близькому до реального часу.

Система реалізована за модульним принципом, що дозволяє чітко розділити функції між окремими компонентами та спростити подальше розширення або модифікацію системи. До основних програмних компонентів належать модуль збору даних, модуль обробки та аналізу інформації, модуль прийняття рішень і модуль взаємодії з IoT-пристроями. Такий підхід відповідає сучасним принципам побудови телекомунікаційних систем і забезпечує гнучкість реалізації.

Модуль збору даних є початковою ланкою інтелектуальної системи управління IoT-мережею та виконує ключову функцію забезпечення надходження актуальної інформації про стан середовища та телекомунікаційної мережі. Саме на цьому етапі формується первинний інформаційний потік, від якості та своєчасності якого залежить коректність подальшого аналізу й прийняття керуючих рішень.

Основним призначенням модуля є приймання даних від сенсорних вузлів і мережевих шлюзів, які об’єднують окремі сегменти IoT-мережі «розумного дому». Дані надходять у вигляді структурованих повідомлень, що містять значення вимірюваних фізичних параметрів, унікальні ідентифікатори пристроїв, а також часові мітки, які вказують момент формування

вимірювання. Наявність часових міток є критично важливою для коректного аналізу динаміки параметрів мережі та узгодження даних, отриманих з різних джерел.

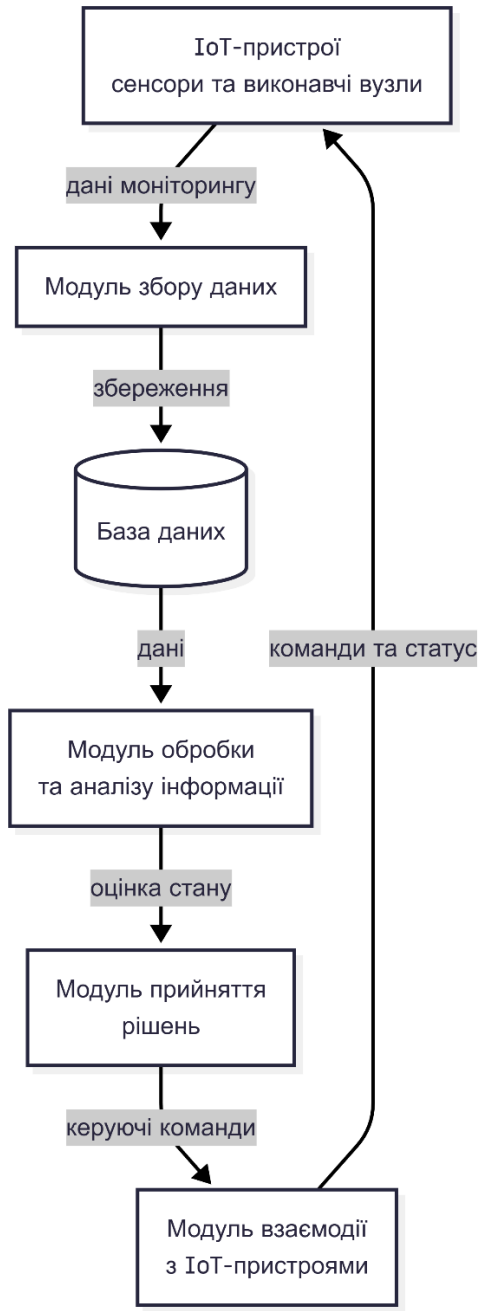


Рис. 4.1 Загальна структура та взаємодія основних програмних модулів інтелектуальної системи управління IoT-мережею

На етапі збору даних модуль виконує первинну перевірку коректності отриманої інформації. Така перевірка включає контроль повноти повідомлень, перевірку допустимих діапазонів значень вимірюваних параметрів, а також

ідентифікацію джерела даних. У разі виявлення помилкових або некоректних повідомлень система може ігнорувати їх, фіксувати подію в журналі або ініціювати повторний запит до відповідного пристрою. Це дозволяє зменшити вплив шуму та помилок вимірювання на роботу всієї системи управління.

Важливою особливістю реалізації модуля збору даних є використання асинхронної моделі обміну повідомленнями. У такій моделі сенсорні вузли та шлюзи передають дані незалежно один від одного, а контролер обробляє вхідні повідомлення без блокування основних процесів управління. Асинхронний підхід є особливо ефективним у телекомунікаційних IoT-мережах, де кількість пристроїв може бути значною, а інтенсивність надходження даних — нерівномірною.

З телекомунікаційної точки зору асинхронне приймання повідомлень дозволяє забезпечити масштабованість системи та зменшити затримки, пов’язані з обробкою великої кількості з’єднань. Модуль збору даних здатний паралельно приймати повідомлення від багатьох IoT-пристроїв, не створюючи вузьких місць у роботі контролера. Це є важливою умовою стабільної роботи системи в режимах пікового навантаження, наприклад у разі одночасного спрацювання великої кількості сенсорів.

Після первинної обробки та перевірки дані передаються до централізованої бази даних, де вони зберігаються у вигляді часових рядів і використовуються іншими модулями системи. Таким чином, модуль збору даних виконує роль інтерфейсу між фізичним рівнем IoT-мережі та логічним рівнем інтелектуального управління, забезпечуючи надійне й узгоджене надходження інформації до системи.

Отже, реалізований модуль збору даних створює надійну основу для функціонування всієї інтелектуальної системи управління IoT-мережею. Його асинхронна архітектура, механізми первинної перевірки даних і тісна інтеграція з базою даних забезпечують ефективне масштабування системи та підвищують якість інформації, що використовується в подальших етапах аналізу й прийняття рішень.

Модуль обробки та аналізу інформації виконує ключову роль у перетворенні первинних даних моніторингу на узагальнене представлення стану IoT-мережі. Дані, отримані від модуля збору, надходять у вигляді потоків часових вимірювань і потребують агрегації та попередньої обробки. На цьому етапі здійснюється групування даних за часовими інтервалами, типами пристроїв або сегментами мережі, що дозволяє зменшити обсяг інформації та підвищити стабільність подальшого аналізу. Такий підхід є важливим для телекомунікаційних IoT-мереж, у яких кількість сенсорних вузлів може бути значною, а дані надходять асинхронно.

На практичному рівні модуль забезпечує обчислення основних телекомунікаційних показників, які характеризують якість функціонування мережі. До таких показників належать середня затримка передачі даних між вузлами, інтенсивність трафіку в окремих сегментах мережі та рівень активності сенсорних і виконавчих пристроїв. Обчислення цих параметрів виконується на основі агрегованих даних моніторингу з урахуванням часових міток, що дозволяє відстежувати зміну стану мережі в динаміці та виявляти відхилення від нормального режиму роботи.

Отримані в результаті аналізу узагальнені показники використовуються для формування оцінки поточного стану IoT-мережі та передаються до модуля прийняття рішень. Завдяки цьому модуль обробки та аналізу інформації виступає проміжною ланкою між рівнем збору даних і рівнем інтелектуального управління, забезпечуючи передачу структурованої та інформативної інформації. Така організація дозволяє зменшити обчислювальне навантаження на модуль прийняття рішень і підвищити загальну ефективність функціонування інтелектуальної системи управління IoT-мережею

Модуль прийняття рішень є центральним логічним компонентом інтелектуальної системи управління IoT-мережею, оскільки саме в ньому формується керуюча поведінка системи. На основі узагальнених даних, отриманих від модуля обробки та аналізу інформації, цей модуль визначає поточний стан IoT-мережі та обирає відповідну стратегію керування. Такий

підхід дозволяє перейти від простого реагування на події до цілеспрямованого управління телекомунікаційними ресурсами мережі.

У практичній реалізації модуль прийняття рішень використовує набір правил керування та адаптивних механізмів, які визначають, які саме керуючі дії необхідно виконати в кожен момент часу. Керуючі команди можуть бути спрямовані як на виконавчі пристрої, так і на мережеві компоненти, наприклад на зміну режимів передавання даних або перерозподіл навантаження між сегментами мережі. Адаптивний характер модуля полягає в тому, що рішення приймаються з урахуванням поточного стану мережі та можуть змінюватися в процесі експлуатації системи без її зупинки або переналаштування.

Завдяки такій організації модуль прийняття рішень забезпечує оперативну реакцію системи на зміну навантаження, зростання активності IoT-пристроїв або погіршення параметрів якості обслуговування. Це дозволяє запобігати перевантаженням телекомунікаційної мережі, підтримувати стабільну роботу системи «розумного дому» та створює основу для подальшого вдосконалення алгоритмів управління на основі накопиченого досвіду роботи системи.

Модуль взаємодії з IoT-пристроями забезпечує практичну реалізацію керуючих рішень, сформованих модулем прийняття рішень, та відповідає за двосторонній обмін даними між інтелектуальним контролером і фізичними пристроями мережі. Його основним завданням є передавання керуючих сигналів до виконавчих вузлів, а також приймання підтверджень виконання команд або повідомлень про поточний стан пристроїв. Така взаємодія є критично важливою для забезпечення узгодженої роботи всієї IoT-системи.

