Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Модель інформаційної взаємодії в мережах IoT

(тема)

Виконав:

студент II курсу, групи КСМм-20-1

Нефедченко О.О.
(прізвище, ініціали)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Комп’ютерні системи та мережі
(повна назва освітньої програми)

Керівник: доц. Токарєв В.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп’ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Нефедченко Олексію Олеговичу
(прізвище, ім’я, по батькові)

1. Тема роботи Модель інформаційної взаємодії в мережах IoT

затверджена наказом по університету від “ 05 ” листопада 2021 р. № 1656Ст

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2021р.

3. Вхідні дані до роботи 1) провести дослідження моделі інформаційної взаємодії сенсорних пристроїв в мережі IoT; 2) провести огляд основних протоколів IoT; 3) CPU Intel Core i5-430M, 2533 MHz (19 x 133); 4) операційна система - Windows 10; 5) тип ядра ОС: Multiprocessor Free (64-bit); 6) представлення вихідних даних: згідно нормативних документів.

4. Перелік питань, що потрібно опрацювати у роботі
1) огляд літератури за темою роботи;
2) аналіз предметної області;
3) вибір та обґрунтування методики дослідження;
4) проведення експериментальних досліджень;
5) висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайд-презентація – 22 слайда

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд літератури за темою роботи	09.11.21 - 12.11.21	
2	Вибір та обґрунтування методики дослідження	13.11.21 - 18.04.21	
3	Вибір інструментальних засобів	19.11.21 - 22.11.21	
4	Проведення експериментів	23.11.21 - 29.11.21	
5	Оформлення матеріалів атестаційної роботи	30.11.21 - 03.12.21	
6	Подання кваліфікаційної роботи керівникові та	08. 12.21 - 09.12.21	
	попередній захист		
7	Подання кваліфікаційної роботи на	10.12.21 - 11.12.21	
	рецензування		

Дата видачі завдання 08 листопада 2021 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Токарєв В.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 65 с., 26 рис., 1 дод., 14 джерел.

БЕЗДРОТОВА СЕНСОРНА МЕРЕЖА, ПРОТОКОЛ, WI-FI.

Метою кваліфікаційної роботи є дослідження моделі інформаційної взаємодії сенсорних пристроїв в мережі IoT.

У ході виконання кваліфікаційної роботи досліджується модель інформаційної взаємодії сенсорних пристроїв в мережі IoT. Такий підхід дозволяє говорити, що модель інформаційної взаємодії побудована з урахуванням фундаментальних характеристик технології IoT, що дозволяє адекватно оцінювати ймовірносно-часові характеристики інформаційної взаємодії. Комплекс математичних моделей поєднує аналітичний та статистичний методи моделювання, що дозволяє оцінити ймовірносно-часові характеристики передачі даних на всіх етапах інформаційної взаємодії в мережі IoT.

ABSTRACT

Master’s thesis: 65 pages, 26 figures, 1 appendices, 14 sources.

PROTOCOL, WI-FI, WIRELESS SENSOR NETWORK.

The purpose of the qualification work is to study the model of information interaction of sensor devices in the IoT network.

In the course of the qualification work, the model of information interaction of sensor devices in the IoT network is investigated. This approach allows us to say that the information interaction model is built taking into account the fundamental characteristics of the IoT technology, it allows to adequately assess the probabilistic-temporal characteristics of information interaction. The complex of mathematical models combines analytical and statistical modeling methods, allows you to evaluate the probabilistic and temporal characteristics of data transmission at all stages of information interaction in the IoT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АЦП – аналого-цифровий перетворювач

ІВ – інформаційна взаємодія

ІМ – імітаційне моделювання

МСО – мережа, яка самоорганізується

СП – сенсорні пристрої

ВСТУП

В даний час технологія Internet of Things (IoT), що розвивається, виглядає багатообіцяючою в різних областях індустрії – виробництві, логістиці, медицині, енергетиці, транспорті, міському господарстві, управлінні надзвичайними ситуаціями. Області застосування технології IoT продовжують стрімко рости. Основна ідея IoT полягає в організації взаємодії різноманітних предметів в навколишньому середовищі, передачі інформації, що генерується цими речами і надання безперебійного з'єднання. Взаємодія речей здійснюється за допомогою вже наявних і розроблюваних інформаційно-комунікаційних технологій. До існуючих вимог технологій Інфокомунікації і взаємодії, таким як забезпечення зв'язку "в будь-якому місці" і "в будь-який час", в просторі IoT з'являється ще одне – "зв'язок з будь-якою річчю". Під цією вимогою розуміють, як взаємодію між речами, так і між річчю і людиною. Технологія IoT знаходиться на стадії ранньої реалізації і активних досліджень. На міжнародному рівні дана концепція вже набуває рис сформованої технології – ведуться активні роботи в області стандартизації архітектури, технічних компонентів, застосунків. Одночасно з урахуванням специфіки інформаційної взаємодії в IoT потрібні нові моделі і алгоритми, що сприяють проектуванню оптимальних рішень IoT. У загальному випадку модель IoT має на увазі наявність у кожної фізичної речі, як мінімум, елемента обладнання для комунікації і деяких опціональних можливостей, наприклад, можливості введення, зберігання, обробки даних або вимірювання будь-яких параметрів. Специфіка інформаційної взаємодії речей визначається фундаментальними характеристиками IoT. Відповідно до рекомендацій Міжнародного Союзу Електрозв'язку (МСЕ-Т) до їх числа відносяться певні метрики, особливості яких не дозволяють застосовувати методи і алгоритми, на базі яких функціонують традиційні комп'ютерні мережі, до IoT. Цьому є кілька причин. Такі метрики як, зв'язність і динамічні зміни робить топологію

мережі нерегулярною, використання бездротових технологій, «туманних» і «хмарних» обчислень викликає появу колізій джерел даних при доступі до ресурсів IoT, а гетерогенність і вимога енергоефективності впливають на імовірносно-тимчасові характеристики інформаційної взаємодії в IoT. Ці обставини необхідно враховувати при проектуванні IoT і з урахуванням специфіки роботи шукати нові методи і алгоритми, що дозволяють отримувати оптимальні рішення по організації інформаційної взаємодії при заданих умовах функціонування IoT.

1 ДОСЛІДЖЕННЯ ОРГАНІЗАЦІЇ МЕРЕЖ IoT

Для досягнення цілей технології Internet of Things (IoT) – об’єднання різних сенсорних пристроїв, гетерогенних комп’ютерних і сенсорних мереж необхідна певна архітектура. Рекомендований МСЕ-Т поділ функцій IoT відбувається на чотири основних рівня:

- рівень взаємодії з середовищем;
- мережевий рівень – відповідає безпосередньо за передачу даних;
- сервісний рівень – для обробки та перетворення інформації;
- рівень взаємодії з користувачем або додатками.

Така архітектура задовольняє системним характеристикам мережі IoT:

- легкість модернізації;
- модульність;
- масштабованість мережі;
- відповідає вимозі адаптивності, що, в свою чергу, дозволяє системам управління підлаштовуватися під зміни або ж змінювати саму мережу в залежності від різних умов функціонування.

З точки зору теорії системного аналізу, при проектуванні мережі IoT необхідно визначити:

- топологію;
- структуру;
- склад основних елементів;
- найбільш важливі взаємозв’язки між елементами;
- сформулювати призначення і основні завдання;
- критерії та показники раціональної організації інформаційної взаємодії.

IoT, як технологія бере початок від територіально розподілених сенсорних мереж, які спочатку розвиваються як локальні сенсорні мережі і, згодом, мають вихід в глобальні мережі Internet і GSM. У науковій літературі

сенсорні мережі (рисунок 1.1) визначаються як «розподілені мережі, що складаються з маленьких бездротових вузлів вузької спеціалізації у великій кількості розосереджених (випадково) на деякій поверхні або області».

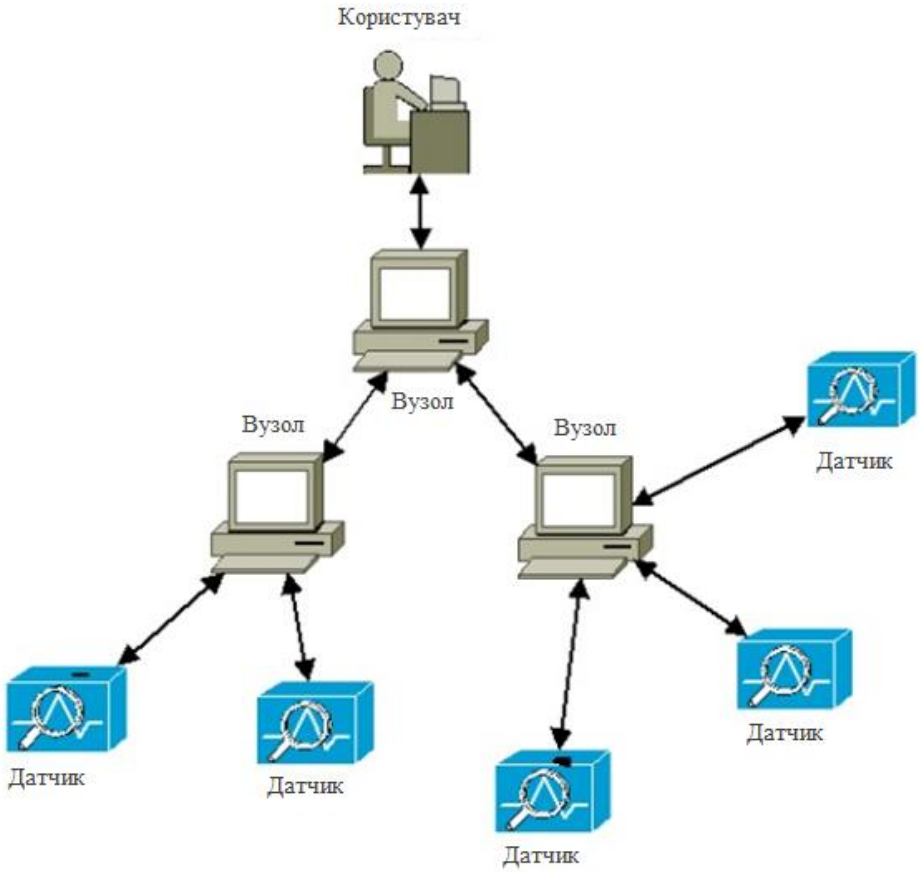

Рисунок 1.1 – Приклад простої сенсорної мережі

Таким чином, сенсорні мережі засновані на спільній роботі великого числа мініатюрних вузлів – сенсорних пристроїв (СП) (рисунок 1.2), розподілених в деякій області з досить високою щільністю.

В області покриття радіосигналу кожного з СП повинно знаходитись як мінімум ще одне СП-сусід. Чим більше «сусідів» у кожного з СП, тим більш високою точністю і надійністю володіє сенсорна мережа. Технології радіодоступу, що застосовуються в СП і засновані на стандарті IEEE 802.15.4, дозволяють передавати дані на відстань до декількох десятків метрів.

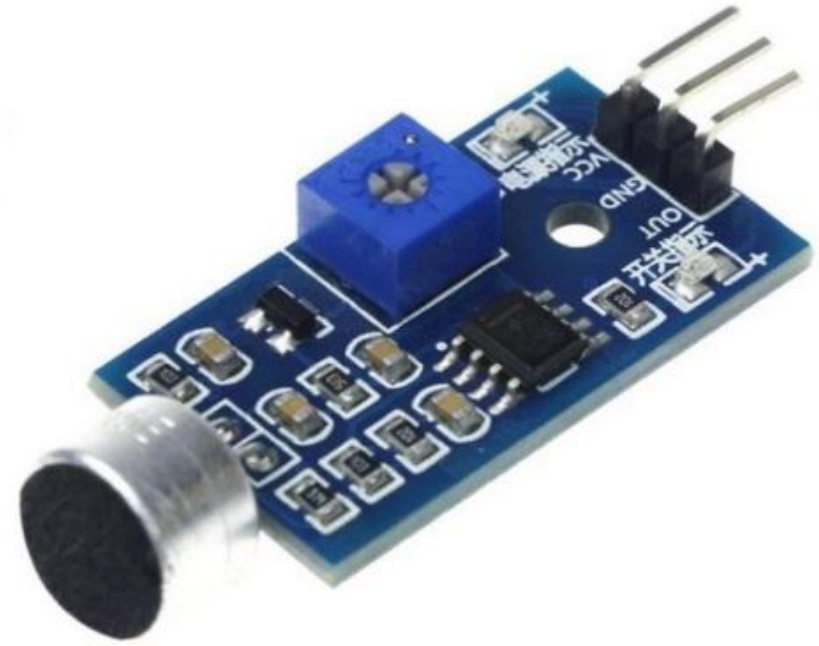

Рисунок 1.2 – Приклад сенсорного пристрою мережі IoT

Сенсорний пристрій складається з чотирьох основних компонентів, як показано на рисунку 1.3:

- блоки збору;
- блоки обробки;
- блоки передачі даних;
- блоки живлення.

Також в складі СП можуть бути модулі визначення місцезнаходження, силовий генератор і мобилизатор. Їх наявність залежить від того, для яких цілей проектується сенсорна мережа.

