Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення

Пояснювальна записка

до магістерської кваліфікаційної роботи
за освітньо-кваліфікаційним рівнем «магістр»
на тему:
МЕТОДИ ПОБУДОВИ БЕЗПРОВІДНИХ МЕРЕЖ СТАНДАРТУ 802.11 ДЛЯ КОНЦЕПЦІЇ "ІНТЕРНЕТ РЕЧЕЙ"
08-34.МКР.001.00.000 ПЗ

Виконав: студент 2-го курсу,
групи ТТК-18м
спеціальності 172 – Телекомунікації та радіотехніка

_____ Бондарев М. В.

Керівник: к.т.н., доцент каф. ТКСТБ

_____ Михалевський Д. В.

«____» _____ 2019 р.

Рецензент: к.т.н., доцент каф.

_____ Коваль К. О.

«____» _____ 2019 р.

Вінниця ВНТУ - 2019 рік

Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення
Освітньо-кваліфікаційний рівень магістр
Галузь знань 17– Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітня програма Технології та засоби телекомунікацій

ЗАТВЕРДЖУЮ
Завідувач кафедри ТКСТБ
к.т.н., проф Г.Г. Бортник

“___” _____2019 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Бондареву Миколі Валерійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Методи побудови безпровідних мереж стандарту 802.11 для концепції "інтернет речей"

керівник роботи Михалевський Дмитро Валерійович, к. т. н, доцент
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «02» 10 2019 року № 254
2. Строк подання студентом роботи 02 грудня 2019 року

3. Вихідні дані до роботи: частотнй діапазон 2,4 ГГц, Пропускна здатність 11 000 кбіт/сек,.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) вступ; техніко – економічне обґрунтування тематики; аналіз параметрів стандарту 802.11 wi–fi; оцінка параметрів безпровідного каналу; опис системи та розрахунок пропускної здатності; економічна частина; охорона праці та безпека в надзвичайних ситуаціях; висновки; література; додатки.

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)
1) Структура безпровідного каналу Wi–Fi 2) Архітектурна будова AWS IoT

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Технічна частина	Михалевський Д. В, доцент каф. ТКСТБ		
Економічна частина	Ратушняк О. Г. доцент каф. ЕПВМ		
Охорона праці та безпека в надзвичайних ситуаціях	Томчук М. А. доцент каф. МБЦО		

7. Дата видачі завдання __ вересня 2018 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка технічного завдання	06.09.2019р.	
2.	Техніко-економічне обґрунтування розробки	13.09.2019р.	
3.	аналіз параметрів стандарту 802.11 wi–fi	04.10.2019р.	
4.	Обчислення характеристик сигналів	25.10.2019р.	
5.	Оцінка параметрів безпровідного каналу; опис системи та розрахунок пропускної здатності	08.11.2019р.	
6.	Аналіз економічної ефективності розробки	15.11.2019р.	
7.	Аналіз безпеки життєдіяльності, цивільний захист	22.11.2019р.	
8.	Оформлення пояснювальної записки та графічної частини	29.11.2019р.	
9.	Нормоконтроль МКР	02.12.2019р.	
10.	Попередній захист МКР, рецензування МКР	06.12. 2019р.	
11.	Захист МКР ДЕК	18.12. 2019р.	

Студент _____ Бондарев М. В.
(підпис)

Керівник роботи _____ Михалевський Д. В.
(підпис)

РЕФЕРАТ

УДК 621.396

Бондарев Микола Валерійович. Методи побудови безпровідних мереж стандарту 802.11 для концепції "Інтернет Речей". Магістерська кваліфікаційна робота. – Вінниця: ВНТУ, 2019. – 120с.

На українській мові. Бібліогр.: 38 назв; Рис.:32; Табл.: 23.

Дана магістерська робота присвячена дослідженню мережі концепції «Інтернет Речей» на основі стандарту IEEE 802.11 Wi-Fi. Оцінено параметри пропускної здатності системи. Прораховано час обслуговування в різних мережах. Розраховано економічний ефект. Розглянуті питання безпеки життєдіяльності та охорони праці. Отримані результати задовольняють вимогам технічного завдання.

Ключові слова: пропускна здатність, мережа, Internet of Thinks.

ABSTRACT

UDC 621.396

Bondarev Mykola Valeriyovych. 802.11 Wireless Networking Methods for the Internet of Things Concept. Master's qualification work. - Vinnitsa: VNTU, 2019. - 120s.

In Ukrainian language. Bibliogr .: 38 titles; Fig. 32; Table: 23.

This master's thesis is devoted to the research of the Internet of Things concept network based on IEEE 802.11 Wi-Fi standard. The system throughput parameters were evaluated. The service time in different networks has been calculated. The economic effect is calculated. The issues of life safety and labor protection are considered. The results obtained satisfy the requirements of the terms of reference.