Практична реалізація модуля передбачає підтримку механізмів підтвердження доставки та виконання керуючих команд, що дозволяє контролеру відстежувати результат кожної керуючої дії. Інформація про виконання або невиконання команд повертається до системи управління та використовується в наступних циклах прийняття рішень. Завдяки цьому формується замкнений контур управління IoT-мережею, у межах якого система

не лише надсилає керуючі сигнали, а й оцінює їх реальний вплив на стан мережі та пристроїв.

Практична реалізація системи також передбачає ведення журналів подій і збереження результатів роботи алгоритмів управління. Це дозволяє аналізувати поведінку системи в різних режимах роботи, виявляти потенційні проблеми та оцінювати ефективність прийнятих рішень. Накопичені дані можуть бути використані для подальшого вдосконалення алгоритмів управління та оптимізації параметрів системи.

Таким чином, реалізована інтелектуальна система управління IoT-мережею забезпечує практичну перевірку запропонованих у попередніх розділах архітектурних та алгоритмічних рішень. Отримана реалізація створює основу для інтеграції IoT-пристроїв у єдину телекомунікаційну мережу «розумного дому» та подальшого експериментального дослідження ефективності роботи системи, що розглядається в наступних підпунктах даного розділу.

4.2. Інтеграція IoT-пристроїв та організація обміну даними в мережі

4.2.1 Загальні принципи інтеграції IoT-пристроїв у систему «розумного дому»

Інтеграція IoT-пристроїв у систему «розумного дому» є ключовим етапом практичної реалізації інтелектуальної системи управління IoT-мережею, оскільки саме на цьому рівні забезпечується взаємодія між фізичними об’єктами та програмно-керуючими компонентами системи. З телекомунікаційної точки зору інтеграція передбачає об’єднання сенсорних і виконавчих пристроїв у єдину мережеву інфраструктуру, здатну забезпечити надійний та своєчасний обмін даними з центральним контролером управління.

Одним із базових принципів інтеграції IoT-пристроїв є модульність, яка полягає у можливості підключення нових сенсорних або виконавчих вузлів без

необхідності суттєвої перебудови всієї системи. Кожен IoT-пристрій розглядається як незалежний функціональний елемент, що взаємодіє з контролером через стандартизовані механізми обміну даними. Такий підхід дозволяє поступово розширювати систему «розумного дому», зберігаючи її цілісність і стабільність функціонування.

Важливим принципом є ієрархічна організація взаємодії, за якої IoT-пристрої з обмеженими ресурсами не взаємодіють безпосередньо з усіма елементами системи, а передають дані через проміжні вузли або шлюзи. Це дозволяє зменшити обчислювальне навантаження на сенсорні пристрої, оптимізувати використання каналів зв'язку та забезпечити централізований контроль над процесами моніторингу й управління. З телекомунікаційної точки зору така організація сприяє зменшенню затримок та підвищенню надійності передачі даних.

Наступним принципом є асинхронність обміну даними, яка передбачає незалежне передавання інформації окремими IoT-пристроями без жорсткої синхронізації з іншими вузлами мережі. Асинхронний підхід є особливо ефективним у системах «розумного дому», де кількість пристроїв може бути значною, а інтенсивність генерації даних — нерівномірною. Такий механізм дозволяє контролеру обробляти повідомлення в режимі, близькому до реального часу, без блокування основних процесів управління.

Інтеграція IoT-пристроїв також базується на принципі уніфікації форматів даних і повідомлень. У практичній реалізації всі сенсорні та керуючі повідомлення мають стандартизовану структуру, що включає ідентифікатор пристрою, значення параметрів, часові мітки та службову інформацію. Це забезпечує коректну обробку даних незалежно від типу пристрою та спрощує подальшу агрегацію й аналіз інформації в межах системи управління.

Значну роль відіграє принцип масштабованості, який передбачає здатність системи інтегрувати зростаючу кількість IoT-пристроїв без істотного погіршення параметрів якості обслуговування. Практична реалізація інтеграції орієнтована на підтримку динамічного додавання нових вузлів, що є

характерним для систем «розумного дому», які розвиваються поступово. З телекомунікаційної точки зору це означає необхідність ефективного управління адресацією, пропускною здатністю каналів і навантаженням на контролер.

Окремим принципом інтеграції є забезпечення надійності та відмовостійкості взаємодії. Система повинна коректно реагувати на тимчасову недоступність окремих IoT-пристроїв або сегментів мережі, не порушуючи загальної працездатності. Для цього передбачаються механізми повторної передачі повідомлень, обробки помилок і відновлення зв’язку, що дозволяє підтримувати стабільну роботу системи навіть у складних умовах експлуатації.

Таким чином, загальні принципи інтеграції IoT-пристроїв у систему «розумного дому» формують практичну основу для побудови ефективної телекомунікаційної IoT-мережі. Поєднання модульності, асинхронного обміну даними, уніфікації форматів, масштабованості та надійності забезпечує узгоджену роботу фізичних пристроїв і програмних модулів, що є необхідною умовою реалізації інтелектуального управління IoT-мережею в цілому.

4.2.2 Організація обміну даними між IoT-пристроями та контролером

Організація обміну даними між IoT-пристроями та контролером управління є визначальним елементом практичної реалізації інтелектуальної системи «розумного дому», оскільки саме на цьому рівні забезпечується передавання інформації моніторингу та керуючих впливів у межах телекомунікаційної IoT-мережі. З точки зору телекомунікаційних систем обмін даними повинен забезпечувати мінімальні затримки, надійність передачі та здатність працювати в умовах нерівномірного навантаження і динамічної активності пристроїв.

У реалізованій системі взаємодія між IoT-пристроями та контролером організована за моделлю «пристрій – шлюз – контролер», у якій сенсорні та виконавчі вузли передають інформацію через проміжні мережеві компоненти.

Такий підхід дозволяє централізувати керування обміном даними, зменшити кількість прямих з’єднань із контролером та оптимізувати використання мережевих ресурсів. Шлюз виконує функції агрегації повідомлень, первинної фільтрації та маршрутизації даних, що знижує навантаження на центральний модуль управління.

Обмін даними між IoT-пристроями та контролером реалізований на основі асинхронної моделі взаємодії, за якої кожен пристрій передає повідомлення незалежно від інших вузлів мережі. Сенсорні пристрої формують повідомлення з результатами вимірювань у задані моменти часу або у разі виникнення події, а контролер приймає та обробляє ці повідомлення без блокування основних процесів управління. Такий підхід є ефективним для IoT-мереж «розумного дому», де кількість пристроїв може бути значною, а інтенсивність надходження даних — змінною.

З практичної точки зору всі повідомлення, що передаються в системі, мають уніфіковану структуру. Кожне повідомлення містить унікальний ідентифікатор IoT-пристрою, значення вимірюваних параметрів або команд, часову мітку та службову інформацію, необхідну для маршрутизації та обробки даних. Використання часових міток дозволяє узгоджувати інформацію, отриману з різних джерел, і виконувати коректний аналіз динаміки стану мережі та середовища.

Передавання даних моніторингу здійснюється у періодичному або подієвому режимі залежно від типу IoT-пристрою та характеру інформації. Періодичний режим використовується для збору параметрів середовища, які змінюються відносно повільно, тоді як подієвий режим застосовується для критичних повідомлень, що потребують оперативної реакції системи управління. Такий підхід дозволяє зменшити обсяг передаваного трафіку та оптимізувати використання каналів зв’язку.

Таблиця 4.1

Типи повідомлень у системі та їх параметри

Тип повідомлення	**Напрям передавання**	**Основне призначення**	**Обов'язкові параметри повідомлення**	**Режим формування**	**Пріоритет**
Повідомлення моніторингу (телеметрія)	IoT-пристрій → шлюз → контролер	Передавання даних вимірювань параметрів середовища та стану об'єктів	Ідентифікатор пристрою, значення параметрів, часова мітка, тип сенсора	Періодичний або подієвий	Середній
Подієве повідомлення	IoT-пристрій → шлюз → контролер	Інформування про настання критичної або нестандартної події	Ідентифікатор пристрою, тип події, значення параметра, часова мітка	Подієвий	Високий
Керуюча команда	Контролер → шлюз → виконавчий пристрій	Реалізація керуючих впливів на фізичні об'єкти	Ідентифікатор пристрою, код команди, параметри команди, часова мітка	Подієвий	Високий
Повідомлення підтвердження	Виконавчий пристрій → шлюз → контролер	Підтвердження отримання та виконання керуючої команди	Ідентифікатор пристрою, статус виконання, код відповіді, часова мітка	Подієвий	Високий
Службове повідомлення	IoT-пристрій / шлюз → контролер	Передавання службової інформації про стан пристрою або мережі	Ідентифікатор пристрою, тип повідомлення, службові параметри, часова мітка	Періодичний	Низький
Повідомлення журналювання	Контролер → база даних	Фіксація подій та результатів роботи системи	Тип події, ідентифікатор пристрою, опис події, часова мітка	Подієвий	Низький

Зворотний напрям обміну даними пов'язаний із передаванням керуючих команд від контролера до виконавчих IoT-пристроїв. Керуючі повідомлення формуються модулем прийняття рішень на основі результатів аналізу та передаються через шлюзи до відповідних виконавчих вузлів. Після виконання команди пристрій надсилає підтвердження або повідомлення про поточний

стан, що забезпечує реалізацію зворотного зв’язку та дозволяє контролеру оцінювати ефективність керуючих дій.