Модуль збору даних складається з датчика і аналого-цифрового перетворювача (АЦП). Аналоговий сигнал, що видається датчиком в результаті спостережуваного явища, перетворюється в цифровий сигнал за допомогою АЦП, а цифровий сигнал подається вже в блок обробки. Модуль обробки, що складається з процесора і пам’яті, реалізує процедури, які дозволяють спільно з іншими вузлами виконувати поставлені завдання спостереження.

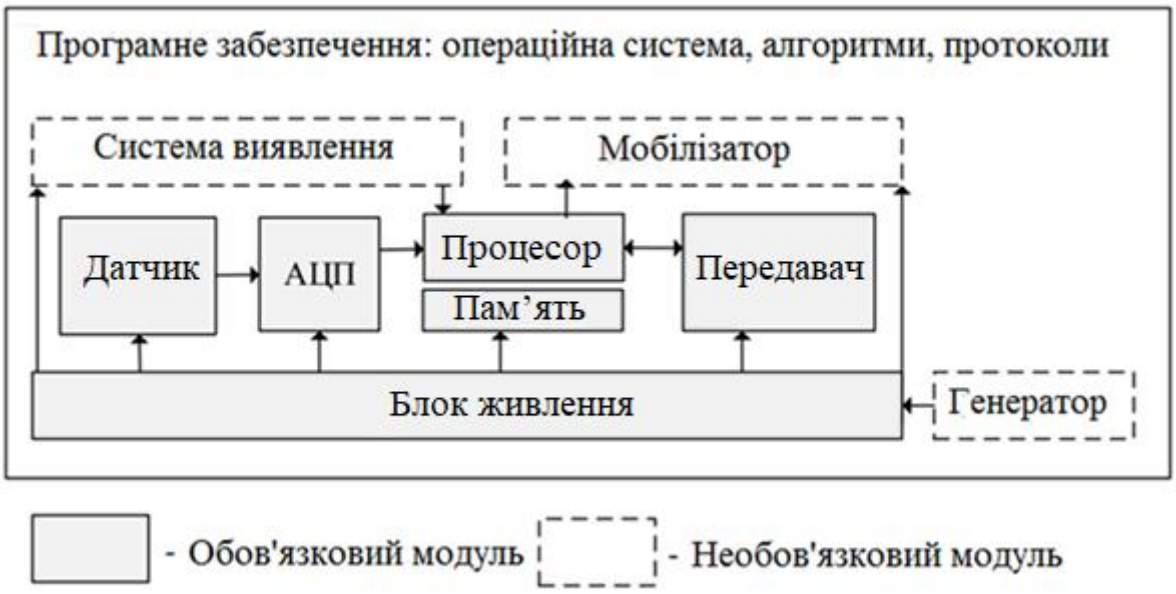

Рисунок 1.3 – Компоненти СП

Завдяки наявності цього модуля в складі СП замість передачі вихідних (сирих) даних, вони обробляються за допомогою якихось простих обчислень і далі вже можна отримувати лише необхідні і частково оброблені дані. Передавач (трансивер) утворює інтерфейс СП з мережею. Більшості сенсорних пристроїв необхідно з досить високою точністю визначати своє місце розташування. З цією метою в схему СП інтегрується модуль визначення місця розташування. При необхідності переміщення СП в схему вбудовується мобілізатор. Всі ці модулі, як правило, містяться в одиному корпусі. Розмір корпусу може бути від декількох десятків кубічних сантиметрів і до кубічного сантиметра та досить легким, щоб залишатися в повітрі. Крім розмірів, до СП пред'являються і інші жорсткі вимоги, наприклад, вони повинні:

- володіти низьким енергоспоживанням;
- взаємодіяти з великою кількістю таких же СП на малих відстанях;
- мати низьку собівартість;
- бути в автономному режимі, тобто без нагляду;
- адаптуватися до навколишнього середовища.

Блок живлення – це один з основних елементів СП. Оскільки сенсорні

пристрої можуть бути недоступними через періодичного переходу в «сплячий» режим, то живучість сенсорної мережі залежить від живлення окремих СП. Живлення є обмеженим ресурсом, наприклад, загальний запас енергії смарт-вузла становить близько 1 Дж. Для бездротової інтегрованої мережі датчиків (WINS) середній рівень заряду, для забезпечення тривалого часу роботи повинен бути менше 30 LA. Збільшити термін експлуатації сенсорних мереж можна, використовуючи підзаряджаючі батареї, наприклад, отримуючи енергію з навколишнього середовища, тобто сонячні батареї. Передавач СП може бути пасивним або активним оптичним пристроєм або радіочастотним передавачем. Для радіочастотної передачі необхідні процеси модуляції сигналу при певній смузі пропущення, фільтрація, демодуляція, реалізація яких в СП робить їх більш складними і дорогими. Крім того, можливі втрати при передачі даних між двома вузлами через те, що антени розташовано близько до землі. Проте, радіозв’язок є кращим, так як передача даних здійснюється на низьких частотах (як правило, менше 1 Гц), аперіодичність циклів передачі часте через малі відстані. Ці можливості дозволяють використовувати низькі частоти. Проектування радіопередавачів з низьким енергоспоживанням є технічно складним завданням. Технології Bluetooth, які теж можна використовувати при проектуванні сенсорних пристроїв не є достатньо ефективними для сенсорних мереж, оскільки споживають багато енергії. Крім розглянутої класичної архітектури СП можливі і інші, що пов’язано, наприклад, з необхідністю не тільки моніторингу або контролю вимірюваних характеристик, але і впливу на об’єкт вимірювань Такий елемент, який має можливість впливу на об’єкт, називається актором, архітектура якого наведена на рисунку 1.4. На відміну від сенсорного вузла в архітектурі актора присутній активний елемент, що взаємодіє із зовнішнім середовищем під управлінням контролера прийняття рішення про вплив на навколишнє середовище, наприклад, пристрій введення інсуліну хворим на діабет.

Рисунок 1.4 – Компоненти акторного вузла

Ще однією особливістю сенсорних мереж є спільна робота окремих сенсорних пристроїв завдяки наявності в них модуля обробки. В даний час процесори постійно зменшують свої габарити і збільшують потужність, але обробка і зберігання даних в СП, без змін, залишається слабким місцем СП. Більшість завдань, пов’язаних з моніторингом, вимагають визначення місця розташування СП. Для цих цілей, як один з варіантів, в кожен вузол вбудовується модуль системи глобального позиціонування GPS, що працює з точністю до 5 метрів або інший варіант – тільки деякі СП використовують GPS, які допомагають іншим пристроям визначити своє положення в просторі. Розміщення СП не обов’язково попередньо розраховувати. Дана властивість дозволяє розміщувати сенсорні пристрої випадковим чином, наприклад, в важкодоступних місцевостях або оперативно розгортати мережу при наданні допомоги на певний час. Це означає, що протоколи сенсорної мережі і алгоритми роботи СП повинні мати можливість самоорганізації, яка і реалізується за допомогою системи визначення місця розташування. Взаємодії СП між собою в рамках однієї сенсорної мережі утворюють топологію mesh (англ. mesh – петля, комірка мережі, отвір сита) (рисунок 1.5), тобто сенсорні

пристрої об’єднуються численними сполуками, що утворюють порожнисту топологію.

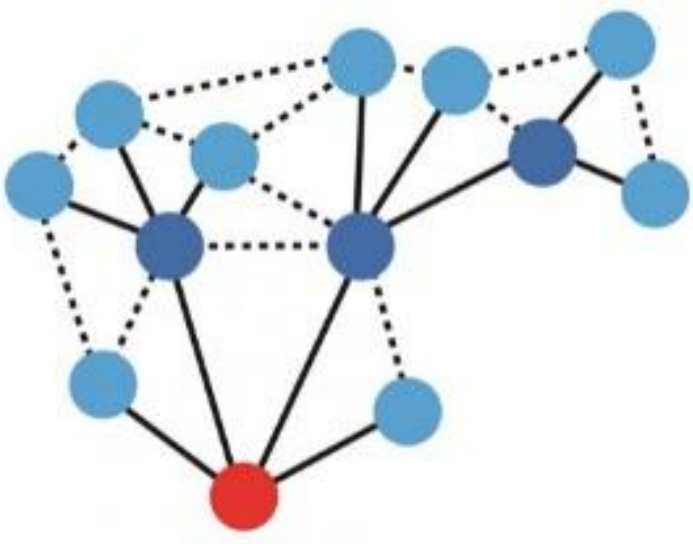

Рисунок 1.5 – Приклад топології Mesh

Самоорганізуюча мережа з топологією mesh дозволяє реалізувати наступні можливості:

- створення зон суцільного інформаційного покриття великої площі;
- масштабованість мережі, тобто збільшення площі зони покриття і щільності інформаційних потоків в режимі самоорганізації;
- використання бездротових транспортних каналів для зв’язку в режимі «кожен з кожним»;
- стійкість мережі до втрати окремих елементів.

Ще одна технологія, яка присутня в ідеї IoT – це технологія M2M (Machine to Machine) (рисунок 1.6). M2M – це загальна назва технологій, що дозволяють машинам проводити обмін інформацією між собою, або передавати її в односторонньому порядку в автоматичному режимі між пристроями без участі людини. Це можуть бути дротові і бездротові системи моніторингу датчиків або будь-яких параметрів пристроїв.

Рисунок 1.6 – Приклад технології Machine to Machine

Або, наприклад, банкомати чи платіжні термінали можуть автоматично передавати інформацію по GSM-мережам. Технологія M2M також використовується в системах безпеки і охорони, системах охорони здоров’я та системах позиціонування рухомих об’єктів на основі систем ГЛОНАСС / GPS. Досконаліть і поширення даної технології дозволило використовувати її в будь-якому мобільному пристрої, в тому числі і вузлах сенсорних мереж.

Вважається, що саме ця технологія породила термін IoT, маючи на увазі під ним якусь відокремлену обчислювальну середу, що складається з пристроїв, які самостійно взаємодіють один з одним і надають користувачеві результати своєї спільної діяльності. З урахуванням з’явившогося терміна, сенсорний пристрій, інтегрований в який-небудь об’єкт – «річ» так само стали називати IoT.

1.1 Архітектура мережі IoT

Архітектура IoT показує, яким чином різні інфокомунікаційні технології, що забезпечують функціонування IoT пов’язані одна з другою. Архітектура IoT включає чотири функціональних рівня, представлених на рисунку 1.7.

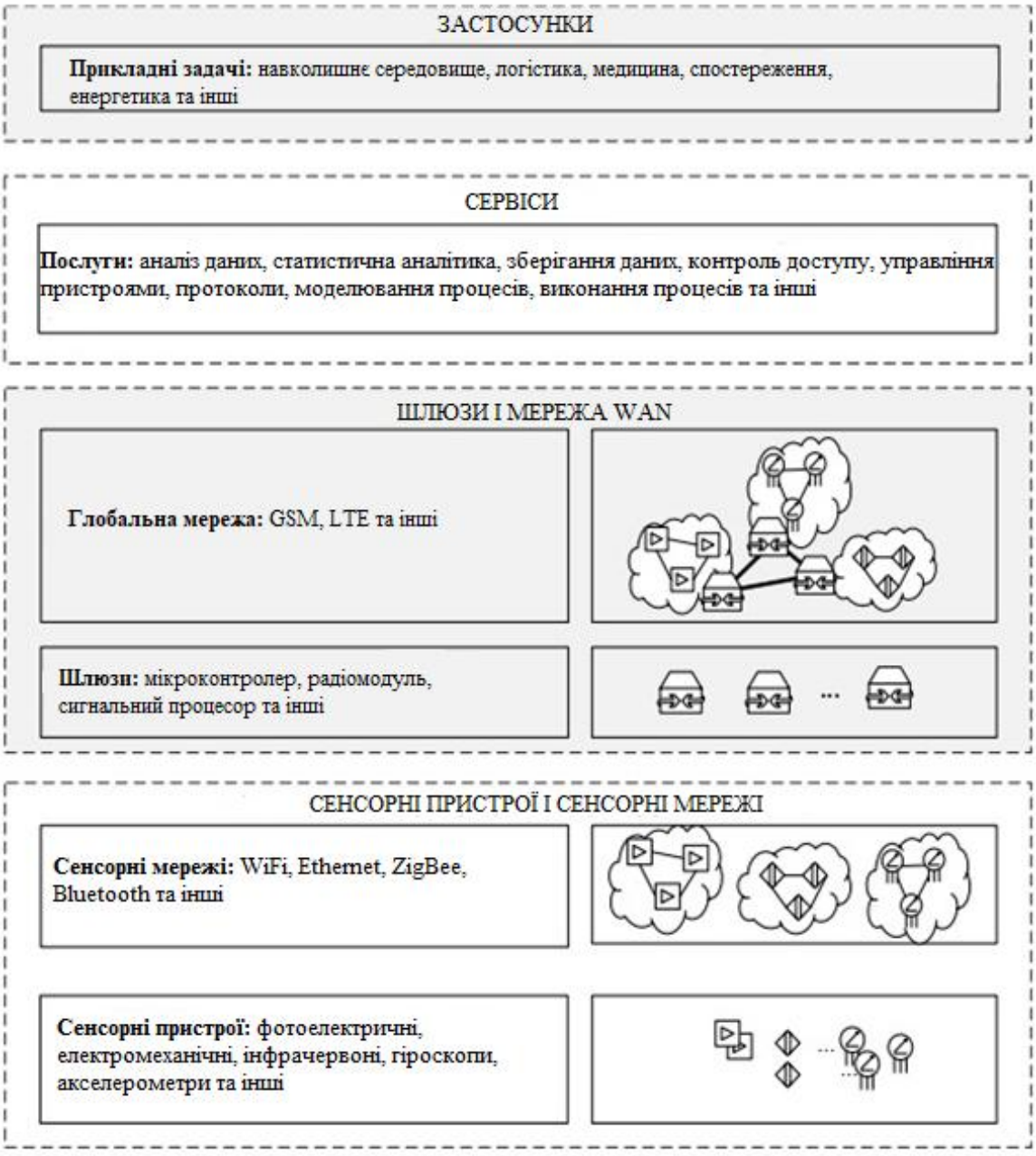

Рисунок 1.7 – Архітектура IoT

Рівень взаємодії з середовищем (сенсори і сенсорні мережі) – це найнижчий рівень архітектури IoT, який складається з «розумних» (смарт) об’єктів, інтегрованих з СП. Сенсори реалізують з’єднання фізичного і віртуального (цифрового) світів, забезпечуючи збір та обробку інформації в реальному масштабі часу.