Keywords: bandwidth, network, Internet of Thinks

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AES (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування

ASIC (Application–specific integrated circuit) – інтегральна схема, спеціалізована для вирішення конкретного завдання

BPM (Business Process Management) – концепція процесного управління організацією, яка розглядає бізнес–процеси як особливі ресурси підприємства

COM (Component Object Model) – платформа компонентно–орієнтованого програмування

CPU (Central processing unit) – функціональна частина комп'ютера, що призначена для інтерпретації команд

GPS (Global Positioning System) – Систе́ма глоба́льного позиціонува́ння

EPC (Electronic Product Code) – електронний код продукту

HTML (HyperText Markup Language) – стандарт намова розмітки веб–сторінок в Інтернеті

IEEE Інституту інженерів з електротехніки та електроніки

IoT (Internet of Things) – інтернет речей

ISP (Internet Service Provider) – Інтернет–провайдер

JSON (JavaScript Object Notation) – об'єктнийзаписJavaScript

LAN (Local Area Network) – об'єднання певного числа комп'ютерів на відносно невеликій території

LTE (Long Term Evolution) – назва мобільного протоколу передачі даних

MIMO (multiple–input multiple–output) – декілька входів, декілька виходів

MSS (Maximum segment size) – максимальний розмір корисного блоку даних в байтах для TCP пакету

NFC (Near Field Communication) – технологія бездротового високочастотного зв’язку малого радіусу дії

OFDM, (Ortogonal Frequency Division Multiplexing) – мультиплексування з ортогональним частотним поділом

OTA (Over–the–air programming) – оновлення через повітря

PAN (Personal Area Network) – мережа, побудована «навкруг» людини

PBCC (Packet Binary Convolutional Coding) – бінарне згорткове кодування пакету

REST (Representational State Transfer) – підхід до архітектури мережевих

RFID (Radio frequency identification) – радіочастотна ідентифікація

QoS (Quality of service) – щость обслуговування

QR (quick response) – швидкий відгук

WPAN (Wireless Personal Network) – безпровідна персональна мережа передачі даних

IP – інтернет речей

ВСТУП

Майже вся наявна інформація, яку ми можемо найти в інтернеті була занесена та введена людьми безпосередньо, через клавіатуру, запис та копіювання даних. Але людина здатна помилятися, має обмежені час, увагу та точність. Це означає, що людина не завжди найкращий інструмент по збору даних чи їх введенню. Якщо ми матимемо пристрої, що самостійно вносять дані ззовні та без втручання людини, то це скоротить час на отримання інформації її втрат та витрат.

Актуальність теми. Магістерської роботи обумовлена тим, що технологія Інтернет речей значно полегшує зчитування даних та може вести контроль всіх аспектів нашого життя. Швидкий розвиток мобільних технологій допомагає прогресувати системі Інтернету речей. Число фізичних об'єктів, підключених до інтернету зростає, що реалізує ідею Інтернету речей. Застосування технології IP досить широке і вже застосовується в таких галузях як землеробство, будівництво, енергетика, транспорт та навіть в приватних будинках (система «розумний дім»).

Аналіз останніх досліджень. Кевін Ештон першим запропонував термін «Інтернет речей» у 1999 році працюючи над роботою Procter & Gamble, де описав систему, у щой фізичні об'єкти були пов'язані з мережею Інтернет. Цей термін Ештон ввів, щоб показати можливості радіочастотної ідентифікації (RFID), яка використовується в промислових системах поставок, щоб вести рахунок і відстежити товари без потреби людського втручання. Сьогодні, IP став популярним терміном при описі систем, у яких інтернет з'єднання і розрахункова здатність поширюються на багато об'єктів, приладів, датчиків і інших об'єктів з повсякденного життя.

Інтерне́т рече́й (англ. Internet of Things, IoT) – концепція мережі, що складається із взаємозв'язаних фізичних приладів, що мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін

даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. Окрім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів.

Інтеграція з Інтернетом має на увазі, що пристрої будуть використовувати IP–адресу як унікальний ідентифікатор. Проте, через обмежені адресні простори в IPv4 (що дозволяє використовувати 4,3 мільярда унікальних адрес), об'єктам IP доведеться використовувати IPv6, який забезпечує унікальними адресами мережевого рівня не менше 300 млн приладів на одного жителя Землі. Об'єктами в IP будуть не тільки пристрої із сенсорними можливостями, але також пристрої, що виконують дії (наприклад, лампочки або замки, якими керують через Інтернет). Значною мірою, майбутнє інтернету речей не буде можливим без підтримки IPv6, отже, глобальне впровадження IPv6 у найближчі роки буде мати вирішальне значення для успішного розвитку IP в майбутньому.

Для бездротової передачі даних особливо важливу роль в побудові інтернету речей відіграють такі характеристики, як ефективність, відмовостійкість, адаптивність, можливість самоорганізації. Основне зацікавлення в цьому сенсі представляє стандарт IEEE 802.15.4, що управляє доступом для організації енергоефективних персональних мереж, і є основою для таких протоколів, як Wi–Fi та Bluetoot.

Wi–Fi – це локальна безпровідна технологія, яка використовує 2,4 ГГц надвисокої частоти або 5 ГГц супер–високочастотної радіохвилі. Ця технологія дуже добре підходить для передавання великих обсягів даних по бездротовій мережі між пристроями, але це також вимагає багато енергії для роботи і має невеликий рівень пропускної здатності даних. При використанні цієї технології необхідно буде замінювати батареї у всіх пристроях на регулярній основі.

Bluetooth – це безпровідна технологія, яка використовується для передачі даних в персональних мережах. Вона передає дані по смузі частот від 2,4 до 2,485 ГГц і працює на коротших відстанях, ніж Wi–Fi. Ви можете синхронізувати пару приладів, таких як телефони, навушники, колонки, комп'ютери і багато іншого. З розвитком Bluetooth v4.0 з'явилася можливість реалізувати функцію низького енергоспоживання і збільшений радіус дії до декількох десятків метрів.