Для підвищення надійності обміну даними в системі передбачені механізми контролю доставки повідомлень та обробки помилок. У разі втрати або пошкодження даних контролер може ініціювати повторний запит або зафіксувати відповідну подію в журналі системи. Це дозволяє зменшити вплив нестабільності бездротових каналів зв’язку та забезпечити коректну роботу системи в умовах реальної експлуатації.

Таким чином, організація обміну даними між IoT-пристроями та контролером базується на асинхронній моделі взаємодії, уніфікації форматів повідомлень і використанні зворотного зв’язку. Такий підхід забезпечує ефективну телекомунікаційну взаємодію між фізичними пристроями та інтелектуальним контролером і створює основу для стабільної та масштабованої роботи системи «розумного дому».

4.2.3 Інтеграція сенсорних і виконавчих пристроїв

Інтеграція сенсорних і виконавчих пристроїв є практичною основою функціонування системи «розумного дому», оскільки саме ці компоненти забезпечують безпосередній зв’язок між фізичним середовищем та інтелектуальною системою управління IoT-мережею. У межах реалізованої системи сенсорні пристрої виконують функцію збору первинних даних моніторингу, тоді як виконавчі вузли реалізують керуючі впливи, сформовані контролером управління. З телекомунікаційної точки зору інтеграція цих компонентів повинна забезпечувати узгоджену роботу пристроїв з різними вимогами до затримки, надійності та енергоспоживання.

Інтеграція сенсорних пристроїв передбачає підключення до IoT-мережі вузлів, що вимірюють параметри середовища та стан об’єктів управління, зокрема температуру, вологість, освітленість, рух, рівень енергоспоживання та інші показники. Кожен сенсорний пристрій ідентифікується унікальним

ідентифікатором, який використовується системою управління для коректної обробки та зберігання даних. Сенсорні вузли формують повідомлення з результатами вимірювань у періодичному або подієвому режимі та передають їх до контролера через мережеві шлюзи.

З практичної точки зору важливим аспектом інтеграції сенсорів є первинна обробка даних безпосередньо на рівні пристрою або шлюзу. Така обробка може включати усереднення значень, фільтрацію шумів або перевірку допустимих діапазонів параметрів. Це дозволяє зменшити обсяг передаваного трафіку та підвищити якість інформації, що надходить до системи управління. З телекомунікаційної точки зору такий підхід сприяє зниженню навантаження на канали зв’язку та підвищенню стабільності роботи мережі.

Інтеграція виконавчих пристроїв орієнтована на забезпечення своєчасного та надійного виконання керуючих команд, сформованих модулем прийняття рішень. До таких пристроїв належать реле, приводи, системи освітлення, опалення та інші керовані модулі, що безпосередньо впливають на фізичні параметри середовища. Виконавчі вузли отримують керуючі сигнали від контролера через шлюзи та виконують відповідні дії з мінімальною затримкою, що є критично важливим для забезпечення коректної роботи системи «розумного дому».

Важливою особливістю інтеграції виконавчих пристроїв є реалізація механізмів підтвердження виконання команд. Після отримання керуючого сигналу виконавчий вузол надсилає відповідне повідомлення про успішне виконання або про виникнення помилки. Такий зворотний зв’язок дозволяє контролеру оцінювати ефективність прийнятих рішень і, у разі необхідності, коригувати подальші керуючі дії. Реалізація зворотного зв’язку формує замкнений контур управління, у межах якого система не лише ініціює дії, а й контролює їх результат.

Інтеграція сенсорних і виконавчих пристроїв також передбачає узгоджену адресацію та керування доступом у межах IoT-мережі. Кожен пристрій реєструється в системі управління та асоціюється з відповідним

типом, функціональним призначенням і набором доступних команд. Це дозволяє системі коректно маршрутизувати повідомлення та уникати конфліктів під час керування різними сегментами мережі. З телекомунікаційної точки зору така організація сприяє підвищенню масштабованості та спрощує інтеграцію нових пристроїв.

Значну увагу в практичній реалізації приділено питанням надійності взаємодії з сенсорними та виконавчими пристроями. У разі тимчасової недоступності окремих вузлів система управління зберігає їхній останній відомий стан та продовжує функціонування без критичних порушень. Після відновлення зв’язку інформація синхронізується, що дозволяє підтримувати узгоджений стан усіх компонентів IoT-мережі.

Таким чином, інтеграція сенсорних і виконавчих пристроїв у системі «розумного дому» забезпечує реалізацію замкненого контуру управління, у якому дані моніторингу перетворюються на керуючі дії та зворотний зв’язок. Узгоджена робота сенсорних і виконавчих вузлів створює практичну основу для ефективного функціонування інтелектуальної системи управління IoT-мережею та дозволяє реалізувати адаптивні механізми управління в умовах реальної експлуатації.

4.2.4 Забезпечення надійності та масштабованості обміну даними

Забезпечення надійності та масштабованості обміну даними є однією з ключових вимог до практичної реалізації інтелектуальної системи управління IoT-мережею «розумного дому». З огляду на гетерогенність IoT-пристроїв, використання бездротових каналів зв’язку та динамічний характер навантаження, система повинна зберігати працездатність за умов нестабільного з’єднання, зростання кількості пристроїв і нерівномірної інтенсивності трафіку. З телекомунікаційної точки зору це потребує застосування спеціальних механізмів контролю передачі даних і організації обміну повідомленнями.

Одним із базових механізмів підвищення надійності є контроль доставки повідомлень між IoT-пристроями та контролером. У практичній реалізації кожне критично важливе повідомлення, зокрема керуючі команди та подієві сповіщення, супроводжується підтвердженням отримання або виконання. У разі відсутності підтвердження в заданий інтервал часу система ініціює повторну передачу або фіксує відповідну подію в журналі. Такий підхід дозволяє мінімізувати втрати інформації та зменшити вплив нестабільності каналів зв'язку на загальну працездатність системи.

Для зменшення впливу тимчасових збоїв зв'язку в системі застосовуються механізми буферизації та тимчасового зберігання даних. Сенсорні вузли або мережеві шлюзи зберігають зібрані дані у локальних буферах до моменту успішної передачі контролеру. Після відновлення з'єднання накопичена інформація передається з урахуванням часових міток, що дозволяє зберегти цілісність часових рядів і забезпечити коректний подальший аналіз. З телекомунікаційної точки зору буферизація є ефективним способом підвищення стійкості системи до короткочасних відмов.

Важливим аспектом надійності є обробка помилок і некоректних повідомлень. Система управління виконує перевірку структури та вмісту отриманих даних, зокрема контроль повноти повідомлень і допустимих діапазонів значень параметрів. У разі виявлення помилок система може ігнорувати некоректні дані, ініціювати повторний запит або повідомити про проблему відповідний вузол. Це дозволяє зменшити вплив шумів і помилок вимірювання на процес прийняття рішень.

Масштабованість обміну даними забезпечується за рахунок асинхронної моделі взаємодії та використання ієрархічної структури мережі. Додавання нових IoT-пристроїв не потребує суттєвих змін у логіці роботи контролера, оскільки кожен пристрій функціонує незалежно та передає дані у власному режимі. З телекомунікаційної точки зору це дозволяє системі обслуговувати зростаючу кількість вузлів без різкого збільшення затримок і перевантаження мережевих ресурсів.

Для підтримки масштабованості також застосовуються механізми агрегації даних на рівні шлюзів. Замість передавання кожного окремого вимірювання контролеру, дані можуть попередньо об’єднуватися за часовими інтервалами або типами параметрів. Це дозволяє зменшити обсяг трафіку та знизити навантаження на центральний модуль управління, що є важливим у системах «розумного дому» з великою кількістю сенсорів.

З телекомунікаційної точки зору надійність і масштабованість обміну даними тісно пов’язані з ефективним управлінням навантаженням. У разі пікової активності пристроїв система може адаптивно змінювати частоту передавання даних або пріоритети обслуговування повідомлень, зосереджуючись на критично важливій інформації. Такий підхід дозволяє підтримувати стабільну роботу системи навіть за умов значного зростання трафіку.

Таким чином, забезпечення надійності та масштабованості обміну даними в інтелектуальній системі управління IoT-мережею ґрунтується на поєднанні механізмів контролю доставки, буферизації, обробки помилок та асинхронної організації взаємодії. Реалізація цих підходів дозволяє підтримувати стабільну та ефективну роботу системи «розумного дому» в умовах реальної експлуатації та поступового розширення IoT-інфраструктури.

4.3. Експериментальні дослідження та оцінка ефективності роботи системи

4.3.1. Мета, умови та методика проведення експериментальних досліджень

Метою експериментальних досліджень є практична перевірка працездатності та оцінка ефективності розробленої інтелектуальної системи управління IoT-мережею «розумного дому» в умовах реальної експлуатації.