Більшість сенсорів вимагають з’єднання з агрегатором сенсорів (шлюзом), які можуть бути реалізовані з використанням локальної обчислювальної мережі, такі як Ethernet, Wi-Fi або персональної мережі (PAN, Personal Area Network).

Мережевий рівень забезпечує транпорт великим обсягом даних, що створюються численними СП на першому рівні IoT і складається з конвергентної мережевої інфраструктури, яка створюється шляхом інтеграції різнорідних мереж в єдину мережеву платформу. Сервісний рівень містить набір інформаційних послуг, які автоматизують технологічні бізнес-операції в IoT:

- підтримки операційної і бізнес діяльності;
- різної аналітичної обробки інформації;
- зберігання даних;
- забезпечення інформаційної безпеки;
- управління бізнес-процесами та ін.

Рівень додатків включає різні типи додатків для відповідних промислових секторів і сфер діяльності, таких як:

- енергетика;
- транспорт;
- торгівля;
- медицина;
- освіта та ін..

Застосунки можуть бути «вертикальними», коли вони є «специфічними» для конкретної галузі промисловості, а також «горизонтальними», які можуть використовуватися в різних секторах економіки.

На практиці реалізують один з трьох способів взаємодії в мережах IoT:

- прямий доступ;
- взаємодія за допомогою шлюзу;
- взаємодія за допомогою сервера.

При прямому доступі звернення до IoT здійснюється безпосередньо з клієнтського застосування за IP-адресою, що ідентифікує інтернет-річ. Інтерфейс взаємодії з інтернет річчю є web-ресурс з графічним оформленням, керований за допомогою web-браузера. Недоліками такого способу є необхідність фіксованою адресації IoT, що викликає залежність від провайдера послуги зв’язку з глобальною мережею Internet. Вирішення цієї проблеми призводить до збільшення часу взаємодії, оскільки IoT доводиться звертатися до проксі-сервера для ідентифікації за псевдонімом.

Обмеження на кількість підключень IoT до сервера для передачі даних через низьку якість зв’язку і обчислювальних можливостей IoT. Вирішення цієї проблеми підключенням IoT до стабільного джерела зв’язку з Internet призводить до втрати мобільності. Альтернативою прямому доступу є взаємодія за допомогою шлюзу. Такий спосіб є більш раціональним і в даний час замінює прямий доступ, особливо при організації зв’язку «туманних обчислень» з «хмарними». Оскільки велика частина стандартів бездротових сенсорних мереж не підтримують протокол IP, використовуючи власні протоколи взаємодії малої зони дії, то дана особливість викликає необхідність наявності спеціального вузла – ретранслятора даних з сенсорної мережі в мережу Internet для узгодженості протоколів. Недоліки підходу реалізації взаємодії за допомогою шлюзу аналогічні випадку прямого доступу, але поширюються вони на шлюз. При організації доступу за допомогою сервера, всі функції взаємодії виконує сервер. У функції сервера входять:

- прийом і передача повідомлень від інтернет-речей користувачам,
- обробка прийнятої інформації і її зберігання,
- забезпечення призначеного для користувача інтерфейсу для двостороннього обміну між користувачем і IoT.

Такий спосіб доступу є найбільш раціональним і застосовуваним, оскільки дозволяє перенести навантаження, пов’язане з обробкою запитів користувачів на централізований сервер, тим самим розвантажуючи слабкий радіо-канал між IoT на провідні канали між сервером і користувачами. Крім розглянутих переваг методу доступу, сервер надає сервіси зберігання та обробки даних, в тому числі і «хмарні обчислення». Даний підхід не виключає застосування шлюзів для організації зв’язку локальних бездротових мереж з сервером.

1.2 Протоколи взаємодії в IoT

В даний час для вирішення завдань в IoT інфраструктурі виділяють наступні групи протоколів:

- протоколи для збору даних сенсорними пристроями і передачі їх серверам;
- протоколи для з’єднання СП з людьми, окремий випадок такої схеми, коли люди з’єднуються з серверами;
- протоколи для з’єднання серверів між собою.

Є різні варіанти їх реалізації. Застосування і вибір протоколів залежить від навантаження мережі, існуючого апаратного забезпечення, архітектури IoT. Проведемо огляд основних протоколів IoT.

Протокол № 1 - CoAP (Constrained Application Protocol) – обмежений протокол передачі даних, аналогічний протоколу HTTP, але адаптований для роботи із сенсорними пристроями низької продуктивності (рисунок 1.8).

Протоколи № 2 – MQTT (Message Queue Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol), AMQP (Advanced Message Queuing Protocol) – ці протоколи обміну повідомленнями із застосуванням брокера, що реалізують модель типу «видавець-передплатник»

(publish/subscribe).

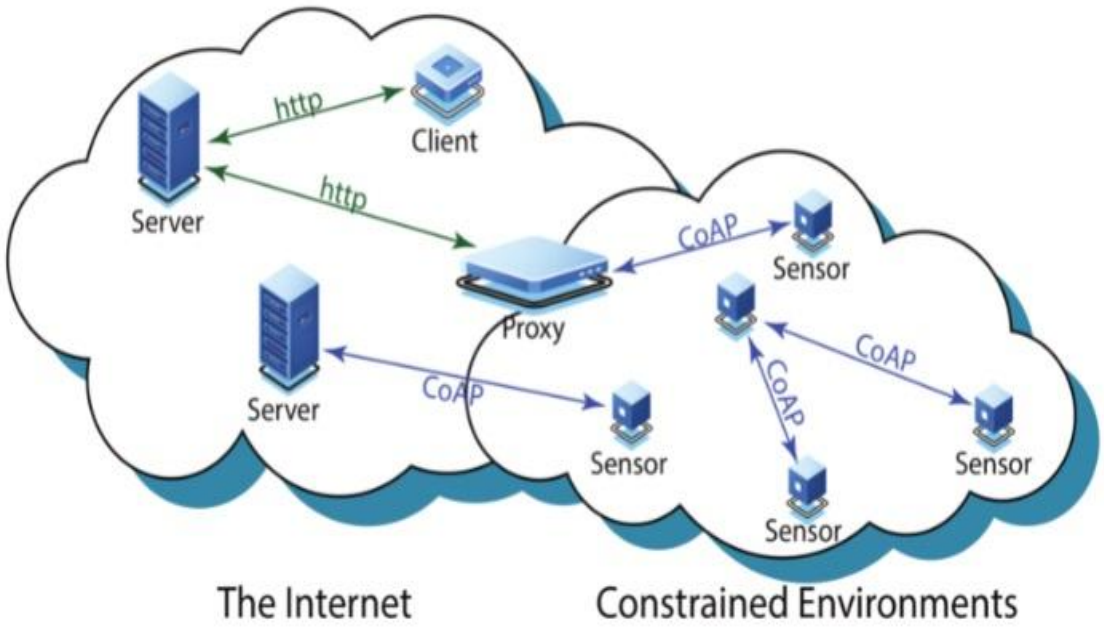

Рисунок 1.8 – Протокол - CoAP

Пристрій типу «Видавець» відправляє повідомлення, яке публікується в централізованому сервісі – брокері повідомлень, а пристрій типу «Абонент» отримує повідомлення з брокера. Для використання брокера необхідно «підписатися» на певні теми публікованих повідомлень. В даний час протокол MQTT (рисунок 1.9) є найбільш поширеним протоколом організації IoT - інфраструктури. Це обумовлено невеликими накладними витратами, які пов’язані з добре продуманим форматом заголовків, в результаті чого витрата енергії акумуляторної батареї знижується і збільшується кількість переданих повідомлень в одиницю часу. Протокол MQTT розроблений спеціально для подолання обмежень, пов’язаних з підключенням швидко зростаючого числа датчиків, приводів, телефонів, мікрокомп’ютерів, планшетів.

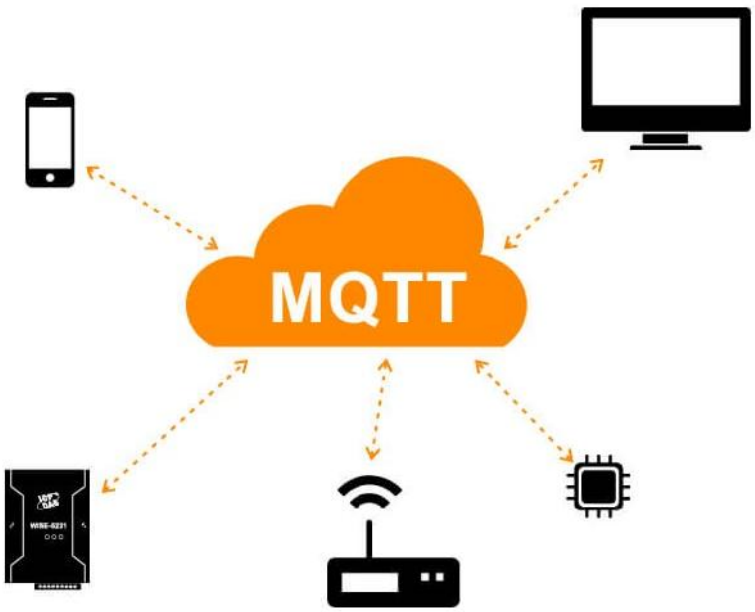

Рисунок 1.9 – Протокол - MQTT

Протокол XMPP забезпечує обмін текстовими повідомленнями між точками доступу (рисунок 1.10).

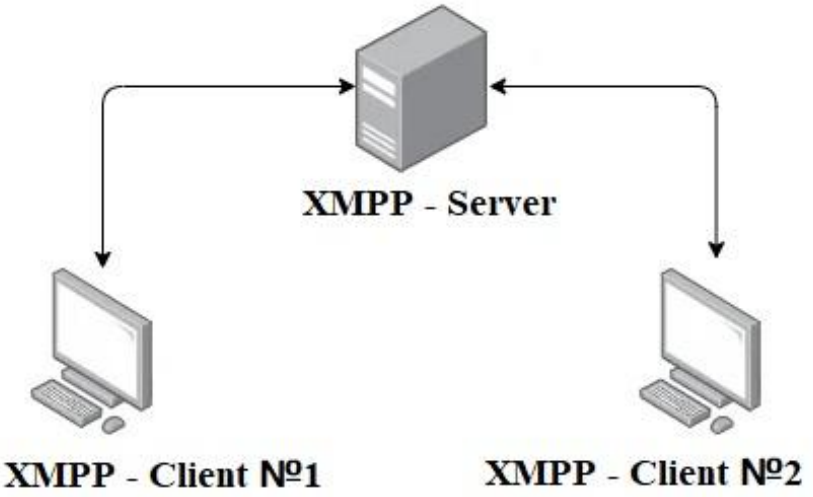

Рисунок 1.10 – Протокол - XMPP

У протоколі XMPP використовується текстовий формат XML в якості вбудованого типу, забезпечуючи природний зв’язок між людьми. Подібно

протоколу MQTT він працює по протоколу TCP або, по протоколу HTTP поверх протоколу TCP.

Його перевагою є метод адресації виду name@domain.com, який допомагає з’єднувати користувачів в величезному просторі Internet. Стосовно до IoT протокол XMPP забезпечує простий спосіб адресації пристроїв. Це особливо зручно, коли дані передаються між віддаленими, найчастіше незалежними точками, як у випадку зв’язку між двома абонентами. Цей протокол не володіє високою швидкістю.

Фактично, в більшості реалізацій цього протоколу використовується метод опитування або перевірки доповнень тільки на вимогу. XMPP-протокол реалізує істотну перевагу, наприклад, при підключенні домашнього термостата до web-серверу, так, що користувач може отримати до нього доступ зі смартфона. Сильними сторонами цього протоколу є адресація, безпека і масштабованість, що робить його ідеальним для додатків IoT з орієнтацією на споживача.

Протокол AMQP (Advanced Message Queuing Protocol, або вдосконалений протокол організації черги повідомлень), який іноді розглядають як протокол IoT (рисунок 1.11).