Вже зараз інтернету речей приділяється увага на вищому рівні, зокрема починаючи з 2009 року у Брюселі при підтримці Єврокомісії проходять конференції Annual Internet of Things, на який виступають з доповідями єврокомісари, науковці та керівники провідних IT–компаній[1]. За прогнозами аналітиків у найближчі роки очікується справжній бум інтернету речей. Так, за прогнозами Gartner, до 2020 року кількість підключених до всесвітньої мережі приладів становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпечення та послуг становитиме 1,9 трлн дол[2]. Дещо інші аналітичні агентства висловлюють ще більш оптимістичні прогнози. Найбільші світові IT компанії вже почали перегони за лідерство на цьому ринку. Так корпорація Intel у 2014 році після випуску «SoC Edison» оголосила конкурс «Make it Wearable» з призовим фондом $1,3 млн на найкраще застосування своєї системи для концепції IoT та створила власний підрозділ «Internet of Things Solutions Group» для розвитку цього напрямку[3][4]. Компанія «Google» на початку 2014 року за 3,2 млрд доларів купила невелику фірму «Nest Labs», яка займається випуском інтелектуальних термостатів[5]. Спеціалісти цієї компанії займались впровадженням на американському ринку технологій IoT. Виробники побутової техніки також працюють у цьому напрямку. Так на виставці CES 2014 у Лас–Вегасі була представлена велика кількість побутової техніки (холодильники, телевізори, пральні машини) з можливістю підключення до інтернет.

Лідерами у розробці та впровадженні інтернету речей є країни, в який розвинена індустрія виробництва мікропроцесорів та вбудованих комп'ютерів –

це Китай, Південна Корея, США. Також значний прогрес у цій галузі демонструють європейські країни та Японія.

Мета та постановка задачі. Метою даної кваліфікаційної роботи є дослідження технології Інтернету речей та методів побудови даних мереж на основі стандарту IEEE 802.11.

Задачами магістерської кваліфікаційної роботи є:

– дослідити технологію Інтернет речей;

– провести аналіз основних характеристик стандарту IEEE 802.11;

– провести аналіз основних характеристик стандарту Bluetooth

– провести аналіз побудови мережі;

– розрахувати основні параметри мережі;

Об'єктом дослідження є методи побудови безпровідних мереж стандарту 802.11 для концепції «Інтернет речей».

Предмет дослідження є пропускна здатність каналів у безпровідних мережах стандарту 802.11

Методи досліджень базуються на використанні теоретичних (методи лінійної алгебри, методи математичного інтегрального аналізу і математичне моделювання) і емпіричних методів (імітаційне моделювання, експериментальне дослідження). Здатність отриманих результатів перевірена за експериментальними даними.

Наукова новизна одержаних результатів. У процесі досліджень та розробок отримано такі нові наукові результати:

1. Виконано дослідження сучасних стандартів безпровідних стандартів Wi–Fi та Bluetooth.

2. Розуміння основних концепцій технології інтернет речей

3. Побудова мережі на основі стандарту 802.11.

4. Аналіз пропускної здатності системи

Практичне значення. Практичне значення роботи полягає в покращенню алгоритмів для проектування безпровідних мереж стандарту 802.11 концепції «Інтернет Речей»

Крім того, результати роботи можна використовувати в навчальному процесі в дисциплінах інфокомунікаційні технології та системи зв'язку; цифрова обробка сигналів в телекомунікаціях;моделювання пристроїв та систем зв'язку; імітаційне моделювання радіотехнічних пристроїв

1 АНАЛІЗ ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ ТА СТАНДАРТУ IEEE 802.11

1.1 Аналіз технології «Інтернет речей»

Зростаючий попит на швидке отримання інформації та контроль повсякденного життя та контроль на виробництві призвело до необхідності підключення нових приладів, що могли б зчитувати та вводити дані з навколишнього середовища. Це і призвело до створення технології «Інтернет речей».

Основною концепцією IP є можливість підключення всіляких об’єктів (речей), що людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль, велосипед і навіть кросівки. Всі ці об’єкти (речі) повинні бути оснащені вбудованими давачами або сенсорами, що мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії в залежності від отриманої інформації. Прикладом впровадження такої концепції є система «розумний будинок» або «розумна ферма». Ця система аналізує дані навколишнього середовища і в залежності від показників регулює температуру в приміщенні. У зимовий період регулюються інтенсивність опалення, а в випадку спекотної погоди будинок має механізми відкривання і закривання вікон, завдяки чому провітрюється будинок, і все це відбувається без втручання людини.

Для об’єднання повсякденних речей у мережу потрібні декілька технологій.

- Для ідентифікації кожного об’єкту потрібна проста, компактна технологія. Тільки при наявності системи унікальної ідентифікації можна збирати та накопичувати інформацію про певний предмет. Такий функціонал

можна забезпечити за допомогою мікросхем RFID (Radio Frequency IDentification). Вони здатні без власного джерела струму передавати інформацію приладам зчитування. Кожна мікросхема має індивідуальний номер. Як альтернатива до даної технології для ідентифікації об’єктів можуть використовуватись QR–коди. Для визначення точного місця знаходження речі підійде технологія GPS, яка ефективно використовуються вже сьогодні у смартфонах та навігаторах.

- Для відслідковування змін у стані елементу чи оточуючого середовища об’єкти повинні оснащуватися сенсорами.
- Для обробки та накопичення даних з сенсорів повинен використовуватися вбудований комп’ютер (наприклад Raspberry Pi, Intel Edison).
- Для обміну інформацією між пристроями можуть бути використані технології бездротових мереж– найпоширеніші типи підключення.

Для постійного оновлення даних, їх зчитування може бути неперервним, і зчитуватися у визначений час циклічно, проходячи усі пристрої мережі. На рис. 1.1 показано принцип опитування приладів мережі циклічного підключення.