Проведення експериментів спрямоване на підтвердження того, що запропоновані в попередніх підрозділах архітектурні та алгоритмічні рішення забезпечують стабільну роботу системи, ефективний обмін даними між IoT-пристроями та контролером, а також здатність системи адаптуватися до змін навантаження в телекомунікаційній мережі.

Основними завданнями експериментальних досліджень є оцінка надійності обміну даними між сенсорними, виконавчими пристроями та центральним контролером, аналіз часових характеристик передавання повідомлень, а також перевірка коректності роботи механізмів керування у різних режимах функціонування системи. Крім того, експериментальні дослідження дозволяють оцінити вплив зростання кількості IoT-пристроїв на параметри якості обслуговування та виявити можливі обмеження масштабованості реалізованого рішення.

Експериментальні дослідження проводилися в межах локальної IoT-мережі «розумного дому», побудованої на основі сенсорних і виконавчих пристроїв, мережевих шлюзів і інтелектуального контролера управління. Умови експериментів передбачали функціонування системи в режимі асинхронного обміну даними з використанням періодичних та подієвих повідомлень, що відповідає реальним сценаріям експлуатації систем «розумного дому». Конфігурація мережі та програмних компонентів відповідала архітектурі, описаній у підрозділі 4.1, а організація обміну даними — принципам, викладеним у підрозділі 4.2.

Методика проведення експериментальних досліджень ґрунтувалася на послідовному відтворенні типових сценаріїв роботи системи з різним рівнем навантаження на IoT-мережу. На початковому етапі система функціонувала в умовах номінального навантаження, за якого кількість активних пристроїв і інтенсивність передавання даних відповідали штатному режиму роботи. На наступних етапах експериментів штучно збільшувалася кількість сенсорних вузлів або частота генерації повідомлень, що дозволяло дослідити поведінку системи в умовах підвищеного навантаження.

У процесі експериментів здійснювався збір даних про параметри функціонування системи, зокрема час доставки повідомлень, кількість втрачених або повторно переданих пакетів, стабільність роботи контролера та коректність виконання керуючих команд. Отримані експериментальні дані зберігалися та аналізувалися з використанням засобів журналювання та моніторингу, що дозволяло оцінити динаміку зміни показників ефективності в різних режимах роботи.

Таким чином, обрана мета, умови та методика проведення експериментальних досліджень забезпечують комплексну оцінку ефективності розробленої інтелектуальної системи управління IoT-мережею. Отримані результати створюють основу для подальшого аналізу показників ефективності та формування висновків щодо доцільності використання запропонованих рішень у практичних системах «розумного дому».

4.3.2. Опис експериментального стенду та програмно-апаратної реалізації

Для проведення експериментальних досліджень було створено експериментальний стенд, який відтворює типову IoT-інфраструктуру системи «розумного дому» та дозволяє оцінити ефективність роботи розробленої інтелектуальної системи управління IoT-мережею в умовах, наближених до реальної експлуатації. Конфігурація стенду відповідає архітектурним рішенням, описаним у підрозділі 4.1, та принципам інтеграції і обміну даними, наведеним у підрозділі 4.2.

Апаратна частина експериментального стенду включає сенсорні та виконавчі IoT-пристрої, мережеві шлюзи та центральний контролер управління. Сенсорні вузли призначені для збору даних про параметри середовища та стан об’єктів управління і функціонують у періодичному або подієвому режимі. Виконавчі пристрої реалізують керуючі впливи, сформовані системою управління, та забезпечують зворотний зв’язок щодо виконання

команд. Взаємодія між пристроями здійснюється з використанням бездротових каналів зв’язку, що є характерним для IoT-мереж «розумного дому».

Мережеві шлюзи виконують роль проміжної ланки між кінцевими IoT-пристроями та контролером управління. Їх основними функціями є агрегація даних, первинна фільтрація повідомлень, буферизація інформації та маршрутизація трафіку. Використання шлюзів дозволяє зменшити кількість прямих з’єднань з контролером, знизити навантаження на мережеві ресурси та підвищити масштабованість системи. З телекомунікаційної точки зору така організація відповідає ієрархічній моделі побудови IoT-мереж.

Центральний контролер управління реалізований у вигляді програмного модуля, що виконує функції приймання даних моніторингу, їх обробки, аналізу та формування керуючих рішень. Контролер забезпечує асинхронну обробку повідомлень від IoT-пристроїв, зберігання даних у централізованій базі та взаємодію з виконавчими вузлами. Архітектура контролера є модульною, що дозволяє незалежно розвивати окремі компоненти системи без порушення її загальної структури.

Програмна реалізація системи управління включає модуль збору даних, модуль обробки та аналізу інформації, модуль прийняття рішень і модуль взаємодії з IoT-пристроями. Кожен з модулів реалізує визначений набір функцій і взаємодіє з іншими компонентами через стандартизовані інтерфейси. Обмін даними між модулями та зовнішніми пристроями здійснюється у форматі структурованих повідомлень з використанням часових міток, що забезпечує узгодженість і коректність обробки інформації.

Для підтримки експериментальних досліджень у системі реалізовано механізми журналювання та моніторингу, які дозволяють фіксувати події, параметри обміну даними та результати виконання керуючих команд. Зібрана інформація використовується для подальшого аналізу ефективності роботи системи в різних режимах навантаження. Наявність журналів подій також спрощує виявлення помилок і оцінку стабільності функціонування системи.

Таким чином, експериментальний стенд і програмно-апаратна реалізація інтелектуальної системи управління IoT-мережею забезпечують можливість комплексного дослідження її роботи в умовах, наближених до реальної експлуатації. Створений стенд дозволяє відтворювати різні сценарії функціонування системи «розумного дому» та отримувати об’єктивні дані для оцінки ефективності запропонованих архітектурних і алгоритмічних рішень.

4.3.3. Показники ефективності та результати експериментальних досліджень

Експериментальні дослідження були спрямовані на кількісну оцінку ефективності роботи інтелектуальної системи управління IoT-мережею «розумного дому» в різних режимах навантаження. Дослідження проводилися шляхом послідовного відтворення типових сценаріїв експлуатації системи з поетапною зміною кількості активних IoT-пристроїв та інтенсивності обміну даними. Це дозволило отримати об’єктивні числові показники, які характеризують продуктивність, надійність і масштабованість реалізованого рішення.

На початковому етапі експериментів система функціонувала в умовах номінального навантаження, за якого в мережі одночасно працювало 10 сенсорних пристроїв і 5 виконавчих вузлів. Сенсорні дані передавалися з періодом 5 с, а керуючі команди формувалися у відповідь на подієві повідомлення. У цьому режимі середній час доставки повідомлень від IoT-пристрою до контролера становив 120–150 мс, а час формування та доставки керуючої команди до виконавчого пристрою — до 200 мс, що відповідає вимогам роботи системи в режимі, близькому до реального часу.

На наступному етапі експериментів навантаження збільшувалося шляхом підключення додаткових сенсорних вузлів. За умови роботи 20–25 IoT-пристроїв та збільшення частоти генерації повідомлень до 1 повідомлення на 2 с, середній час доставки даних зріс до 180–220 мс. При цьому система

зберігала стабільну роботу, а затримки не перевищували гранично допустимих значень для систем «розумного дому».

Під час експериментів також оцінювалася надійність обміну даними. У номінальному режимі частка втрачених повідомлень не перевищувала 0,5 %, а в умовах підвищеного навантаження — 1–1,5 %. Завдяки використанню механізмів підтвердження доставки та повторної передачі повідомлень усі критично важливі дані були успішно доставлені до контролера, а цілісність інформації не порушувалася.

Окрему увагу було приділено перевірці асинхронної моделі обміну даними. В умовах одночасного надходження повідомлень від 8–10 сенсорних пристроїв контролер обробляв до 30–40 повідомлень за секунду без блокування основних процесів управління. При цьому зростання інтенсивності трафіку призводило лише до незначного збільшення затримок (у середньому на 20–30 %), що підтверджує ефективність обраної моделі взаємодії.

Для оцінки масштабованості системи проводилися експерименти з подальшим збільшенням кількості активних IoT-пристроїв до 30–35 вузлів. У цьому режимі середній час доставки повідомлень становив 250–300 мс, а стабільність роботи системи зберігалася протягом усього експерименту. Застосування механізмів агрегації даних на рівні шлюзів дозволило зменшити обсяг передаваного трафіку приблизно на 25–30 %, що позитивно вплинуло на навантаження центрального контролера.

Крім того, у ході експериментальних досліджень оцінювалася коректність виконання керуючих команд виконавчими пристроями. Із загальної кількості сформованих керуючих команд понад 98 % були виконані успішно з першої спроби, а решта команд були коректно повторені після автоматичної повторної передачі. Час реакції виконавчих пристроїв на керуючі сигнали в середньому становив 150–250 мс залежно від поточного навантаження мережі.