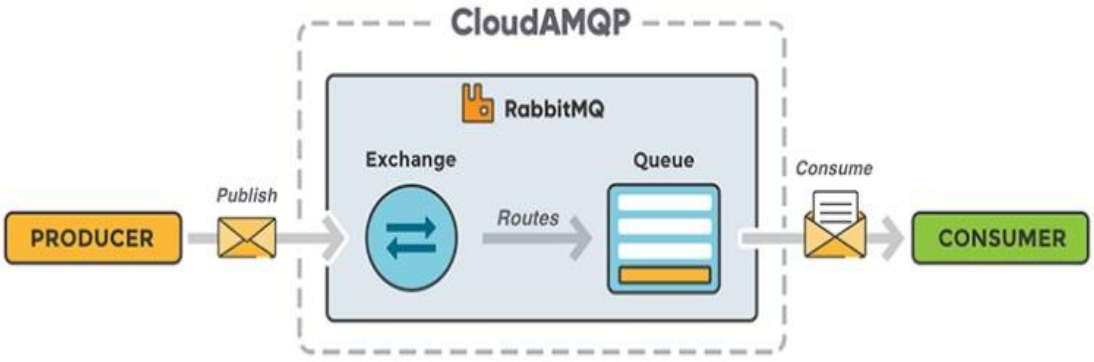

Рисунок 1.11 – Протокол - XMPP

Як випливає з назви, AMQP обслуговує виключно черги. Він пересилає транзакційні сполучення між серверами. У протоколі AMQP велику увагу

приділено боротьбі з втратою повідомлень. Різні комунікаційні лінії – від постачальників контенту до комутаторів каналів і від списків черговості до користувачів – використовують протокол TCP, який забезпечує високонадійне двухточечное з'єднання. Крім того, кінцеві точки повинні підтверджувати прийняття кожного повідомлення. Даний стандарт описує також опціональний режим транзакцій з формальною багатофазною послідовністю відновлення транзакцій. Програмне забезпечення AMQP сфокусовано на спостереженні за всіма повідомленнями і забезпеченні їх доставки за призначенням, незалежно від наявності збоїв і перезавантаження системи. AMQP використовується головним чином в обміні діловими повідомленнями. Зазвичай під «пристроями» розуміють мобільні телефони, що підтримують зв'язок з центрами обробки даних в операційних офісах. У разі IoT AMQP найкращим чином підходить для реалізації аналітичних функцій на базі серверів WiFi - це набір стандартів бездротового зв'язку IEEE 802.11, який можна використовувати для побудови бездротової локальної обчислювальної мережі IoT на основі стека TCP / IP. Стек протоколів стандарту IEEE 802.11 складається з фізичного рівня і канального рівня з підрівнями управління доступом до середовища і логічної передачі даних.

Протоколи IEEE 802.11 (WiFi) відносяться до рівня мережевих інтерфейсів в стеці TCP / IP. Бездротова локальна мережа WiFi підключена до Internet за допомогою шлюзу або маршрутизатора. Для побудови локальних бездротових мереж IoT організація Wi-Fi Alliance створила нову специфікацію IEEE 802.11s, яка забезпечує технологію побудови пористих мереж. Крім того, для IoT створений і новий стандарт Wi-Fi HaLow (специфікація IEEE 802.11ah) з низьким енергоспоживанням.

BLE 4.2 це нова версія стандарту Bluetooth Low Energy, яка призначена для побудови бездротових мереж типу Smart Home (рисунок 1.12).

Новий стандарт Bluetooth Mesh з комірчастою топологією впроваджений в 2016р. Стек комунікаційних протоколів BLE 4.2 підтримує мережевий протокол IPv6 over BLUETOOTH (R) Low Energy або 6LoWPAN, протоколи

транспортного (UDP, TCP) і прикладного (CoAP і MQTT) рівнів. Версія BLE 4.2 забезпечує мінімальне енергоспоживання обладнання і вихід в IP-мережі.

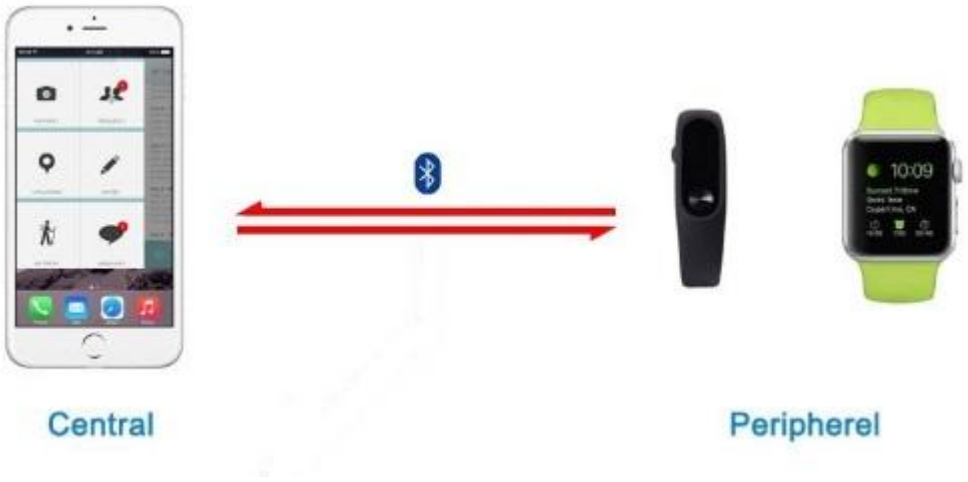

Рисунок 1.12 – Стандарт - BLE

ZigBee – протокол бездротових сенсорних мереж. ZigBee це по суті не окремий протокол, а специфікація мережевих протоколів верхнього рівня (застосувань і мережевого), що використовують сервіси нижніх рівнів управління доступом до середовища і фізичного рівня, регламентованих стандартом IEEE 802.15.4 (рисунок 1.13).

ZigBee та IEEE 802.15.4 описують бездротові персональні обчислювальні мережі. Специфікація ZigBee орієнтована на програми, що вимагають гарантованої безпечної передачі даних при відносно невеликих швидкостях і можливості тривалої роботи мережевих пристроїв від автономних джерел живлення. Основна особливість технології ZigBee полягає в тому, що вона при малому енергоспоживанні підтримує не тільки прості топології мережі («точка-точка», «дерево» і «зірка»), а й самоорганізовану і самовідновлювану порожнисту (mesh) топологію з ретрансляцією і маршрутизацією повідомлень.

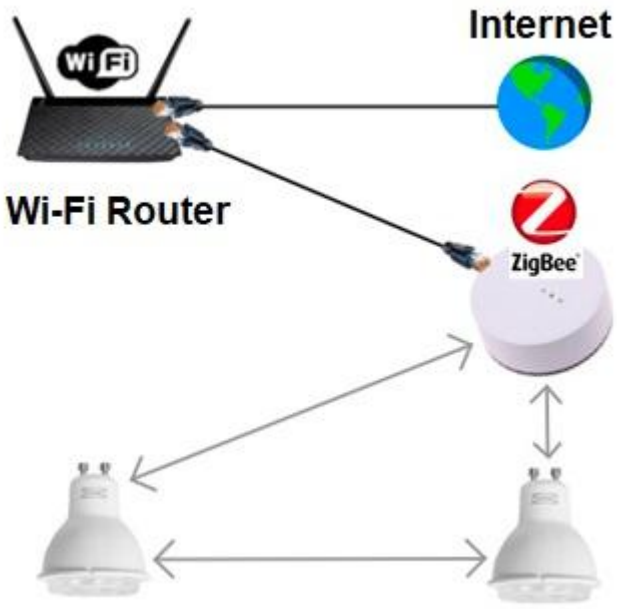

Рисунок 1.13 – Протокол - ZigBee

Крім того, специфікація ZigBee містить можливість вибору алгоритму маршрутизації, в залежності від вимог програми та стану мережі, механізм стандартизації застосувань, профілі застосувань, бібліотека стандартних кластерів, кінцеві точки, прив’язки, гнучкий механізм безпеки, а також забезпечує простоту розгортання, обслуговування та модернізації.

1.3 Постановка задачі дослідження

Сформулюємо задачу дослідження для магістерської кваліфікаційної роботи, як завдання розробки моделей і алгоритмів, що сприяють вибору оптимальних режимів інформаційної взаємодії в мережах IoT. При вирішенні поставленого завдання засобами моделювання будемо оцінювати функціональну залежність між набором параметрів P, які задають мережу IoT кількісно і ймовірносно-тимчасовими характеристиками H, що описують інформаційну взаємодію якісно, тобто формально:

$$H = f(P), \qquad (1.1)$$

У такій постановці це дозволить при різних умовах вирішувати всі три види завдань моделювання, необхідних при проектуванні:

- пряму – оцінювати характеристики при наявних параметрах мережі IoT;

- зворотну – при заданих допустимих значеннях характеристик проектувати мережу IoT з елементів з відповідними параметрами;

- налаштування – будувати моделі, засновані на запропонованих методах і алгоритмах, що дозволяють виявити функціональну залежність між множинами P і H.

До множини параметрів P віднесемо потокові і структурні метрики:

- кожний СП характеризується інтенсивністю ідентифікації себе в просторі IoT, періодами активності і пасивності;

- кожний вузол IoT задається параметрами продуктивності;

- структура зв’язків відповідає топології mesh;

- елементи зв’язків СП-вузол і вузол-вузол задаються часом передачі виклику в прямому і зворотному напрямках;

- значення ймовірностей зайнятості або відсутності зв’язку.

Мережа побудована як сукупність «туманів», на які поділяється територія покриття, кількість «туманів» теоретично не обмежена. В одному такому «тумані» може розміщуватися кілька шлюзів, які підключаються до магістрального інформаційного каналу за допомогою оптичного або електричного кабелю або по радіоканалу з використанням систем широкосмугового доступу. Шлюзи в «тумані» з’єднуються між собою по радіоканалу. Протоколи, які реалізують функції транспортування в mesh-мережі засновані на створенні таблиці маршрутизації з контролем стану транспортного каналу і підтримкою динамічної маршрутизації, що дозволяє кожному з них відправляти трафік за оптимальним маршрутом між сусідніми вузлами. При втраті будь-якого з вузлів відбувається автоматичне перенаправлення трафіку за іншим маршрутом, що гарантує не тільки

доставку трафіку, а доставку за мінімальний час. В умовах різких стрибків трафіку як всередині мережі, так і на її кордонах проблема може вирішуватися установкою нових шлюзів в межах сенсорної мережі, інтеграція яких в існуючу мережу відбувається автоматично. Збільшення зон покриття зводиться до додавання в мережу нових СП та шлюзів, що відбувається так само автоматично і таким чином виконується масштабування мережі IoT.

2 МОДЕЛІ ОЦІНКИ ЙМОВІРНОСНО-ЧАСОВИХ ХАРАКТЕРИСТИК ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

З урахуванням фундаментальних характеристик мереж IoT при розробці моделі інформаційної взаємодії вдамося до імітаційного моделювання (ІМ). У практичній реалізації імітаційне моделювання спирається на чотири парадигми: дискретно-подієве моделювання, динамічне моделювання, системна динаміка в сенсі Форрестера і мультиагентний підхід. Всі чотири «парадигми», по суті, просто різні реалізації ІМ, різні підходи до побудови траєкторій зміни станів. Всі вони використовують причинно-наслідковий механізм просування процесів в часі. Відмінності відносяться лише до вибору того чи іншого набору базових математичних і програмних об’єктів, а логіка імітації процесів однакова. Побудова траєкторії функціонування об’єкта, що моделюється, виконується просуванням системного часу. З точки зору реалізації математичних і програмних об’єктів зупинимося на мультіагентному моделюванні інформаційної взаємодії (рисунок 2.1).

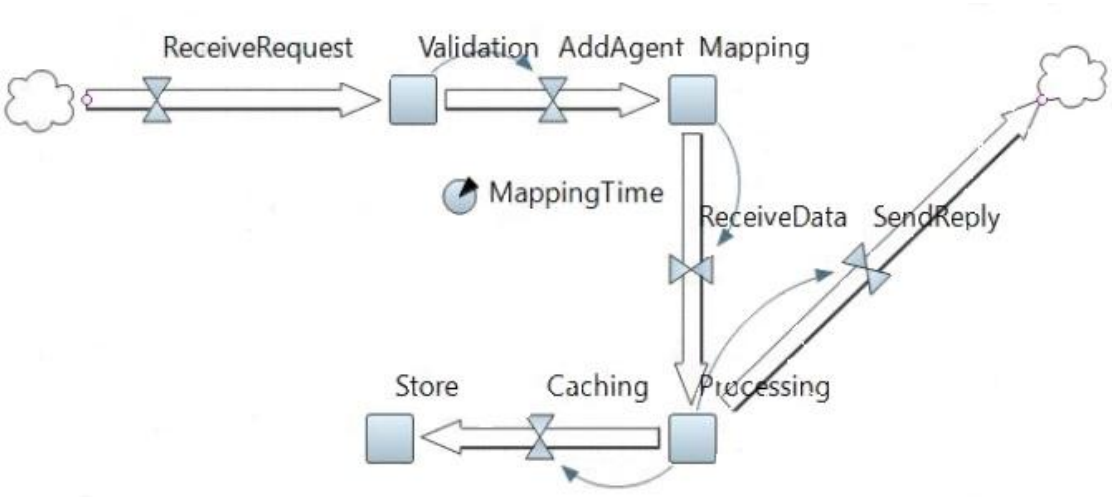

Рисунок 2.1 – Імітаційна модель взаємодії

Модель функціонує наступним чином. Стохастичним чином задані

запити надходять від agent network. Якщо agent проходить валідацію і сертифікований на прийом/передачу інформації і передає запит вперше з моменту виявлення в network, то він додається в «карту» network, для ідентифікації його в просторі. Після обробки та збереження інформації в пам’яті, відбувається відправка керуючої команди від server до agent, на яку agent повинен відправити нотифікацію про отримання.