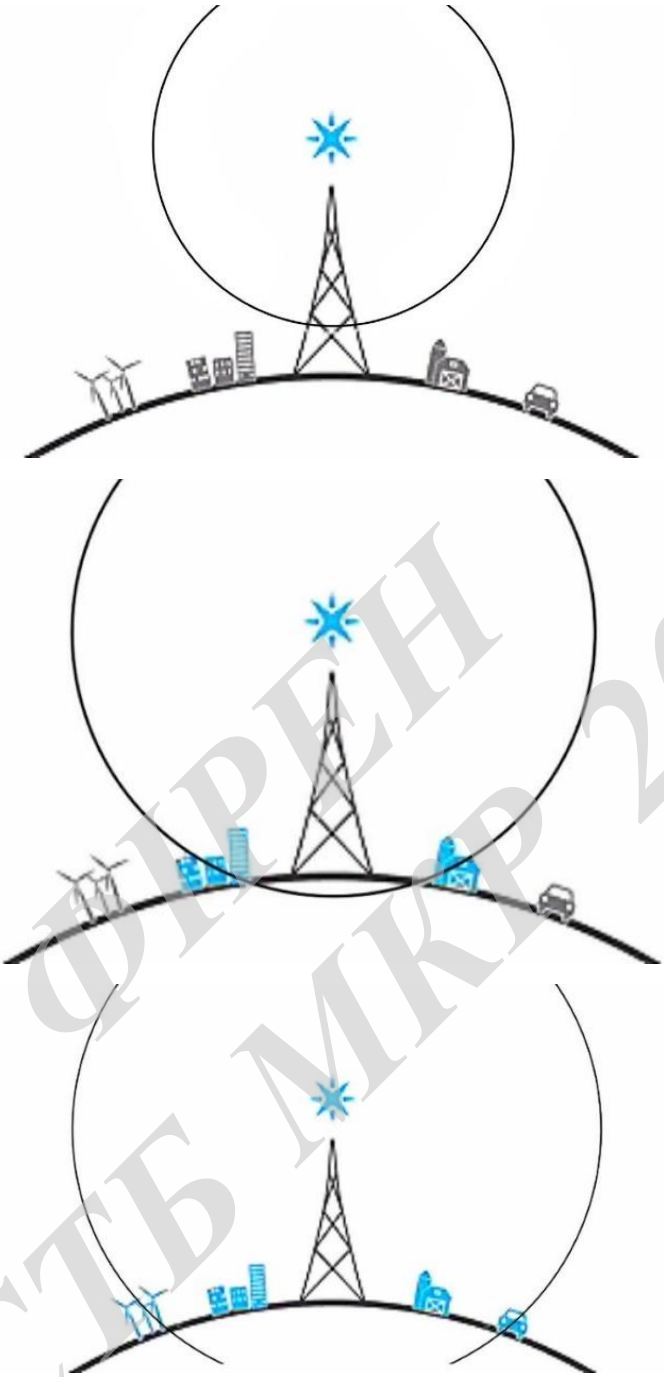


Рисунок 1.1 – Процес підключення приладів IP (нескінченний цикл)

1.1.1 Опис IP з точки зору інфокомунікацій

Мережева топологія системи IP базується на простих вузлах, що збирають і перенадають обмежену кількість інформації до центрального контролера або шлюзу, який забезпечує підключення до інтернету. Вузли та шлюзи розроблені таким чином, щоб звести на мінімум споживання енергії, забезпечити надійні мережеві з'єднання і розширити діапазон бездротового підключення до мережі, наскільки це можливо. В основі системи IP знаходиться процесор або мікроконтролер, який обробляє дані і запускає програмні стеки, що підключаються до пристрою бездротового зв'язку. Розширений IP сенсорні вузли виконують функції датчиків і використовуються як 8–розрядний мікроконтролер або 32–бітовий пристрій, для запуску стек–протоколів невеликих радіочастот. Ці пристрої, як правило, із власним живленням і підключаються до шлюзів, де відбувається масивна обробка і передача даних. Датчики вузлів, як правило перенадають невеликі обсяги даних і працюють автономно роками. Ці пристрої також повинні бути портативними, надійно з'єднані і здатні працювати в різних умовах навколишнього середовища, незалежно від радіочастотних перешкод або фізичних бар'єрів.

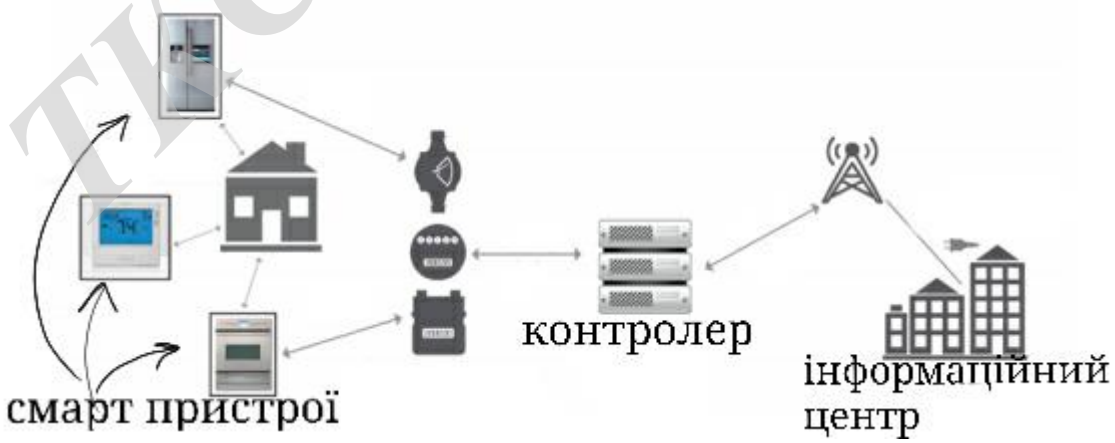


Рисунок 1.1.1 – Схема підключення пристроїм IP

1.2 Аналіз стандартів Wi–Fi та Bluetooth і обгрунтування вибору безпровідного зв'язку