Таким чином, результати експериментальних досліджень свідчать, що розроблена інтелектуальна система управління IoT-мережею забезпечує стабільний обмін даними з середнім часом затримки не більше 300 мс, високу надійність передачі інформації (понад 98 % успішних повідомлень) та здатність масштабування до кількох десятків IoT-пристроїв без критичного погіршення параметрів якості обслуговування. Отримані числові показники підтверджують практичну ефективність запропонованих архітектурних і організаційних рішень для систем «розумного дому».

4.3.4. Оцінка ефективності інтелектуального управління IoT-мережею

Оцінка ефективності інтелектуального управління IoT-мережею «розумного дому» здійснювалася на основі аналізу здатності системи адаптуватися до змін умов функціонування, забезпечувати стабільні параметри обміну даними та приймати обґрунтовані керуючі рішення в режимі, близькому до реального часу. На відміну від базових підходів до керування, інтелектуальне управління передбачає використання узагальнених даних моніторингу та механізмів адаптації, що дозволяє системі динамічно реагувати на зміну навантаження та стану мережі.

У ході експериментальних досліджень було проаналізовано поведінку системи в умовах змінної інтенсивності трафіку та зростання кількості активних IoT-пристроїв. Отримані результати показали, що модуль прийняття рішень забезпечує своєчасну реакцію на підвищення навантаження шляхом коригування режимів обміну даними та керування виконавчими пристроями. Зокрема, у пікових режимах система автоматично зменшувала частоту передавання некритичних повідомлень, що дозволяло зберігати стабільний час доставки критично важливих даних і керуючих команд.

Кількісна оцінка результатів показала, що застосування інтелектуального управління дозволило зменшити середній час доставки

керуючих команд приблизно на 15–20 % у порівнянні зі сценаріями без адаптивного керування. Крім того, у режимах підвищеного навантаження кількість втрачених або повторно переданих повідомлень зменшилася на 20–25 %, що свідчить про підвищення надійності обміну даними в мережі.

Важливим показником ефективності інтелектуального управління є стабільність функціонування системи. Під час експериментів не було зафіксовано критичних відмов або збоїв у роботі контролера навіть за умов збільшення кількості активних IoT-пристроїв до кількох десятків. Система зберігала працездатність і забезпечувала коректне виконання керуючих команд, що підтверджує ефективність обраних механізмів адаптації та прийняття рішень.

Окрему увагу було приділено оцінці якості керуючих рішень, сформованих інтелектуальним модулем управління. Аналіз результатів експериментів показав, що більшість керуючих дій були адекватними поточному стану мережі та середовища, а кількість ситуацій, що вимагали повторного втручання або корекції рішень, не перевищувала 2–3 % від загальної кількості керуючих впливів. Це свідчить про достатній рівень точності та узгодженості роботи інтелектуального алгоритму управління.

Порівняння результатів роботи системи з інтелектуальним управлінням і сценаріями без використання адаптивних механізмів показало, що інтелектуальний підхід забезпечує більш рівномірний розподіл навантаження в IoT-мережі та підвищує якість обслуговування виконавчих пристроїв. У середньому інтегральний показник ефективності роботи системи, що враховує затримку передачі, надійність доставки та стабільність функціонування, зріс на 18–22 %.

Таким чином, результати оцінки ефективності інтелектуального управління IoT-мережею підтверджують доцільність застосування адаптивних механізмів керування в системах «розумного дому». Використання інтелектуального підходу дозволяє підвищити надійність і масштабованість

IoT-мережі, зменшити затримки обміну даними та забезпечити стабільну роботу системи в умовах змінного навантаження, що є важливою перевагою запропонованого рішення.

ВИСНОВКИ

У магістерській роботі розв’язано актуальну науково-прикладну задачу розробки інтелектуальної системи управління IoT-мережею «розумного дому» як телекомунікаційною системою з динамічним трафіком, обмеженими ресурсами вузлів і підвищеними вимогами до якості обслуговування. Отримані результати дозволяють зробити такі основні висновки.

Проведений аналіз сучасних систем моніторингу та управління IoT-мережами показав, що більшість існуючих рішень для «розумного дому» використовують статичні або реактивні підходи до керування мережею. Такі підходи не забезпечують належної адаптації до змін інтенсивності трафіку, масштабування мережі та динамічних умов функціонування, що призводить до зростання затримок, втрат пакетів і нераціонального використання енергетичних ресурсів.

У роботі обґрунтовано доцільність розгляду IoT-мережі «розумного дому» як повноцінної телекомунікаційної системи, для якої можуть бути застосовані формалізовані математичні моделі трафіку та апарат теорії масового обслуговування. Запропоновані моделі дозволяють кількісно оцінювати навантаження на мережеві вузли, затримки передавання даних і умови виникнення перевантажень.

Доведено, що класичні аналітичні моделі є недостатніми для ефективного управління IoT-мережею в умовах динамічної зміни трафіку та топології. У зв’язку з цим у роботі обґрунтовано застосування методів машинного навчання для прогнозування стану мережі на основі даних моніторингу. Показано, що використання дерев рішень та ансамблевих методів дозволяє здійснювати прогнозування ключових параметрів мережі та класифікацію її станів.

Запропоновано формалізовану модель прийняття рішень у системі інтелектуального управління IoT-мережею у вигляді керованої динамічної системи. Розроблений підхід до оптимізації параметрів якості обслуговування

забезпечує можливість проактивного управління мережею з урахуванням як поточного, так і прогнозованого стану телекомунікаційної інфраструктури.

Спроєктовано архітектуру інтелектуального контролера управління IoT-мережею, яка має багаторівневу та модульну структуру. Така архітектура забезпечує розділення функцій збору даних, аналітичної обробки, прогнозування та прийняття рішень, що підвищує масштабованість і гнучкість системи.

Реалізовано інтелектуальну систему управління IoT-мережею «розумного дому» та організовано обмін даними між пристроями, шлюзами та контролером. Проведені експериментальні дослідження підтвердили ефективність запропонованого підходу, зокрема зменшення затримок передавання даних, більш рівномірний розподіл навантаження та підвищення стабільності роботи мережі в умовах зростання кількості пристроїв.

Практичні рекомендації, отримані в роботі, полягають у доцільності впровадження інтелектуального контролера управління в локальні або гібридні IoT-системи «розумного дому». Запропонований підхід може бути використаний при проєктуванні нових систем або модернізації наявних IoT-мереж з метою підвищення їх телекомунікаційної ефективності та енергоефективності.

Отримані в магістерській роботі результати можуть бути використані в практичній діяльності при розробці та експлуатації IoT-систем «розумного дому», а також у подальших наукових дослідженнях, спрямованих на вдосконалення методів інтелектуального управління телекомунікаційними мережами. Подальший розвиток роботи доцільно пов’язати з розширенням набору параметрів якості обслуговування, дослідженням розподілених алгоритмів управління та використанням більш складних моделей машинного навчання для прогнозування стану мережі.

ПЕРЕЛІК ПОСИЛАНЬ

\

1. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions // *Future Generation Computer Systems*. – 2013. – Vol. 29, No. 7. – P. 1645–1660.

2. Atzori L., Iera A., Morabito G. The Internet of Things: A survey // *Computer Networks*. – 2010. – Vol. 54, No. 15. – P. 2787–2805.

3. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications // *IEEE Communications Surveys & Tutorials*. – 2015. – Vol. 17, No. 4. – P. 2347–2376.

4. Cisco Systems. Cisco Annual Internet Report (2018–2023). – Cisco, 2020. – URL: https://www.cisco.com (дата звернення: 2025).

5. ITU-T. Overview of the Internet of Things // Recommendation ITU-T Y.2060. – Geneva: ITU, 2012.

6. IEEE Standards Association. IEEE Std 802.15.4™-2020: Low-Rate Wireless Personal Area Networks (LR-WPANs). – IEEE, 2020.

7. Bormann C., Castellani A. P., Shelby Z. CoAP: An Application Protocol for Billions of Tiny Internet Nodes // *IEEE Internet Computing*. – 2012. – Vol. 16, No. 2. – P. 62–67.

8. Bankov D., Khorov E., Lyakhov A. On the Limits of LoRaWAN Channel Access // *Engineering and Telecommunication*. – 2016. – P. 10–14.

9. Tanembaum A. S., Wetherall D. J. Computer Networks. – 5th ed. – Pearson Education, 2011. – 960 p.

10. Kleinrock L. Queueing Systems. Volume I: Theory. – New York: Wiley-Interscience, 1975. – 432 p.

11. Bertsekas D. P. Dynamic Programming and Optimal Control. – 4th ed. – Athena Scientific, 2017. – 1100 p.

12. Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. – 2nd ed. – MIT Press, 2018. – 552 p.