В процесі проходження всіх етапів схеми можуть виникнути такі ситуації.

1. Запит agent на передачу даних відхилений в силу виникнення колізій джерел даних або маршрут для передачі ще не побудований.

2. Багаторазове додавання одного і того ж agent в карту. Проблема вирішується шляхом видалення об’єкта з карти, якщо після закінчення заданого часу від нього не надходить відповідь.

3. «Зациклення» – відправка однієї і тієї ж команди agent після відключення/підключення. Якщо agent не може виконати передану команду (виражається у відсутності даних, які очікується отримати у відповідь), то система буде пропонувати виконати цю команду знову до тих пір, поки вона не буде виконана, або після закінчення певної кількості спроб, інформація про які зберігається в пам’яті.

4. Запит успішно проходить – інформаційна взаємодія відбулася.

Передбачається, що мобільний об’єкт має можливість переміщатися вільно, або дотримуючись певного алгоритму. У процесі свого переміщення він може залишати і входити в зону покриття мережі. В залежності від стандарту і використовуваного частотного діапазону радіус покриття може відрізнятися (IEEE 802.11). Таким чином, перші два блоки схеми описують рух і підключення agent до network, після якого стає можливим обмін інформацією з іншими agent і учасниками network. Підключившись, agent починає передавати і отримувати повідомлення. Слід зазначити, що валідація agent (дозвіл на прийом/передачу) проводиться на рівні всієї системи. При відсутності відповіді на повідомлення, agent вважається відключеним від

network. Крім ймовірності відключення agent від network, існує також можливість виникнення колізії між декількома об’єктами, які намагаються одночасно передати інформацію.

2.1 Оцінка часу доступу в foggy computing з дозволом колізій джерел даних

Всі методи доступу розглядаються в тимчасовій області. Колізією або конфліктом називається накладення сигналів від різних СП один на одного. Пропонуються наступні моделі доступу в foggy computing з дозволом колізій джерел даних, що реалізують режими:

- опитування;
- переривань;
- множинний доступ.

2.1.1 Модель доступу в режимі опитування

У такій системі є центральний node (route, gateway або server) і деяка кількість СП, яка в силу динамічних змін заздалегідь «невідома» node. Сенсорні пристрої починають передачу даних тільки за запитом центрального node. Якщо у СП немає підготовленого для передачі пакета даних, то спеціальний логічний механізм СП формує ідентифікаційний пакет, що містить унікальний ідентифікаційний номер (ID) сенсорного пристрою. Завдання центрального node ідентифікувати всі сенсорні пристрої, які знаходяться в зоні його покриття і якщо у СП є дані для передачі, то прийняти їх. Процес опитування – часовий інтервал, який розділений на блоки – вікна. Вікна – нефіксовані відрізки часу, розмір яких визначається кількістю слотів, на які він ділиться. Розмір слота – фіксована величина для кожного сенсорного пристрою. Так як слот – це теж часовий інтервал, його розмір визначається швидкістю передачі даних від СП до node, тобто його визначає обладнання,

що використовується в системі. Приклад поділу часу опитування наведено на рисунку 2.2.

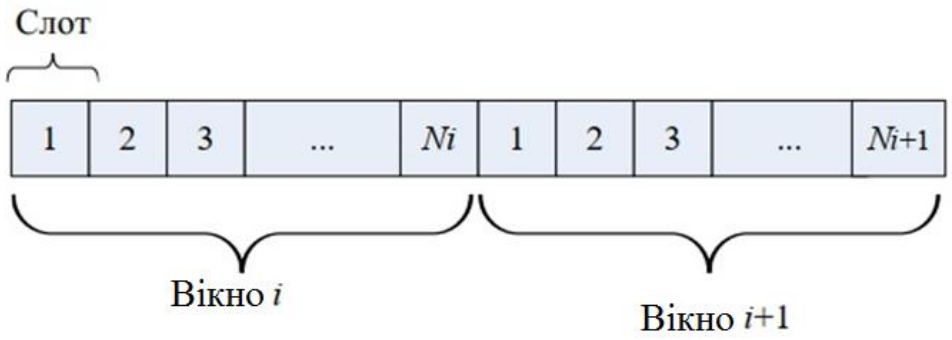

Рисунок 2.2 – Поділ часу опитування на вікна і слоти

На початку процесу node посилає сигнали «опитування» всім сенсорним пристроям, які знаходяться в зоні його покриття. У цих сигналах міститься час початку доступу і тривалість, тобто кількість слотів. СП, прийнявши ці сигнали, випадковим чином вибирають слот, в якому будуть передавати свої дані. В процесі доступу в слоті можливе виникнення трьох подій.

Подія № 1. Порожньо – в тому випадку, коли жоден з СП не вибрав поточний слот для передачі даних.

Подія № 2. Успіх – коли тільки один СП передає дані в поточному слоті.

Подія № 3. Конфлікт – коли більше одного СП починають передавати дані в поточному слоті.

Опитування СП, які перебувають в зоні покриття центрального node закінчується, коли у вікні з’являються тільки слоти з успішною передачею і порожні слоти. Приклад доступу в режимі «опитування» представлено на рисунку 2.3. Центральний node посилає сигнал «опитування» зі значенням часу початку доступу і кількості слотів, в даному випадку – 5. Сенсорні пристрої, що знаходяться в зоні покриття, в даному прикладі їх 4 штуки, приймають сигнал і за отриманими даними вибирають випадковим чином слот від 1 до 5. На рисунку 2.3 видно, що 4-й СП вибрав перший слот, а 1-й і 2-й

СП вибрали другий слот, 3-й СП вибрав 4-й слот. Відповідно до вибраного слоту, СП передають свої ідентифікатори і дані при наявності.

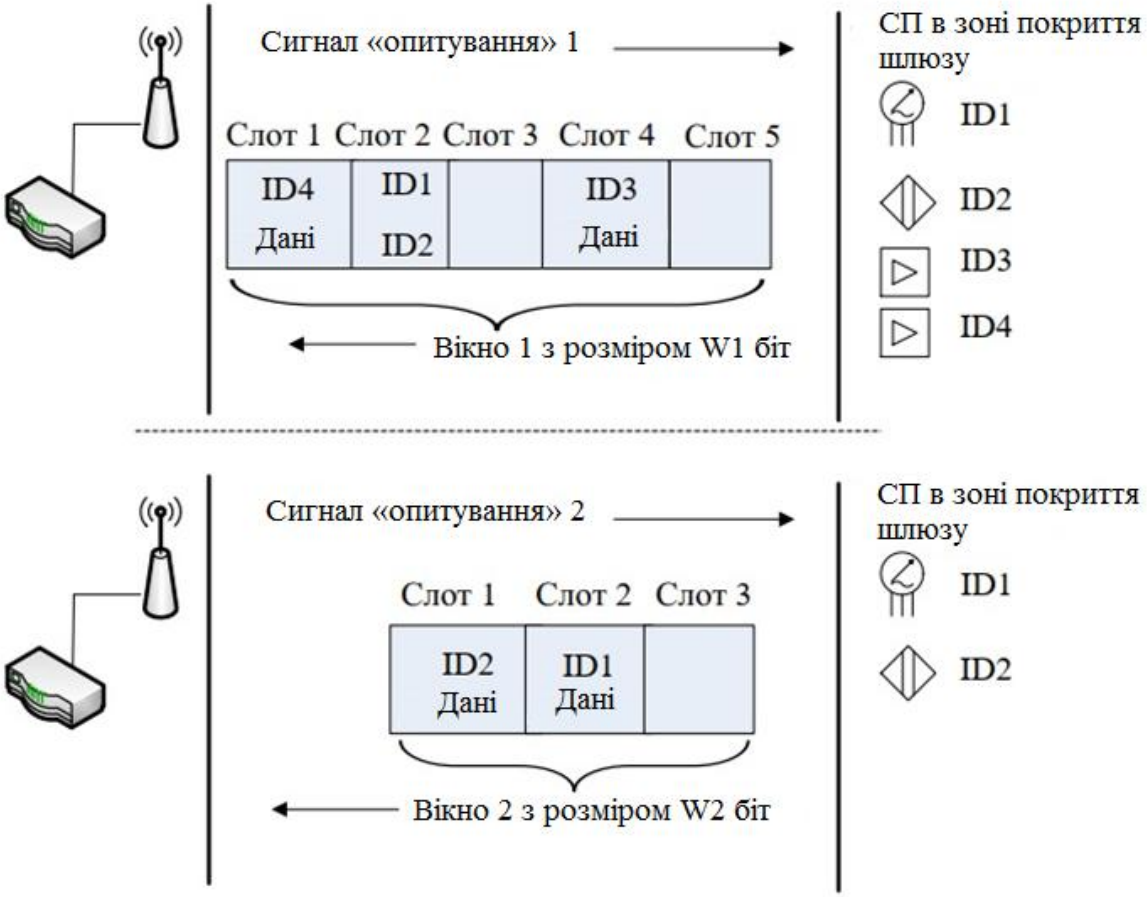

Рисунок 2.3 – Приклад роботи режиму «опитування»

Центральний node аналізує кожен слот і виконує деякі дії. Якщо слот - успішний, то він реєструє СП по його ідентифікатору і збільшує лічильник успішних вікон, якщо слот – порожній, збільшується лічильник порожніх вікон, якщо слот – конфліктний, збільшується лічильник конфліктних слотів. По завершенню поточного вікна, відбувається обчислення розміру наступного вікна. Розмір наступного вікна W визначається від кількості конфліктів Er поточного вікна за правилом:

$$W = Er \cdot 2 + 1, \qquad (2.1)$$

Лічильник конфліктних слотів обнуляється. Даний спосіб є евристичним, оскільки параметри вибираються природним шляхом. У прикладі на малюнку 2.3 node розрахував розмір наступного вікна рівного 3-м слотів.

Час, необхідний для виконання операції опитування залежить від фізичних характеристик каналу взаємодії, які і визначають затримку поширення. Час обслуговування t_s сенсорного пристрою в режимі опитування формується таким чином:

$$t_s = t_p + \frac{\bar{b}}{C}, \qquad (2.2)$$

де t_p – час, що витрачається на сигнал опитування, с;

$\bar{b}$ – середнє значення довжини пакета, біт;

C – пропускна здатність каналу, біт/с.

Відповідно, повний цикл взаємодії N сенсорних пристроїв і центрального вузла становить $T = N \cdot t_s$. Зв’язок цих змінних представлена на рисунку 2.4. Час t_p включає як час формування опитування, так і затримку поширення. Ставлення b/C – це час, необхідний для передачі b біт зі швидкістю C біт в секунду.

Якщо опитуваний СП не має готового повідомлення для передачі, то b - дуже мало, оскільки передається тільки ID сенсорного пристрою. Якщо ж в буфері сформований пакет даних, то b дорівнює числу біт ідентифікаційного номера СП плюс пакет даних.

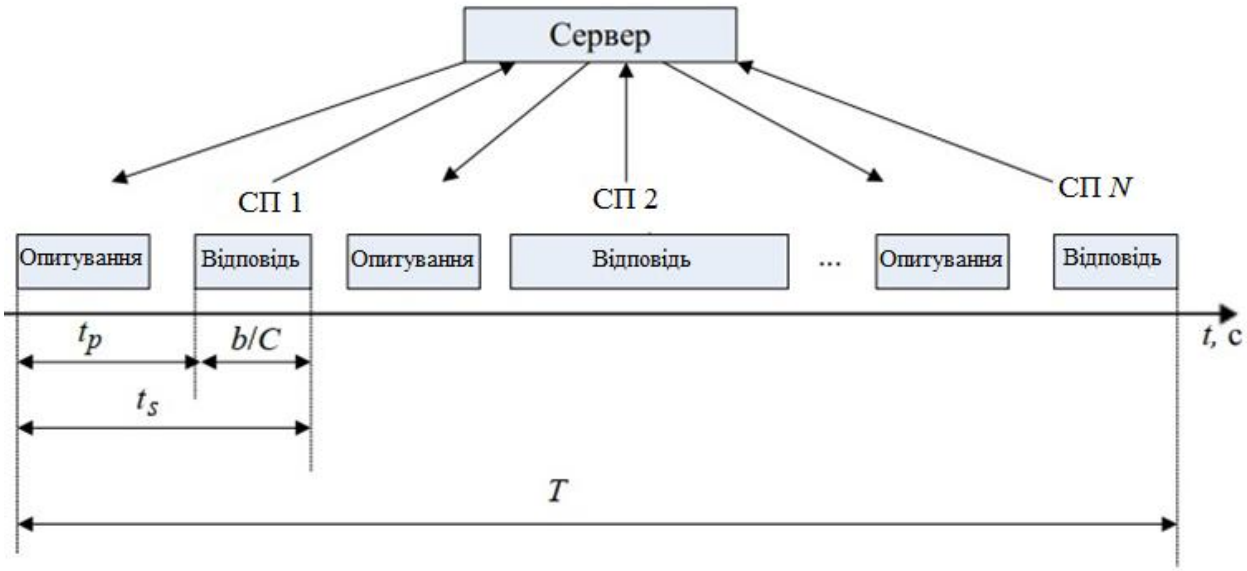

Рисунок 2.4 – Тимчасова діаграма реалізації режиму опитування

Відношення (2.2) дозволяє оцінити середній час обслуговування одного СП за умови, що дисперсія b значно менше, ніж $\overline{b}$. Якщо кожен СП передає в середньому пакет в секунду, то при наявності в системі N сенсорних пристроїв, загальна інтенсивність потоку даних складе N пакетів в секунду, а середній інтервал між їх надходженнями 1/N с.