1.2.1 Аналіз стандартів IEEE 802.11

Стандарт IEEE 802.11 є базовим стандартом для побудови бездротових локальних мереж (Wireless Local Network – WLAN) [1]. Стандарт IEEE 802.11 постійно вдосконалювався, і в даний час існує ціле сімейство, до якого відносять специфікації IEEE 802.11 з літерними індексами a, b, c, d, e, g, h, i, j, k, l, m, n, o , p, q, r, s, u, v, w. Однак тільки чотири з них (a, b, g і i) є основними і користуються найбільшою популярністю у виробників обладнання, інші ж (з–f, h–n) є доповнення, удосконалення або виправлення прийнятих специфікацій. У свою чергу, Інститут інженерів з електроніки та електротехніки (IEEE) тільки розробляє і приймає специфікації, на перераховані вище стандарти. В його обов'язки не входять роботи з тестування обладнання різних виробників на сумісність. Для просування на ринку обладнання для бездротових локальних мереж (WLAN) була створена група, яка отримала назву Альянс Wi–Fi. Цей альянс здійснює керівництво роботами по сертифікації обладнання різних виробників і видачі дозволу на використання членами Альянсу Wi–Fi логотипу торгової марки Wi–Fi. Наявність на обладнанні логотипу Wi–Fi гарантує надійну роботу і сумісність обладнання при побудові бездротової локальної мережі (WLAN) на обладнанні різних виробників. В даний час Wi–Fi–сумісним є обладнання, побудоване за стандартом IEEE 802.11a, b і g (може також використовувати стандарт IEEE 802.11i для забезпечення захищеного з'єднання). Крім того, наявність на обладнанні логотипу Wi–Fi означає, що робота обладнання здійснюється в діапазоні 2,4 ГГц або 5 ГГц. Отже, під Wi–Fi слід розуміти сумісність обладнання різних виробників, призначеного для

побудови бездротових локальних мереж.

Перелік основних стандартів:

IEEE 802.11 – початковий стандарт бездротових локальних мереж, заснований на бездротовій передачі даних у діапазоні 2.4 ГГц. Підтримує обмін даними зі швидкістю до 1 – 2 Мбіт/с. Прийнятий у 1997 році стандарт передбачав два типи модуляції – DSSS і FHSS.

IEEE 802.11a – стандарт бездротових локальних мереж, заснований на бездротовій передачі даних в діапазоні 5 ГГц. Діапазон роздільний на три непересічні піддіапазони. Максимальна швидкість обміну даними становить 54 Мбіт/с, при цьому доступні також швидкості 48, 36, 24, 18, 12, 9 і 6 Мбіт/с.

IEEE 802.11b – стандарт бездротових локальних мереж, заснований на бездротовій передачі даних в діапазоні 2,4 ГГц. У всьому діапазоні існує три непересічні канали, тобто на одній території, не впливаючи один на одного, можуть працювати три різні бездротові мережі. У даному стандарті застосований метод модуляції DSSS. Максимальна швидкість роботи становить 11 Мбіт/с, при цьому доступні також швидкості 5.5, 2 та 1 Мбіт/с.

Стандарт IEEE 802.11b був прийнятий в 1999 році в розвиток прийнятого раніше стандарту IEEE 802.11. Він також передбачає використання діапазону частот 2.4 ГГц, але тільки з модуляцією DSSS. Продукти стандарту IEEE 802.11b, що поставляються різними виробниками, тестуються на сумісність і сертифікуються організацією Wireless Ethernet Compatibility Alliance (WECA), яка більше відома під назвою Wi–Fi Alliance. Сумісні бездротові продукти, що пройшли випробування за програмою «Альянсу Wi–Fi» можуть бути маркіровані знаком Wi–Fi.

IEEE 802.11g – стандарт бездротових локальних мереж, заснований на бездротовій передачі даних в діапазоні 2.4 ГГц. Діапазон розділений на три непересічні канали, тобто на одній території, не впливаючи одна на одну, можуть працювати три різні бездротові мережі. Для збільшення швидкості

обміну даними при ширині каналу, схожій з 802.11b, застосований метод модуляції з ортогональним частотним мультиплексуванням (OFDM, Ortogonal Frequency Division Multiplexing), а також метод двійкового пакетного згорткового кодування PBCC (Packet Binary Convolutional Coding).

IEEE 802.11e (QoS, Quality of service) – додатковий стандарт, що дозволяє забезпечити гарантовану щость обміну даними шляхом перестановки пріоритетів різних пакетів; необхідний для роботи таких потокових сервісів як VoIP або IPTV.

IEEE 802.11i – стандарт, що знімає недоліки у сфері безпеки попередніх стандартів. 802.11i вирішує проблеми захисту даних канального рівня і дозволяє створювати безпечні бездротові мережі практично будь–якого масштабу.