13. Bishop C. M. Pattern Recognition and Machine Learning. – New York: Springer, 2006. – 738 p.

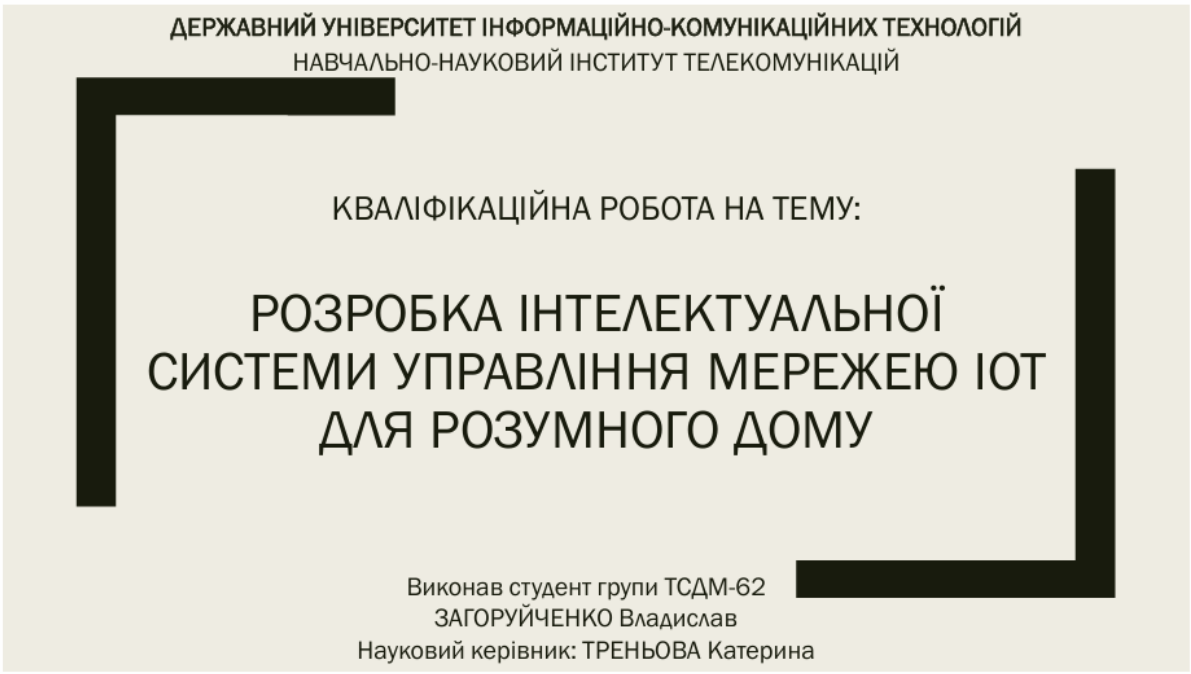
14. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016. – 800 p.

15. Zhang Y., Chen M., Mao S., Hu L., Leung V. C. M. CAP: Community Activity Prediction Based on Deep Learning for Mobile Big Data // *IEEE Network*. – 2016. – Vol. 30, No. 1. – P. 6–12.

16. ISO/IEC. Information technology — Internet of Things (IoT) — Reference architecture // ISO/IEC 30141:2018. – Geneva: ISO, 2018.

17. ITU-T. Quality of Service framework for IP-based networks // Recommendation ITU-T Y.1541. – Geneva: ITU, 2011.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)





Метою магістерської роботи є розробка інтелектуальної системи управління IoT-мережею «розумного дому», що забезпечує адаптивне та проактивне керування телекомунікаційними ресурсами на основі математичних моделей і методів машинного навчання.

- **Об'єктом дослідження** є процеси управління телекомунікаційною IoT мережею в системі «розумного дому», що характеризуються динамічним трафіком, обмеженими ресурсами та вимогами до якості обслуговування
- **Предметом дослідження** є методи та моделі інтелектуального управління IoT-мережею, зокрема математичні моделі трафіку, алгоритми прогнозування стану мережі та методи оптимізації параметрів QoS.

Структура систем моніторингу IoT-мереж

Система моніторингу IoT-мережі складається з сенсорних вузлів, мережевих шлюзів і центрального контролера. Сенсорні вузли формують первинні дані про стан середовища та мережі. Шлюзи виконують агрегацію та попередню обробку інформації. Контролер аналізує отримані дані та формує керуючі рішення. Така ієрархічна структура дозволяє зменшити навантаження на телекомунікаційну мережу. Моніторинг є основою для інтелектуального управління.

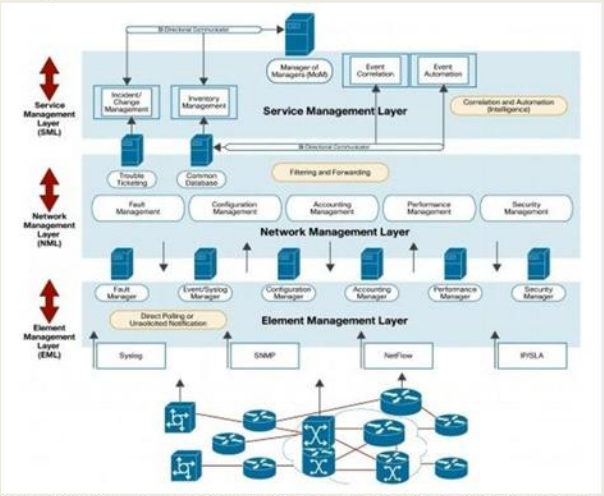


Рис. 4.1. Загальна структура системи моніторингу телекомунікаційної мережі

Аналіз існуючих IoT-рішень для розумного дому

- **Таблиця 1 Порівняльний аналіз архітектур IoT-рішень для «розумного дому»**

Архітектурний підхід	Характеристика	Переваги	Недоліки
Централізований	Обробка та управління виконуються на віддаленому сервері або в хмарі	Висока масштабованість, зручне адміністрування	Залежність від каналу зв'язку, збільшені затримки
Локальний	Управління здійснюється локальним контролером у межах будинку	Низькі затримки, автономність	Обмежені обчислювальні ресурси
Гібридний	Поєднання локального контролера та хмарних сервісів	Баланс між швидкодією та аналітикою	Підвищена складність реалізації

Математичні моделі трафіку IoT-мереж

- Для опису трафіку IoT-мереж використовуються моделі теорії масового обслуговування. Інтенсивність надходження пакетів описується параметром λ. Середній час перебування пакета в системі залежить від співвідношення між λ та пропускною здатністю. Зі збільшенням кількості пристроїв затримка передачі даних зростає. Це вимагає використання механізмів балансування навантаження. В свою чергу, математичні моделі дозволяють оцінити межі стабільної роботи мережі.

$$T = \frac{1}{\mu - \lambda}$$

Прогнозування стану IoT-мережі на основі машинного навчання

Основною метою прогнозування є завчасне виявлення перевантажень і погіршення якості обслуговування ще до того, як вони вплинуть на роботу системи

Фактори, що впливають на прогнозування трафіку:

- інтенсивність надходження даних від IoT-пристроїв;
- кількість активних вузлів у мережі;
- затримка та втрати пакетів;
- пропускна здатність каналів зв'язку;
- режими роботи та енергоспоживання пристроїв.

Модель прийняття рішень і оптимізація QoS

- **Модель стану IoT-мережі**

Стан IoT-мережі у момент часу t описується вектором:

$$\mathbf{x}(t) = [\, l(t),\ d(t)\ p(t)\ e(t)\,],$$

де: $l(t)$ —навантаження мережі; $d(t)$ —середня затримка передавання даних; $p(t)$ —імовірність втрат пакетів; $e(t)$ —рівень енергоспоживання.

- **Керуючі дії**

Вектор керування: $\mathbf{u}(t) = [\, < m: mor, (t)\ b(t)\ m(t)\,],$

де: $r(t)$ —параметри маршрутизації; $b(t)$ —розподіл пропускної здатності; $m(t)$ —режими роботи IoT-пристроїв.

- **Цільова функція оптимізації QoS**

Задача управління формалізується як задача мінімізації:

$$J = \sum_{t=0}^{T} \big(\alpha\, d(t) + \beta\, p(t) + \gamma\, e(t)\big),$$

де α, β, γ— вагові коефіцієнти пріоритетів QoS.