Отже, щоб уникнути необмеженого зростання черг, час обслуговування t_s повинно відповідати умові:

$$\overline{t}_s = \overline{t}_p + \frac{\overline{b}}{C} \le \frac{1}{\lambda N}, \qquad (2.3)$$

Вирішуючи (2.3) щодо C, отримаємо умову, яка гарантуватиме відсутність черги для кожного сенсорного пристрою:

$$C \ge \frac{\lambda N \overline{b}}{1 - \lambda N t_p}, \qquad (2.4)$$

Це пояснюється тим, що будь-який з СП опитується кожні 1/λ секунди і в той же час в ньому формується черговий пакет даних.

2.2 Модель оцінки ймовірнісно-часових характеристик інформаційної взаємодії в мережі IoT

У бездротових сенсорних мережах число СП в залежності від розв'язуваної задачі може змінюватися від кількох сотень до тисяч. Тому, в специфікаціях Zig Bee число СП, розташованих в одній зоні, може досягати 64000. Мережі великого масштабу і високої щільності з лімітованою пропускною здатністю повинні, до того ж, надавати послуги з певним рівнем якості обслуговування. На відміну від традиційних мереж, бездротові сенсорні мережі організуються випадковим чином, і взаємозв'язки СП в них також випадкові у часі. Сенсорні вузли можуть виходити з ладу внаслідок недостатнього рівня електроживлення, виникнення критичних умов у зовнішньому середовищі, виходу з ладу апаратної частини і т.д.

Якщо вийшло з ладу кілька сенсорних вузлів, це не повинно викликати істотних наслідків як для сенсорної мережі в цілому, так і для її фрагментів. Іншими словами, мережа IoT повинна бути нечутлива до відмови будь-якого СП і продовжувати підтримувати далі необхідний рівень якості обслуговування.

Для обчислювальних мереж якість обслуговування виражається в ймовірносно-часових характеристиках. Відповідно до моделі інформаційної взаємодії, оцінка ймовірносно-часових характеристик інформаційної взаємодії в мережі IoT буде являти собою суму:

$$t_{і.в.} = t_{в.з.} + t_{п.д.}, \qquad (2.5)$$

де $t_{і.в.}$ – час інформаційної взаємодії;

$t_{в.з.}$ – час, необхідний на встановлення з'єднання для інформаційної

взаємодії;

$t_{п.д.}$ – час передачі даних по встановленому з'єднанню інформаційної взаємодії.

Для оцінки $t_{в.з.}$ застосуємо вірогідну модель встановлення з'єднання, з додатком на мережі IoT. Оцінку $t_{п.д.}$ пропонується виконати із застосуванням апарату систем масового обслуговування.

2.2.1 Особливості реалізації імітаційної моделі встановлення з'єднання

Процес встановлення інформаційної взаємодії (ІВ) в мережі IoT може займати деякий час в силу її динамічних властивостей:

- топологія мережі може багаторазово змінюватися в процесі функціонування внаслідок введення нових вузлів;
- відмов існуючих вузлі;
- критичних змін зовнішнього середовища.

Всі ці можливості повинні бути враховані при розробці моделі встановлення з'єднання для інформаційної взаємодії. Встановити інформаційну взаємодію – це значить побудувати логічний канал, що зв'язує сенсорний пристрій зі шлюзом адресата для подальшої передачі по ньому даних.

Таких логічних каналів, що зв'язують джерело і адресат, може бути кілька в силу mesh-топології мережі IoT (рисунок 2.5). Логічний канал складається з фізичних каналів, що зв'язують сусідні СП. Побудова логічного каналу виконується надсиланням сигналу-виклику на встановлення з'єднання. При проходженні виклику від одного СП до іншого стан фізичного каналу приймає один з двох станів:

- «1» – канал зайнятий, і дані по ньому не пройдуть;
- «0» – канал вільний для передачі даних.

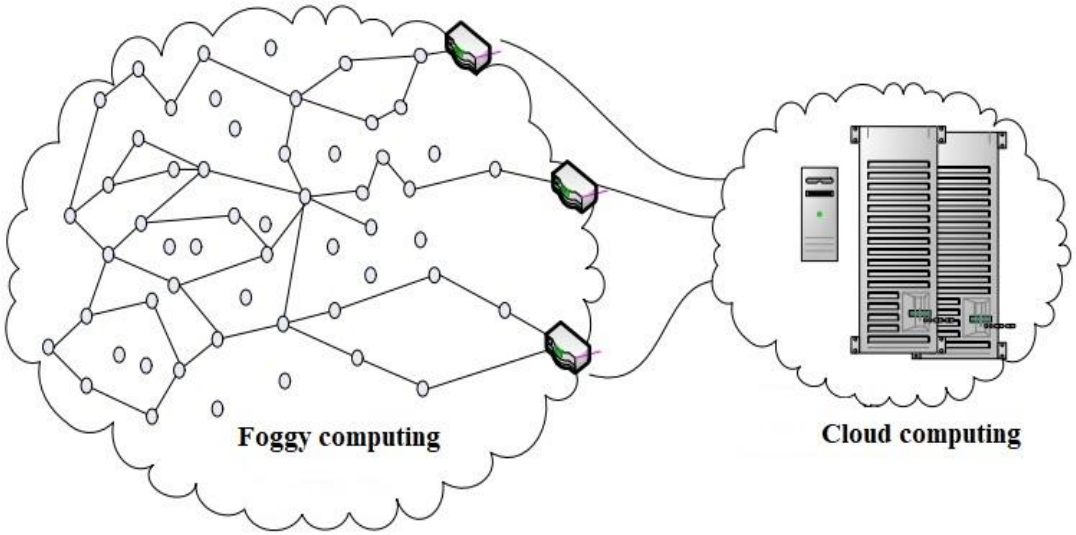

Рисунок 2.5 – Логічні канали для передачі даних від СП в «хмару»

Повторні спроби встановлення з’єднання надають стохастичності цьому процесу, тому що виникають вимушені повернення на попередні СП і число фізичних каналів, пройдених викликом при його доставці адресату, виявляється випадковим числом.

Облік даного аспекту дозволяє вдатися до імітаційного моделювання процесу встановлення логічного каналу для інформаційної взаємодії. Таким чином, час встановлення інформаційної взаємодії $t_{в.з.}$ визначимо як випадкову величину, яка може бути знайдена виразом:

$$t_{в.з.} = \sum_{i=1}^{n_k} t_{k_i} + \sum_{i=1}^{n_o} t_{o_i} + n_n t_n , \qquad (2.6)$$

де n_k – число фізичних каналів в логічному каналі, побудованого від СП джерела до СП-адресату;

n_o – число фізичних каналів, на які виклик повернувся назад при пошуку альтернативного логічного каналу;

n_n – число спроб в зафіксованій реалізації процесу встановлення ІВ.

У загальному випадку n_n визначається:

$$0 \le n_n < n_{доп.}, \qquad (2.7)$$

де $n_{доп}$ – допустима кількість спроб встановлення ІВ.

Кожен експеримент на імітаційній моделі дає реалізацію трьох випадкових величин: n_k, n_o и n_n, що дозволяє оцінити час встановлення інформаційної взаємодії $t_{в.з.}$ відповідно до виразу (2.6). Отримане значення $t_{в.з.}$ визначає результат встановлення ІВ:

- якщо $t_{в.з.} \le t_{доп.}$, то ІВ встановлено;
- якщо $t_{в.з.} > t_{доп.}$, то ІВ встановлено, але з низькою якістю обслуговування, і для даних термінової доставки це має критичне значення, тому що вони могли втратити свою актуальність;
- якщо $n_n > n_{доп.}$, то з'єднання не встановлено.

Вихідними даними для моделювання є:

- безліч логічних каналів, які можуть бути побудовані від джерела до адресата, позначимо як L_{ij};
- характеристика фізичних каналів: час передачі сигналу-виклику з фізичного каналу в прямому і зворотному напрямках;
- значення ймовірностей повної зайнятості фізичних каналів;
- допустимий час встановлення ІВ;
- число спроб встановлення ІВ;
- час, виділений на повторну спробу – переключення на інший логічний канал.

У моделі накопичуються статистики, що дозволяють оцінити ймовірність встановлення ІВ за час, що не перевищує допустимий, а також середні і середньоквадратичні значення $t_{в.з.}$, що характеризують процес встановлення ІВ в мережі IoT.

На всій безлічі логічних каналів L_{ij} проводиться їх упорядкування за кількістю зайнятих фізичних каналів *c*, тобто $(c = c_{min},...,c_{max})$. В окремому експерименті розігрується число *c* номерів зайнятих фізичних каналів в безлічі L_{ij} і на отриманій реалізації імітується процес проходження виклику від джерела і до адресата j. За фактом встановлення ІВ фіксуються значення $n_{тр}$, $n_{от}$ та $n_{п}$. процедура повторюється N раз.

За результатами експериментів обчислюється середня оцінка часу встановлення ІВ. Реалізація кількості втрачених фізичних каналів *c* зводиться до «вибору навмання» номерів каналів з d можливих, $c \in d$. Черговий номер втраченого фізичного каналу z визначається за формулою:

$$z = \lceil Ud + 1 \rceil, \tag{2.8}$$

де U – випадкове число, $U \in [0,1]$, отримуване шляхом звернення до датчика випадкових чисел. Дужки $\lceil\ \rceil$ означають округлення в меншу сторону.

Фізичному каналу з номером z присвоюється «1» в безлічі L_{ij}.

Процедура визначення z повторюється *c* раз. Задача розрахунку характеристик встановлення ІВ може бути зведена до задачі оцінювання математичного очікування $M\xi$ дискретної випадкової величини:

$$\xi = f(\alpha), \tag{2.9}$$

де $\alpha = (\alpha_1,...,\alpha_d)$ має закон розподілу ймовірностей p (тобто $\alpha \sim p$), який відомий.

Випадкова величина ξ приймає два значення, тобто $\xi\{0,1\}$:

- ξ=0 відповідає встановленню з’єднання;
- ξ=1 відповідає невстановленню з’єднання.

Значення $M\xi = P\{\xi = 1\}$ має сенс ймовірності невстановлення з'єднання. Випадкова величина ξ невироджена, тобто $0 < M\xi < 1$.

Інтерпретуємо випадкову величину α як вектор $\alpha = (\alpha_1^{\upsilon},...,\alpha_d^{\upsilon})$, що відображує стан фізичних каналів, які входять в модельовану безліч L_{ij} в сенсі їх статусу: є або немає. З урахуванням класифікації L_{ij} по *c*, оцінку $M\xi$ знайдемо у вигляді:

$$M\xi = \sum_{c_{min}}^{c_{max}} M\xi(c), \qquad (2.10)$$

де $M\xi$ – оцінка ймовірності невстановлення ІВ при наявності *c* фізичних каналів, які не проводять виклик.

Для завдання станів $L_{ij}(c)$ на k-му розіграші застосовується випадковий вибір номерів фізичних каналів *c*, які не проводять виклик на встановлення ІВ.

В результаті вектор α отримує конкретну реалізацію x, що містить *c* одиниць і $(d - c)$ нулів. Відповідно до правила проходження виклику по безлічі альтернативних логічних каналів L_{ij} і правилу встановлення ІВ обчислюється значення:

$$\xi(x \mid c)_k = f[L_{ij}^k], \qquad (2.11)$$

де $\xi(x \mid c)_k$ – результат встановлення (невстановлення) ІВ при k-му випробуванні (k-й реализації L_{ij}), $\xi(x \mid c)_k \in (0,1)$, і ймовірність отриманої реалізації:

$$p(x) = p[L_{ij}^k], \qquad (2.12)$$

Значення $\xi(x\,|\,c)_k = 1$ має місце, якщо сигнал виклику не дійшов до адресата (не побудовано жодного логічного каналу з безлічі L_{ij}), або число спроб перевищило допустиме значення, або виклик дійшов до адресата і встановлено ІВ, але без належної якості обслуговування $t_{в.з.} > t_{доп.}$. Оцінка ймовірності встановлення ІВ між СП при *c* втрачених фізичних каналів на безлічі всіх L_{ij} визначається у вигляді:

$$M\xi(c) = \frac{C_d^c}{N_{2c}} \sum_{k=1}^{N_{2c}} p(L_{ij}^k \,|\, \xi(x\,|\,c) = 1), \qquad (2.13)$$

де N_c – число розіграних станів (реалізацій) безлічі L_{ij}.

Таким чином, вираз (2.13) повністю відображає ймовірнісний підхід до встановлення ІВ в IoT з топологією Mesh.

3 ЕКСПЕРИМЕНТ НА МОДЕЛІ ВСТАНОВЛЕННЯ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ

Постановка імітаційного експерименту. Побудуємо залежності абсолютних і імовірнісних характеристик встановлення інформаційного з'єднання, такі як ймовірність встановлення інформаційної взаємодії $P_{в.в.}$ та часу встановлення з'єднання $t_{в.з.}$ від:

- кількості втрачених каналів c;
- кількості втрачених сенсорних пристроїв N;
- кількості спроб $n_п$.