IEEE 802.11n – сучасний стандарт бездротових локальних мереж покоління, заснований на бездротовій передачі даних в діапазоні 2.4 ГГц. Стандарт 802.11n значно перевищує за швидкістю обміну даними попередні стандарти 802.11b і 802.11g, забезпечуючи швидкість на рівні Fast Ethernet; зворотно сумісний з 802.11b і 802.11g. Основна відмінність від попередніх версій Wi–Fi – додавання до фізичного рівня (PHY) підтримки протоколу MIMO (multiple–input multiple–output). Теоретична швидкість може складати 150 Мбіт/с

IEEE 802.11ac – новий стандарт бездротових локальних мереж Wi–Fi на частотах 5–6 ГГц. Якщо обидва пристрої підтримують цю технологію, то швидкість обміну даними може бути більшою за 1 Гбіт/с (до 6 Гбіт/с 8x MU–MIMO). Стандарт передбачає використання до 8 антен MU–MIMO та розширення каналу до 80 або 160 МГц. 20 січня 2011 прийнята перша редакція версії 0.1, а вже 1 лютого 2013 редакція версії 5.0.

Таблиця 1.2 – Технічні характеристики стандартів IEEE 802.11a, b, g.

Стандарт	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
частотний діапазон	2,4–2,483 ГГц	5,15–5,25 ГГц 5,67–5,85 ГГц	2,4–2,483 ГГц
матод доступу	CSMA-CA	CSMA-CA	CSMA-CA
метод модуляції	BPSK, CCK	OFDM	OFDM
швидкість передачі	11 Мбіт/с	54 Мбіт/с	54 Мбіт/с
кількість абонентів на канал	64	64	64
дальність сигналу	20–100 м	10–20 м	20–50 м

1.2.2 Аналіз безпровідної технології передачі даних BlueTooth

BlueTooth Технологія (стандарт IEEE 802.15) стала першою технологією, що дозволяє організувати бездротову персональну мережу передачі даних (WPAN – Wireless Personal Network). Вона дозволяє здійснювати передачу даних і голосу по радіоканалу на невеликі відстані (10–100 м) в неліцензованому діапазоні частот 2,4 ГГц і з'єднувати ПК, мобільні телефони та інші пристрої при відсутності прямої видимості. Своєму народженню BlueTooth зобов'язана фірмі Ericsson, яка в 1994 році почала розробку нової технології зв'язку. Спочатку основною метою була розробка радіоінтерфейсу з низьким рівнем енергоспоживання і невисокою вартістю, який дозволяв би встановлювати зв'язок між стільниковими телефонами і бездротовими гарнітурами. Однак згодом роботи з розробки радіоінтерфейсу плавно переросли в створення нової технології.

На телекомунікаційному ринку, а також на ринку комп'ютерних засобів успіх нової технології забезпечують провідні фірми–виробники, що приймають рішення про доцільність і економічну вигоду від інтеграції нової технології в свої нові розробки. Тому в 1998 році фірма Ericsson організувала консорціум BlueTooth SIG (Spesial Interest Group), перед яким ставилися наступні завдання:

- подальша розробка технології BlueTooth

- просування нової технології на ринку телекомунікаційних засобів

До консорціуму BlueTooth SIG [5] входять такі фірми, як Ericsson, Nokia, 3COM, Intel, National Semiconductor. Консорціумом BlueTooth SIG, були розроблені стандартизації нової технології з метою сумісності BlueTooth–приладів, розроблених різними фірмами. Також були розроблені специфікації характеристики протоколів передачі даних. В результаті був розроблений пакет протоколів бездротової передачі даних BlueTooth (рис.1.2.1).

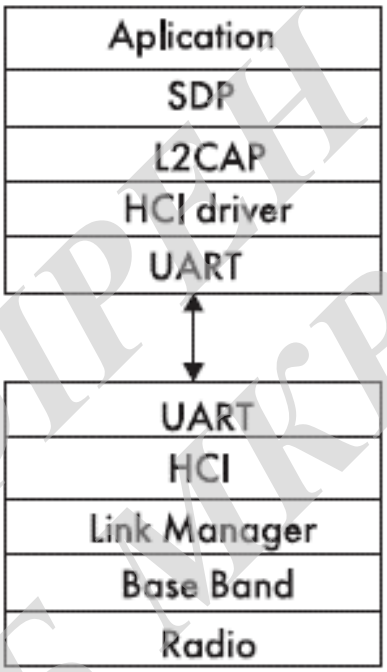


Рисунок 1.2.1 – Стек протоколу BlueTooth

Технологія BlueTooth підтримує як з'єднання типу «точка–точка», так і «точка–багатоточка». Коли два або більше приладів використовують один і той же канал – утворюється пікомережа. Один з приладів працює як основний (master), а решта – як підлеглі (slave). В одній пікомережі може бути до семи активних підлеглих приладів, при цьому інші підлеглі пристрої знаходяться в стані «паркування», залишаючись синхронізованими з основним пристроєм. Взаємодіючі пікомережі утворюють «розподілену мережу». У кожній

пікомережі діє тільки один основний пристрій, крім того, основний пристрій однієї пікомережі може бути підлеглим в інший (рис. 1.2.2).

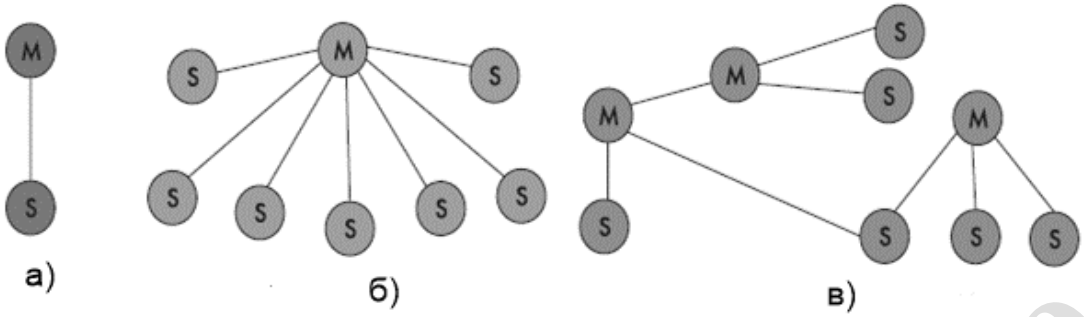


Рисунок 1.2.2 – Пікомережі: а) мережа з одним підлеглим, б) мережа з кількома підлеглими, в) розподілена мережа