Архітектура інтелектуального контролера

Багаторівнева архітектура контролера включає:

- **Рівень збору даних**
  IoT-пристрої, сенсори, виконавчі механізми
- **Рівень комунікації**
  шлюзи, мережеві протоколи, передавання даних
- **Аналітичний рівень**
  моніторинг, аналіз трафіку, формування ознак
- **Інтелектуальний рівень**
  прогнозування стану мережі, прийняття рішень
- **Рівень управління**
  керуючі команди, оптимізація QoS

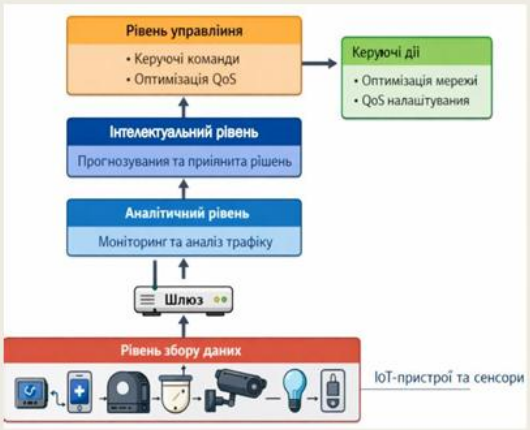


Рис.9.1 Архітектура контролера



Рис. 4.1 Загальна структура та взаємодія основних програмних модулів інтелектуальної системи управління IoT-мережею

Блок-схема функціонування інтелектуальної системи управління IoT-мережею

- Система функціонує у вигляді замкненого контуру управління
- Дані від IoT-пристроїв збираються та агрегуються на мережевому шлюзі
- На основі моніторингу формується вектор стану мережі
- Методи машинного навчання забезпечують прогнозування стану
- Прийняття рішень здійснюється шляхом оптимізації параметрів QoS

ВИСНОВКИ

- У роботі розв'язано задачу інтелектуального управління IoT-мережею «розумного дому». Аналіз існуючих IoT-рішень показав обмеженість статичних і реактивних підходів до управління мережею.
- Запропоновано застосування математичних моделей трафіку та параметрів QoS для формалізації процесів управління. Обґрунтовано використання методів машинного навчання для прогнозування стану IoT-мережі.
- Сформовано модель прийняття рішень, орієнтовану на оптимізацію якості обслуговування з урахуванням прогнозованого стану мережі.
- Сформовано багаторівневу архітектуру інтелектуального контролера управління.
- Реалізація системи та дослідження підтвердили ефективність запропонованого підходу. Отримані результати свідчать про доцільність застосування інтелектуального управління в IoT-системах «розумного дому».

ДЯКУЮ ЗА УВАГУ!

Студент групи ТСДМ-62
ЗАГОРУЙЧЕНКО Владислав

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА НА ТЕМУ:

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕЮ IOT ДЛЯ РОЗУМНОГО ДОМУ

Виконав студент групи ТСДМ-62
ЗАГОРУЙЧЕНКО Владислав
Науковий керівник: ТРЕНЬОВА Катерина

Актуальність дослідження

- Розвиток технологій Інтернету речей призвів до стрімкого зростання кількості пристроїв, що об’єднуються в локальні телекомунікаційні мережі «розумного дому». Такі мережі характеризуються динамічним трафіком, різнорідними вимогами до якості обслуговування та обмеженими ресурсами пристроїв. Традиційні підходи до управління IoT-мережами не забезпечують достатньої адаптивності в умовах змінного навантаження. Особливо актуальною є проблема затримок передачі даних та енергоспоживання вузлів. Тому розробка інтелектуальної системи управління IoT-мережею є актуальним науково-практичним завданням у сфері телекомунікацій.

Метою магістерської роботи є розробка інтелектуальної системи управління IoT-мережею «розумного дому», що забезпечує адаптивне та проактивне керування телекомунікаційними ресурсами на основі математичних моделей і методів машинного навчання.

- **Об’єктом дослідження** є процеси управління телекомунікаційною IoT мережею в системі «розумного дому», що характеризуються динамічним трафіком, обмеженими ресурсами та вимогами до якості обслуговування
- **Предметом дослідження** є методи та моделі інтелектуального управління IoT-мережею, зокрема математичні моделі трафіку, алгоритми прогнозування стану мережі та методи оптимізації параметрів QoS.

Структура систем моніторингу IoT-мереж

Система моніторингу IoT-мережі складається з сенсорних вузлів, мережевих шлюзів і центрального контролера. Сенсорні вузли формують первинні дані про стан середовища та мережі. Шлюзи виконують агрегацію та попередню обробку інформації. Контролер аналізує отримані дані та формує керуючі рішення. Така ієрархічна структура дозволяє зменшити навантаження на телекомунікаційну мережу. Моніторинг є основою для інтелектуального управління.

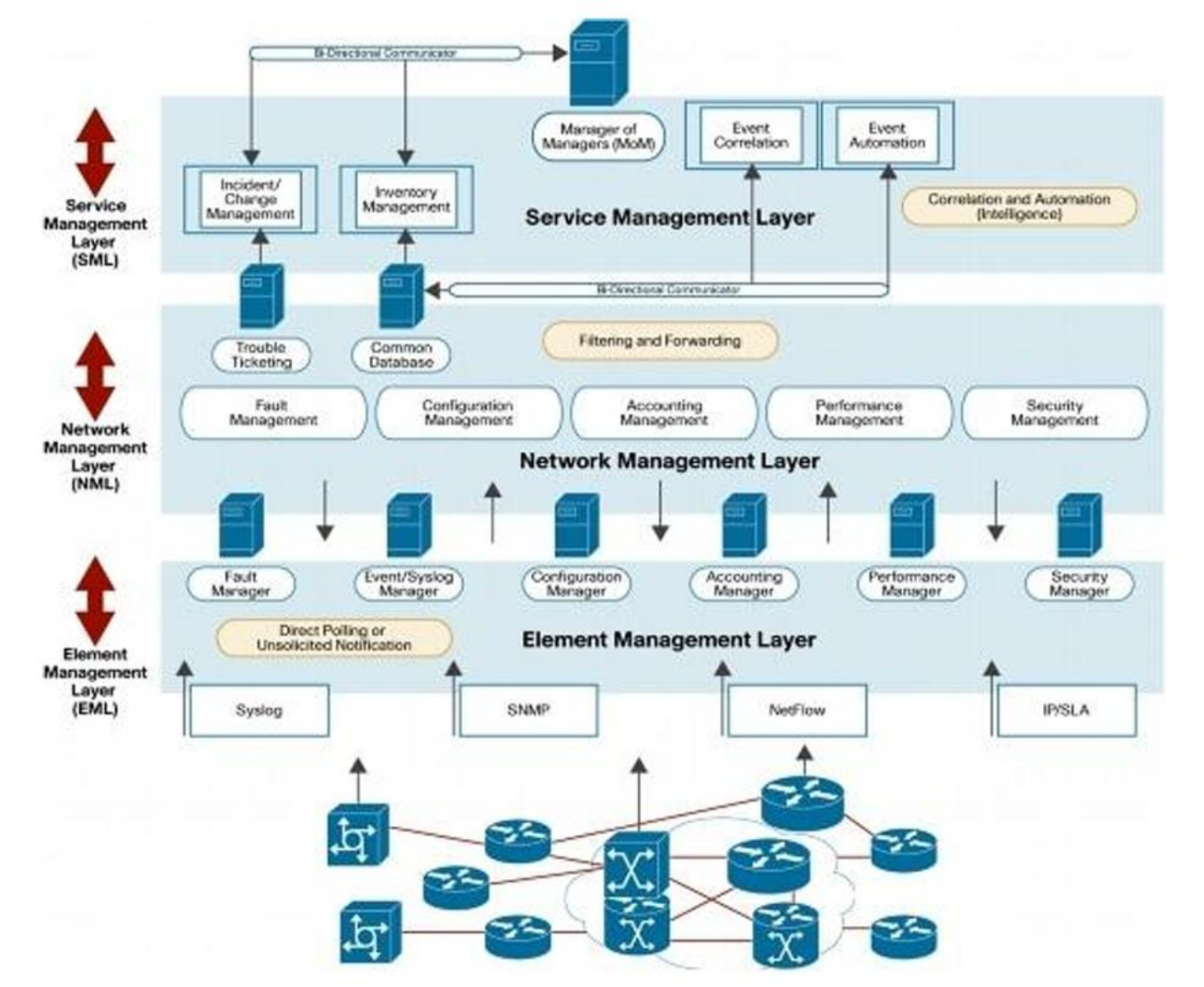


Рис. 4.1. Загальна структура системи моніторингу телекомунікаційної мережі

Аналіз існуючих IoT-рішень для розумного дому

- **Таблиця 1 Порівняльний аналіз архітектур IoT-рішень для «розумного дому»**

Архітектурний підхід	Характеристика	Переваги	Недоліки
Централізований	Обробка та управління виконуються на віддаленому сервері або в хмарі	Висока масштабованість, зручне адміністрування	Залежність від каналу зв’язку, збільшені затримки
Локальний	Управління здійснюється локальним контролером у межах будинку	Низькі затримки, автономність	Обмежені обчислювальні ресурси
Гібридний	Поєднання локального контролера та хмарних сервісів	Баланс між швидкодією та аналітикою	Підвищена складність реалізації

Математичні моделі трафіку IoT-мереж

- Для опису трафіку IoT-мереж використовуються моделі теорії масового обслуговування. Інтенсивність надходження пакетів описується параметром λ. Середній час перебування пакета в системі залежить від співвідношення між λ та пропускною здатністю. Зі збільшенням кількості пристроїв затримка передачі даних зростає. Це вимагає використання механізмів балансування навантаження. В свою чергу, математичні моделі дозволяють оцінити межі стабільної роботи мережі.

$$T = \frac{1}{\mu - \lambda}$$

Прогнозування стану IoT-мережі на основі машинного навчання

Основною метою прогнозування є завчасне виявлення перевантажень і погіршення якості обслуговування ще до того, як вони вплинуть на роботу системи

Фактори, що впливають на прогнозування трафіку:

- інтенсивність надходження даних від IoT-пристроїв;
- кількість активних вузлів у мережі;
- затримка та втрати пакетів;
- пропускна здатність каналів зв’язку;
- режими роботи та енергоспоживання пристроїв.