Експеримент проведено на мережі з топологією mesh, наведеної на рисунку 3.1.

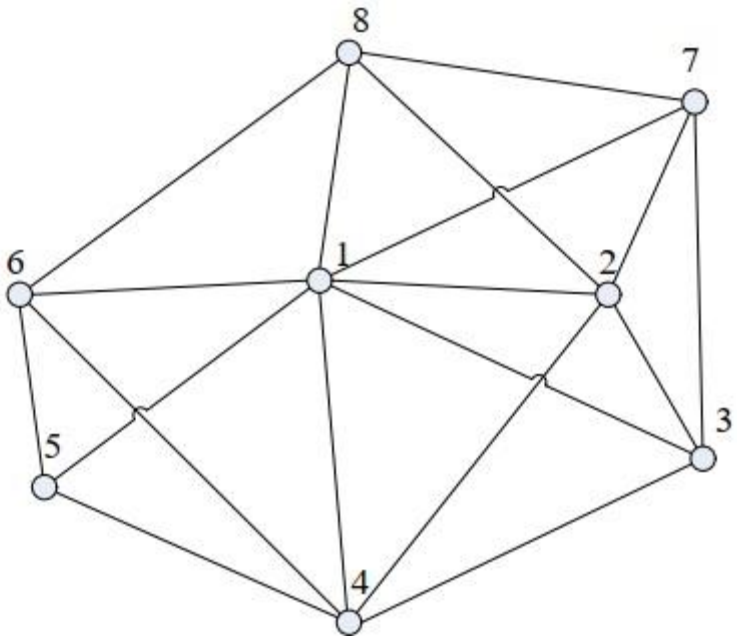

Рисунок 3.1 – Топологія Mesh-мережі

Задані такі параметри, що характеризують СП і канали зв'язку:

- пропускна здатність всіх каналів зв'язку - 9600 бод;

- швидкість проходження і-го фізичного каналу в прямому і зворотному напрямках однакові, тобто $t_{k_i} = t_{o_i}$;

- час переключення на інший маршрут $t_п - 10^{-2}$ мс;

- допустимий час на встановлення з'єднання $t_{доп.}$ можна варіювати в залежності від вимог і рекомендацій до доставки трафіку IoT.

Зібрані в результаті моделювання статистики дозволяють побудувати важливі ймовірносно-часові залежності, що характеризують інформаційну взаємодію мережі IoT. На рисунку 3.2 і рисунку 3.3 наведені залежності ймовірності встановлення з'єднання від допустимого часу на доставку виклику при фіксованих n_n і *c*. При зміні значень n_n і *c* характер графіків не змінюється. Призначення цих залежностей – знайти необхідні параметри, що забезпечують гарантований час встановлення з'єднання, наприклад, якщо в оточенні восьми СП буде втрачено три канали і одна спроба побудувати інший логічний канал, то для забезпечення 100% встановлення інформаційної взаємодії необхідний час – не менше 5 мс (рисунок 3.2).

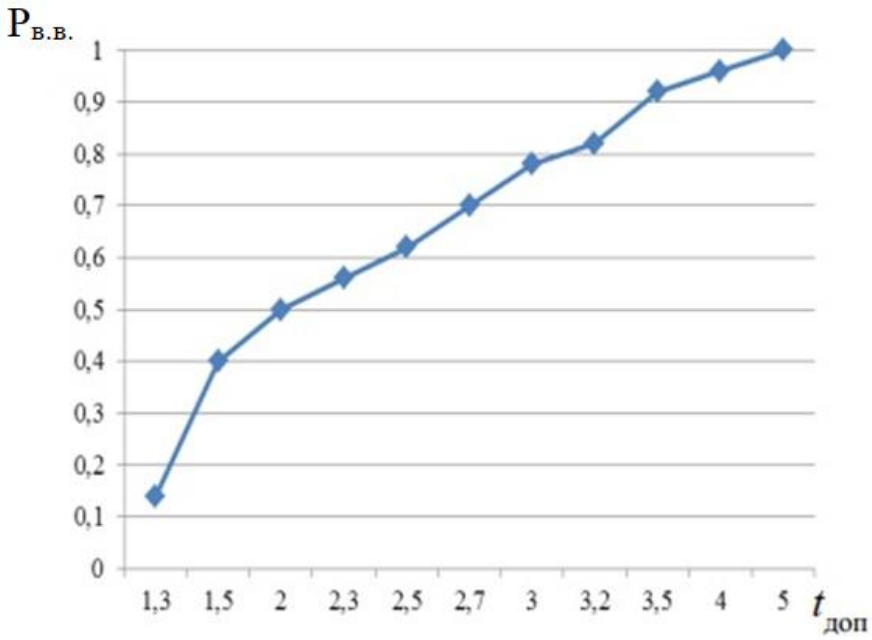

Рисунок 3.2 – Залежність $P_{в.в.}$ від $t_{доп.}$

А при тих же умовах і при наявності трьох спроб, необхідний час – не менше 4 мс (рисунок 3.3).

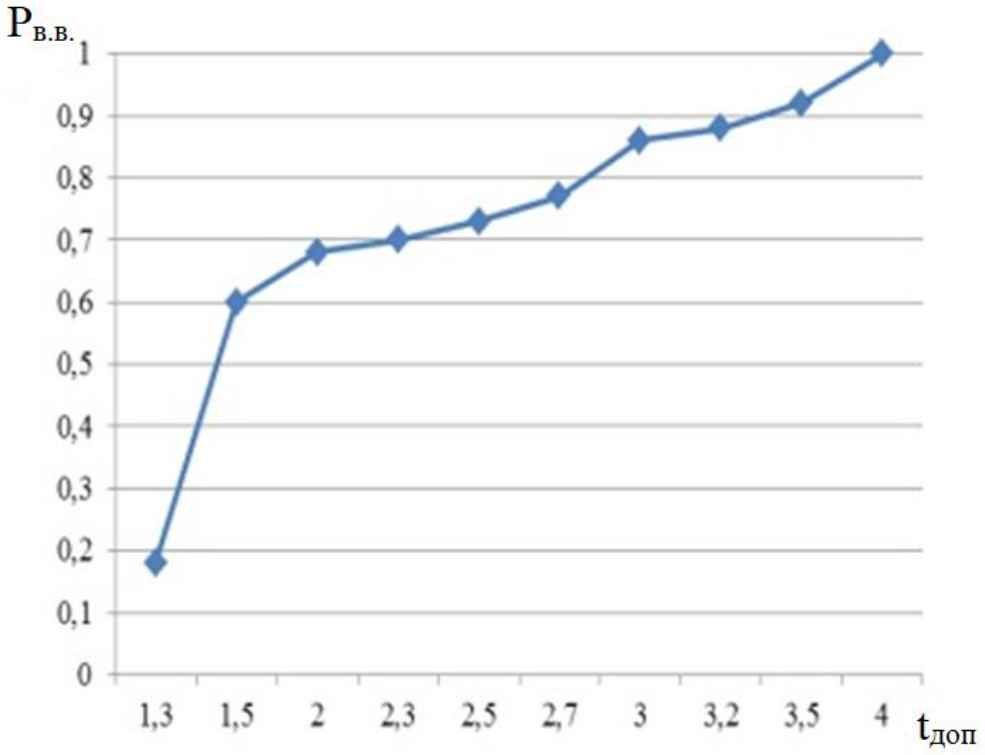

Рисунок 3.3 – Залежність $P_{в.в.}$ від $t_{доп.}$

Залежності ймовірності встановлення з'єднання від числа втрачених каналів і втрачених СП наведені на рисунку 3.4 і рисунку 3.5 відповідно, результати отримані при $n_п = 3$. Очевидно, що ймовірність встановлення з'єднання знижується зі збільшенням кількості втрачених каналів і СП.

Графіки дозволяють знайти максимально можливу кількість втрачених каналів і СП, при яких гарантується встановлення інформаційної взаємодії за допустимий час.

На рисунку 3.6 приведена залежність $P_{в.в.}$ від $n_п = 3$, а на рисунку 3.7 приведена залежність $t_{в.з.}$ від кількості спроб $n_п = 3$. Призначення графіків на рисунку 3.6 і рисунку 3.7 – визначити кількість необхідних спроб при відомій кількості втрачених елементів мережі.

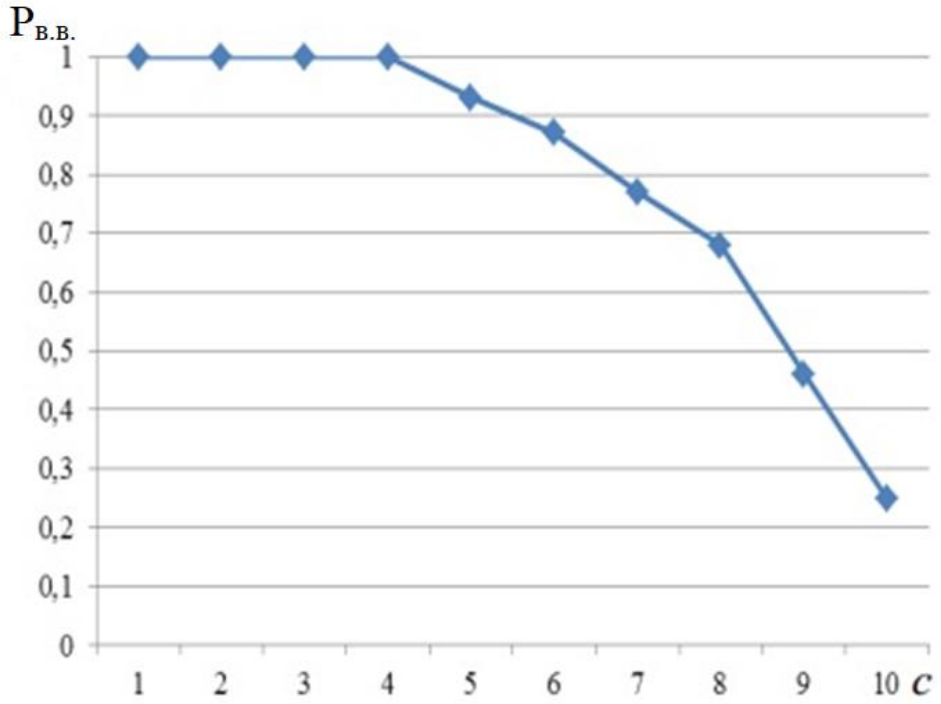

Рисунок 3.4 – Залежність $P_{в.в.}$ від кількості втрачених каналів *c*

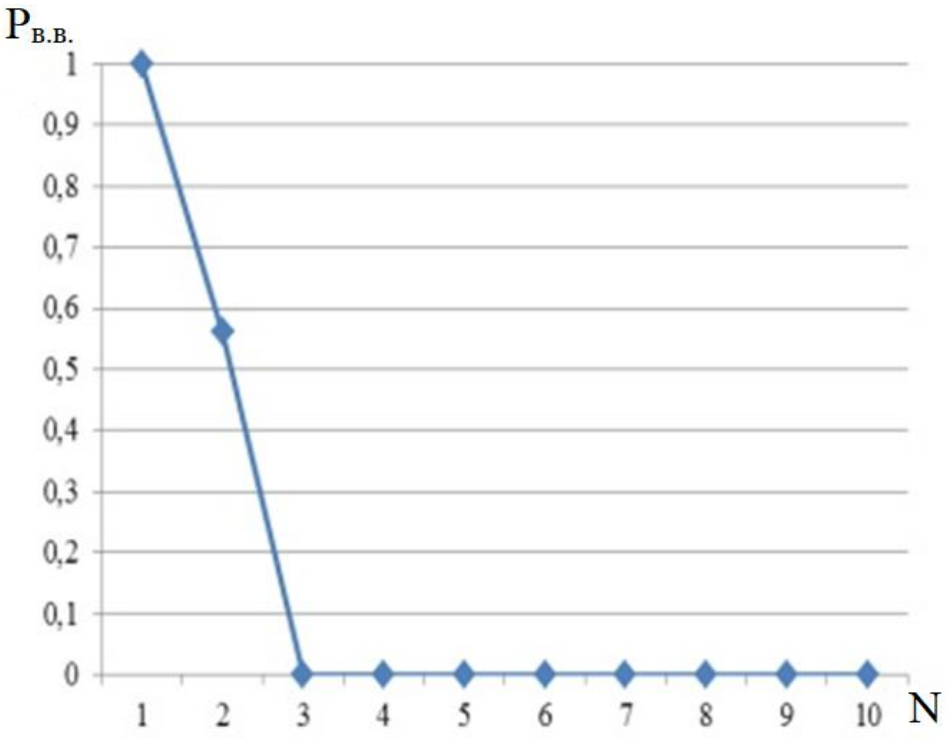

Рисунок 3.5 – Залежність $P_{в.в.}$ від кількості втрачених сенсорних пристроїв N