В даний час на ринку працює велика кількість фірм, що пропонують модулі BlueTooth, а також компоненти для самостійної реалізації апаратної частини BlueTooth–пристрої. Практично всі виробники пропонують модулі, що підтримують специфікації BlueTooth версії 1.1 і 1.2 і відповінадають класу 2 (діапазон дії 10 м) і класу 1 (діапазон дії 100 м). Найвживанішою версією даної технології є BlueTooth 2.0 (одна з останніх модифікацій), що забезпечує радіус дії 10 м при перешкодах та 30 м при прямій видимості, натомість дозволяє здійснювати передачу даних на швидкості до 3 Мбіт/с.

1.2.3 Обґрунтування вибору безпровідної мережі

Для того щоб визначити доцільність використання безпровідного стандарту складемо порівняльну характеристику обох типів мережі у вигляді таблиці. Як видно з таблиці 1.4, наведеної нижче, доцільніше використовувати безпровідний стандарт – Wi–Fi

Таблиця 1.4 – Порівняльна характеристика стандартів Wi–Fi та Bluetooth

Технологія зв’язку	Wi–Fi	Bluetooth
Частотний діапазон	2,4 ГГц	2,4 ГГц
Пропускна здатність	11 000 кбіт/с	723,1 кбіт/с
Розмір стека протоколу	понад 1000	понад 250
Кількість вузлів в мережі	10	7
Радіус дії	20–300 м	10–100 м

1.3 Цілі Дослідження

Цілі цього дослідження включають в себе методи побудови безпровідних мереж стандарту 802.11 для концепції «Інтернет речей». .

- Розуміння основних концепцій технології інтернет речей
- Побудова мережі на основі стандарту 802.11.
- Аналіз пропускної здатності системи.

1.4 Висновки до розділу

В ході проведеного дослідження було визначено звідки походить концепція технології «Інтернет речей», для чого застосовується. Було встановлено, що дана концепція базується на основі безпровідних мереж і використання стандартів Wi–Fi та Bluetooth. Також в ході аналізу були поставлені цілі подальшого дослідження.

2 АНАЛІЗ ПАРАМЕТРІВ СТАНДАРТУ 802.11 WI–FI

2.1 Аналіз останніх досліджень та постановка проблеми

Аналізуючи існуючих наукові роботи можна сказати, що на сьогодні дослідження в галузі безпровідних технологій стандарту 802.11 [1] набувають все більшого поширення. Із них можна виділити нижче наведені.

У роботі [2] було наведено основні характеристики безпровідних систем та зображено загальний вираз для потужності приймального сигналу. Поряд із дослідженнями стандартів 802.11 проводяться дослідження стандарту 802.16 [3]. Вони подібні між собою, а також для них характерна наявність однакових типів завад у середовищі передачі. У цій роботі [4] було оцінено причини та наведено методи боротьби з міжканальними інтерференційними завадами для багатопозиційних сигналів. Внаслідок чого було встановлено, що при використанні великої кількості підносійних, збільшується швидкість передачі в каналі, а також збільшуються вимоги до параметра сигнал / шум. Тип модуляції – це той вагомий фактор, який необхібно враховувати.

У стандарті 802.11 використовуються два види модуляції MPSK для низькошвидкісної передачі та QPSK для високошвидкісної передачі. Як показують дослідження [5, 6] одним із критеріїв ефективності передачі інформації є забезпечення відповідного рівня сигнал / шум.

Як відомо, основним параметром, який характеризує будь–який канал передачі є пропускна здатність [7]. Саме забезпечення цього параметра у певних межах та шляхи підвищення його, говорять про ефективність роботи каналу. З іншого боку розглядаючи безпровідні канали стандарту 802.11 Wi–Fi, можна спостерігати невеликий виділений частотний/ ресурс на якому розміщується велика кількість мереж, що використовують однакові канали для

передачі інформації [8]. Особливо це стосується сфер із високою складністю забудови та густиною населення (кількість мереж може досягати понад 50). У такому випадку, при співпадінні частотних каналів, інформаційні пакети кожної мережі займають часові проміжки між пакетами іншої мережі. Усі ці фактори призводять до виникнення завад та зменшення параметра корисної пропускної здатності. Тому при розробці ефективних методів для оцінки параметрів безпровідних Wi–Fi мереж необхідно насамперед розв'язати задачу побудови каналу, що враховує усі фактори, що впливають на величину пропускної здатності під час передачі корисної інформації.

2.2 Побудова безпровідного каналу

Характеристику передачі сигналу для будь–якого безпровідного загалом можна показати так [9]:

$$S(t) = a(t)A(t) + n(t)\,, \qquad (2.1)$$

де S(t) – передавальний сигнал; A(t) – приймальний сигнал; a(t) – коефіцієнт, який враховує послаблення та завмирання передавального сигналу; n(t) – коефіцієнт, який враховує наявність інших джерел випромінювання у каналі. Коефіцієнти a(t) і n(t) є завадами що діють у каналі та мають випадковий характер і впливають на щость передачі інформації.