Модель прийняття рішень і оптимізація QoS

- **Модель стану IoT-мережі**

Стан IoT-мережі у момент часу t описується вектором:

$$\mathbf{x}(t) = [\, l\,(t),\ d(t)\ p(t)\ e(t)\,],$$

де: $l(t)$ —навантаження мережі; $d(t)$ —середня затримка передавання даних; $p(t)$ —імовірність втрат пакетів; $e(t)$ —рівень енергоспоживання.

- **Керуючі дії**

Вектор керування: $\mathbf{u}(t) = [\, < m\colon mor\,(t)\ b(t)\ m(t)\,],$

де: $r(t)$ —параметри маршрутизації; $b(t)$ —розподіл пропускної здатності; $m(t)$ —режими роботи IoT-пристроїв.

- **Цільова функція оптимізації QoS**

Задача управління формалізується як задача мінімізації:

$$J = \sum_{t=0}^{T} \left(\alpha\, d(t) + \beta\, p(t) + \gamma\, e(t)\right),$$

де α, β, γ— вагові коефіцієнти пріоритетів QoS.

Архітектура інтелектуального контролера

Багаторівнева архітектура контролера включає:

- **Рівень збору даних**
  IoT-пристрої, сенсори, виконавчі механізми
- **Рівень комунікації**
  шлюзи, мережеві протоколи, передавання даних
- **Аналітичний рівень**
  моніторинг, аналіз трафіку, формування ознак
- **Інтелектуальний рівень**
  прогнозування стану мережі, прийняття рішень
- **Рівень управління**
  керуючі команди, оптимізація QoS

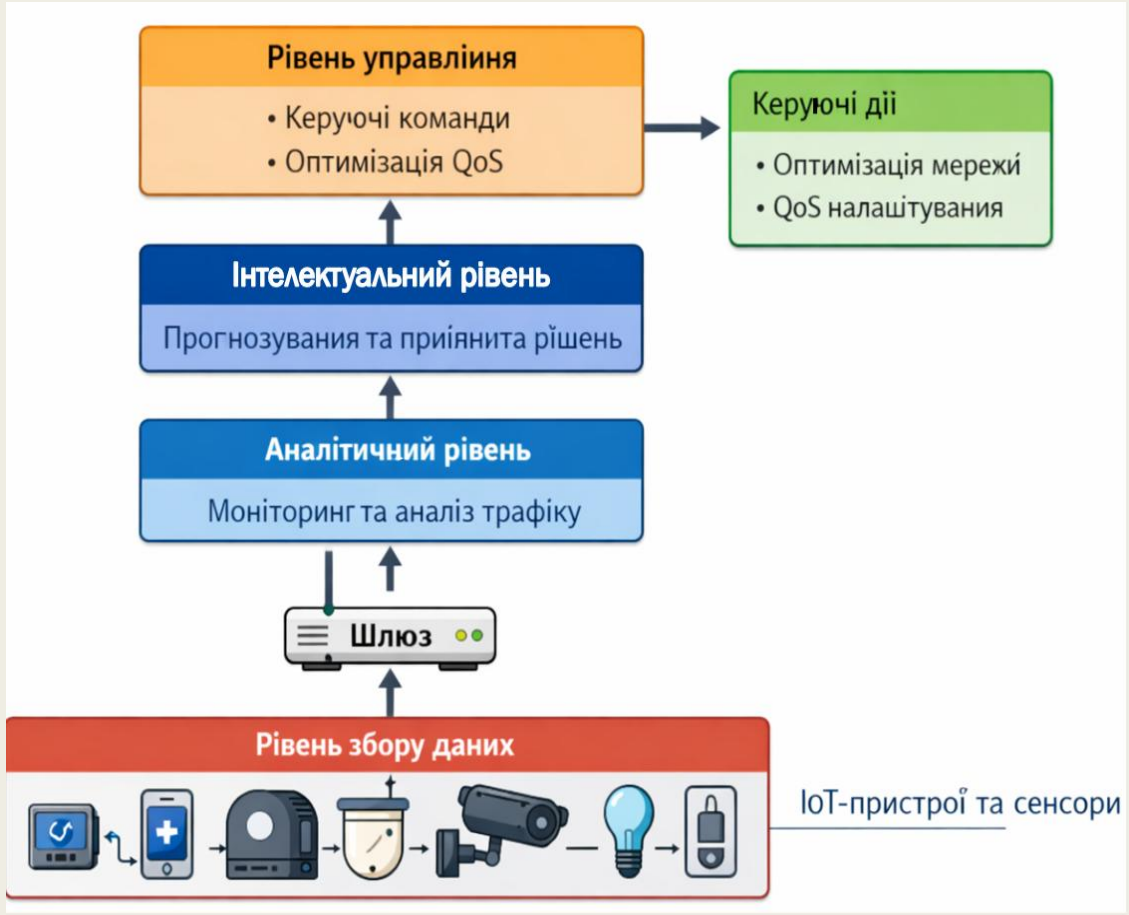


Рис.9.1 Архітектура контролера

Блок-схема функціонування інтелектуальної системи управління IoT-мережею

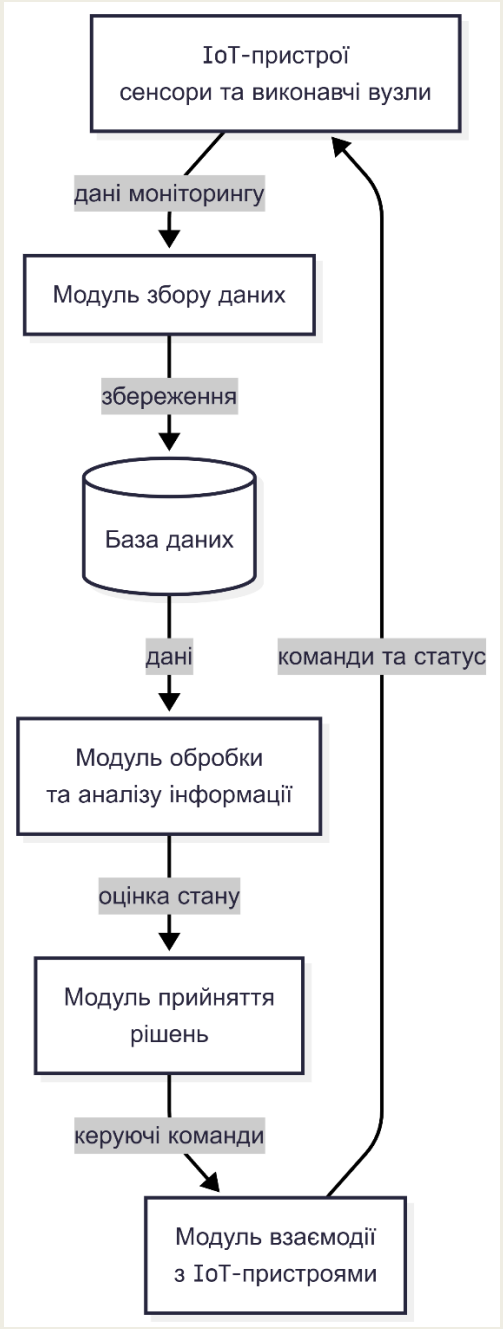


Рис. 4.1 Загальна структура та взаємодія основних програмних модулів інтелектуальної системи управління IoT-мережею

- Система функціонує у вигляді замкненого контуру управління
- Дані від IoT-пристроїв збираються та агрегуються на мережевому шлюзі
- На основі моніторингу формується вектор стану мережі
- Методи машинного навчання забезпечують прогнозування стану
- Прийняття рішень здійснюється шляхом оптимізації параметрів QoS

ВИСНОВКИ

- У роботі розв’язано задачу інтелектуального управління IoT-мережею «розумного дому». Аналіз існуючих IoT-рішень показав обмеженість статичних і реактивних підходів до управління мережею.
- Запропоновано застосування математичних моделей трафіку та параметрів QoS для формалізації процесів управління. Обґрунтовано використання методів машинного навчання для прогнозування стану IoT-мережі.
- Сформовано модель прийняття рішень, орієнтовану на оптимізацію якості обслуговування з урахуванням прогнозованого стану мережі.
- Сформовано багаторівневу архітектуру інтелектуального контролера управління.
- Реалізація системи та дослідження підтвердили ефективність запропонованого підходу. Отримані результати свідчать про доцільність застосування інтелектуального управління в IoT-системах «розумного дому».

ДЯКУЮ ЗА УВАГУ!

Студент групи ТСДМ-62
ЗАГОРУЙЧЕНКО Владислав

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Владислав ЗАГОРУЙЧЕНКО

Назва: Розробка інтелектуальної системи управління мережею IoT для розумного дому

Координатор: Катерина ТРЕНЬОВА

Підрозділ: ННІТ

Коефіцієнт подібності 1:0.37

Коефіцієнт подібності 2:0

Тривога: 11

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*