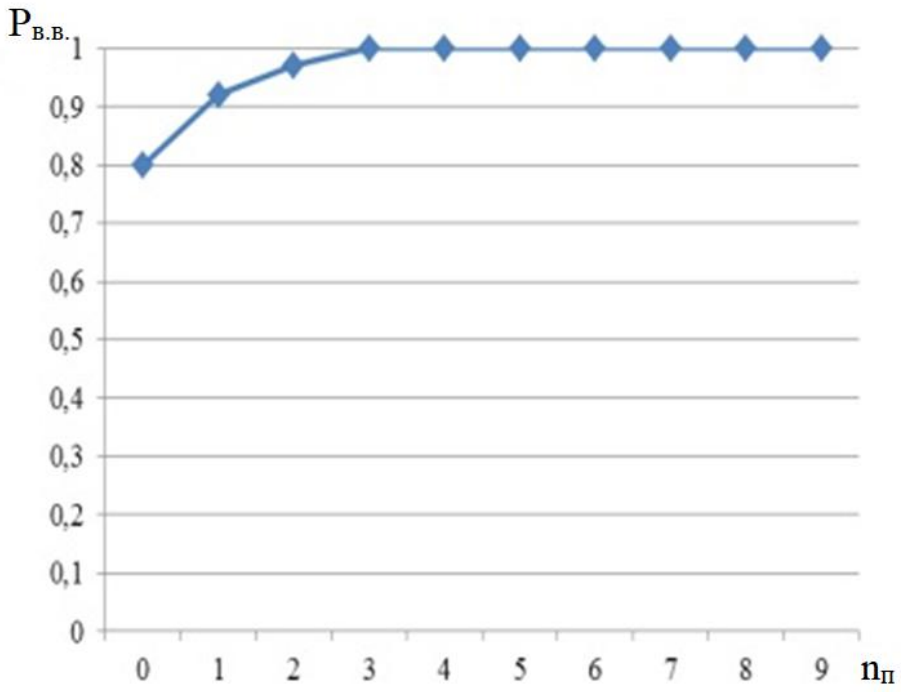

Рисунок 3.6 – Залежність $P_{в.в.}$ від $n_п$ при с=4

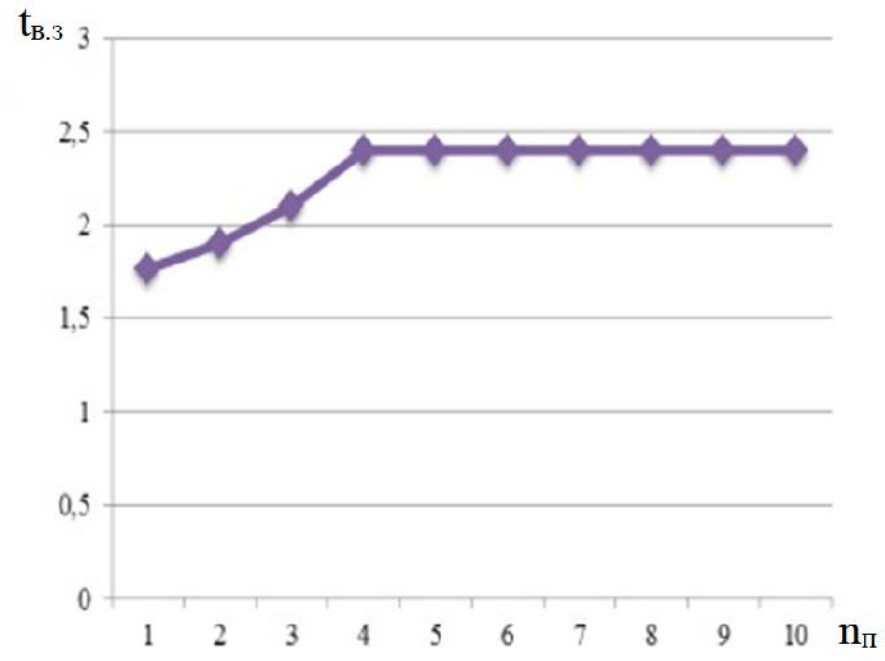

Рисунок 3.7 – Залежність $t_{в.з.}$ від кількості спроб $n_п = 3$.

Оскільки в моделі можна змінювати допустимий час $t_{доп.}$, і за результатами експерименту рекомендувати його значення при дотриманні

необхідної $P_{в.в.}$, то відповідно можна оцінити умовну ймовірність (ймовірність встановлення взаємодії за умови, що час доставки менше допустимого). Графіки на рис.3.8 показують залежність ймовірності $P_{в.в.}$ встановлення з'єднання від числа втрачених каналів *c*.

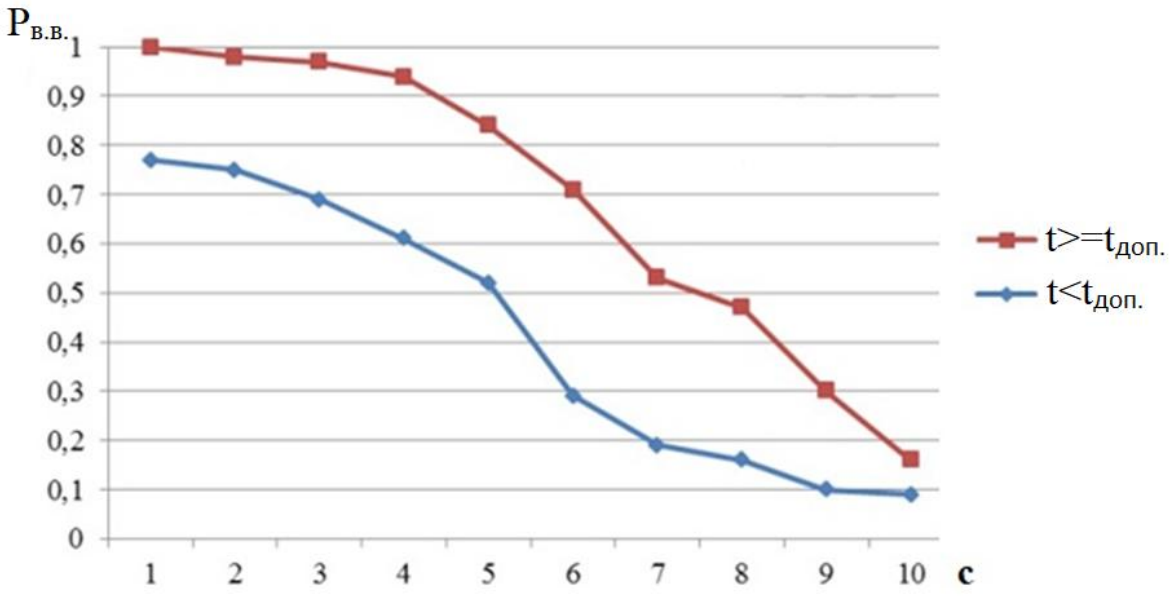

Рисунок 3.8 – Залежність $P_{в.в.}$ від *c*

ВИСНОВКИ

В результаті виконання магістерської кваліфікаційної роботи була досліджена модель інформаційної взаємодії сенсорних пристроїв в мережі IoT.

Виконано аналіз результатів моделювання доступу в туманних обчисленнях, який показав можливість вибору ефективного методу доступу при плановому навантаженні як за кількістю підключених СП, так і по часу отримання доступу.

Проведено експеримент на моделі встановлення інформаційної взаємодії між джерелом і адресатом в мережі Інтернету речей, який показав, що можливе вирішення як прямої задачі моделювання – визначення часу встановлення з’єднання, так і зворотної – підбір параметрів для забезпечення допустимого часу встановлення з’єднання при дотриманні ймовірності гарантованої доставки виклику.

Оскільки в моделі можна змінювати допустимий час $t_{доп.}$, і за результатами експерименту рекомендувати його значення при дотриманні необхідної $P_{у.в.}$, то відповідно можна було оцінити умовну ймовірність (ймовірність встановлення взаємодії за умови, що час доставки менше допустимого).

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ткачов В.М., Токарев В.В., Радченко В.О., Лебедєв В.О. Проблема передачі даних типу BIG DATA у мобільній системі «Мультикоптер- сенсорна мережа» / В.М. Ткачов, В.В. Токарев, В.О. Радченко, В.О. Лебедєв // Системи управління, навігації та зв'язку. - 2017. №2(42). - С.154-157

2. Радченко В.О., Руденко Д.А., Ткачов В.Н., Токарев В.В. Мобильная подсистема «Мультикоптер-сенсорная сеть» в компьютерной системе хранения BIG DATA / В.О. Радченко, Д.А. Руденко, В.Н. Ткачов, В.В. Токарев // Системи управління, навігації та зв'язку. - 2017. №4(44). - С.102-105.

3. Пат. 118921 Україна, МПК H04W 64/00. Спосіб передачі цифрових даних мультикоптерною системою між сегментами розподіленої сенсорної мережі та базовою станцією / В.М. Ткачов, В.В. Токарєв - № u201704085; заявл. 24.04.2017; опубл. 28.08.2017. Бюл. № 16. 5с.

4. Радченко В.А., Токарев В.В., Ткачев В.Н. Мобильная система передачи данных на базе динамически реконфигурируемых мультикоптерных устройств / В.А. Радченко, В.В. Токарев, В.Н. Ткачев // Проблеми інформатизації: тези доповідей V - наук. - техн. конф., 13 - 15 лист. 2017р. - Харків, 2017. - С.36.

5. Рубан И.В., Чурюмов Г.И., Токарев В.В., Ткачев В.Н. Функциональная стойкость универсальной мобильной реконфигурируемой системы при воздействии электромагнитного излучения высокой мощности / И.В. Рубан, Г.И. Чурюмов, В.В. Токарев, В.Н. Ткачев // Информационные технологии и безопасность: (ИТБ-2017), материалы докладов XVII Международной научно-практической конференции, 30 нояб. 2017г. - Киев, 2017. - С.205 - 210.

6. Створення науково-методичних основ забезпечення живучості мережевих систем обміну інформацією в умовах зовнішнього впливу потужного НВЧ випромінювання: звіт про НДР (заключ.) № держреєстрації

0117U003916.: Ф76/109-2017 / Харків. нац. ун-т радіоелектроніки; керівник Г. И. Чурюмов. – Харків, 2017. – 116 с.

7. Ruban I.V., Churyumov G.I., Tokarev V.V., Tkachov V.M. Provision of Survivability of Reconfigurable Mobile System on Exposure to High-Power Electromagnetic Radiation / I.V. Ruban, G.I. Churyumov, V.V. Tokarev, V.M. Tkachov // Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security: (ITS 2017). CEUR Workshop Processing., 30 nov. 2017 y. - Kyiv, 2017. - P. 105-111.

8. Serkov A., Kravets V., Yakovenko I., Churyumov G., Tokariev V., Nannan W. Ultra Wideband Signals in Control Systems of Unmanned Aerial Vehicles / A. Serkov, V. Kravets, I. Yakovenko, G. Churyumov, V. Tokariev, W. Nannan // The 10h IEEE International Conference on Dependable Systems, Services and Technologies: (DESSERT'2019)., 5-7 june, 2019 y. - Leeds, 2019. - P.26 - 29.

9. Серков О. А., Пустовойтов П. Є., Яковенко І. В., Лазуренко Б. О., Чурюмов Г. І., Токарєв В. В., Наннан Ванг. Надширокосмугові технології в системах управління мобільними об'єктами. / О. А. Серков, П. Є. Пустовойтов, І. В. Яковенко, Б. О. Лазуренко, Г. І. Чурюмов, В. В. Токарєв, Ванг Наннан // Сучасні інформаційні системи. - 2019. - Т.3, №2. - С.22-27.

10. Серков О.А., Князєв В.В., Лазуренко Б.О., Яковенко І.В., Чурюмов Г.І., Токарєв В.В. Надширокосмугові технології в задачах забезпечення електромагнітної сумісності рухомих об'єктів / О.А. Серков, В.В. Князєв, Б.О. Лазуренко, І.В. Яковенко, Г.І. Чурюмов, В.В. Токарєв // Проблеми електромагнітної сумісності перспективних бездротових мереж зв'язку (ЕМС-2019):збірник наукових робіт четвертої міжн. наук.-техн. конф., 24 жовт. 2019 р. - Харків, 2019. - С. 55-57.

11. Кривуля Г.Ф., Токарев В.В., Щербак В.К. Моделирование компьютеризированных систем управления с использованием интеллектуальных средств / Г.Ф. Кривуля, В.В. Токарев, В.К. Щербак // Інформаційно-керуючі системи на залізничному транспорті: тези доповідей 32-ї міжн. наук.-практ. конф., 24-25 жовт. 2019р. - Харків, 2019. - С. 90 - 91.

12. Krivoulya G., Tokariev V., Ilina I, Shcherbak V. Mathematical Model for Finding Probability of Detecting Victims of Man-Made Disasters Using Distributed Computer System with Reconfigurable Structure and Programmable Logic / G. Krivoulya, V. Tokariev, I. Ilina, V. Shcherbak // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology: (PIC S&T), 06-09 oct. 2020y. - Kharkiv, 2020. - P.197 - 201.

13. Лебедев О.Г., Ткачев В.Н., Токарев В.В., Чурюмов Г.И. Темпоральная модель адаптации интегрированной информационной системы путем реконфигурации логической структуры / О.Г. Лебедев, В.Н. Ткачев, В.В. Токарев, Г.И. Чурюмов // Комп’ютерні та інформаційні системи і технології: тези доповідей другої міжн. наук. - техн. конф., 18 - 19 квітн. 2018 р. - Харків, 2018. - С.6-7.

14. Нефедченко О.О. Модель інформаційної взаємодії в мережах IoT / О.О. Нефедченко // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення: збірник тез доповідей, 12 жовтн. 2021р. - Тернопіль: 2021. - випуск 62. - С.42 - 44.