З погляду побудови безпровідних Wi–Fi мереж, канали передачі для аналізу можна подати як точки доступу та абонентські адаптери інтерфейси. Кожен такий пристрій містить і передавач, і приймач, що виконують обмін радіосигналами через середовище передачі, а також виконують роль перетворювачів інформації від мережних інтерфейсів у радіосигнали та навпаки.

Стандарт 802.11 насамперед описує канальний та фізичний рівні моделі OSI [10], тому найпростіше враховувати [9], побудову безпровідного каналу передачі, можна запропонувати як пару передавач та приймач, що показано на рис. 1.

На канальному рівні (підрівні LLC та MAC) та підрівні PLCP виконується завадостійке кодування, так званим канальним кодером (КК). Тут виконується формування кадру PPDU, який вміщує у собі службову та корисну інформацію для передачі. Підрівень PMD канального рівня, перетворює двійкову послідовність у модульоване ВЧ коливання за допомогою квадратурного модулятора (М) та блока розширення спектру (БРС). Для стандартів 802.11n та вище використовується OFDM, а для нижчих – DSSS. На виході передавальної антени (Апд) формується сигнал S(t) та надходить у середовище передачі. Потужність сигналу передавача є наперед визначеною величиною та складає для стандарту Wi–Fi 100 мВт. При таких значення внутрішні шуми електричних кіл передавача є незначними і ними можна нехтувати. Основні завади, що приводять до зміни та затухання сигналу діють у середовищі передачі.

Перший тип завад описуються у формулі (2.4) як часова залежність a(t). Цей вид завад характеризується зміною параметрів середовища під час передачі під впливом природніх явищ. Сюди входить ефект багатопроменевого розповсюдження хвиль, що виникає під час руху абонента у будівлях із складною забудовою. Внаслідок чого у середовищі можуть виникати загальновідомі максимуми та мінімуми напруженості електричного поля.

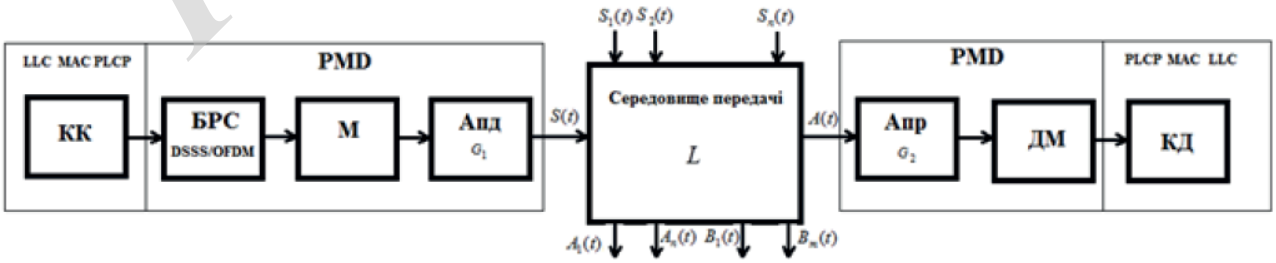


Рисунок 2.3 – Структура безпровідного каналу Wi–Fi

Другий тип завад n(t) описує завади що є самостійними джерелами випромінювання. На рис. 1 завади, що мають природний характер, та завади від приладів інших систем передачі та побутових приладів, позначені як 1 n B (t)...B (t). Їх загалом прийнято вважати шумами. Завади 1 n A (t)...A (t) , що вносять інші передавачі стандарту Wi–Fi 1 n S (t)…S (t) – вважаються інтерференційними завадами.

Приймальна частина виділяє корисний сигнал із середовища передачі A(t), який є подібним до початкового сигналу S(t). Цей сигнал надходить до приймальної антени ($A_{пр}$) і потім виконуються зворотні функції перетворення стосовно передавальної частини блоком демодулятора (ДМ). У такий спосіб на підрівні PLCP канального декодера (КК) отримується кадр PPDU.

2.3 Оцінка параметрів безпровідного каналу

Основним параметром що впливає на швидкість передачі кадрів PPDU, а також на наявність у них помилок є рівень потужності прийнятого сигналу на вході приймача RX P. Ця потужність залежить від потужності випромінювання передавача TX P та параметрів середовища передачі. Тому тут можна застосувати рівняння взаємозв’язку цих потужностей, що розташовані на відстані один від одного, так зване рівняння бюджету каналу:

$$P_{RX} = P_{TX} + G_1 + G_2 - L_{RX} - L_{TX} - L \ (\text{дб}),$$

де L_{RX} L_{TX} – затухання в антенно–фідерних пристроях приймача та передавача; G_1 , G_2 – коефіцієнти підсилення антен передавача та приймача, L – втрати потужності сигналу в середовищі передачі.

Втрати потужності сигналу в середовищі передачі можна визначити за такою формулою:

$$L = \frac{(4\pi d)^2}{\lambda^2 G_1 G_2 \eta_1 \eta_2},$$

де η_1 ,η_2 – коефіцієнти корисної дії фідерів передавача та приймача; λ – довжина хвилі, d – відстань між антенами.

Враховуючи дослідження моделі Хата у [11] для стандарту 802.11 втрати потужності в умовах складних забудов записуються так:

$$L = -27{,}6 + 20\log(1000d) + 20\log(f) + \\ + \text{fix}\left(\frac{1000d}{d_к}\right)L_п + k_f^{\left(\frac{k_f+2}{k_f+1}-b\right)}L \text{ (дб)},$$

$$k_f = \text{fix}\left(\frac{|h_2 - h_1|}{h_п}\right),$$

де $d_к$ – довжина кімнати; $L_с$ – втрати завдяки внутрішнім стінам; $L_п$ – втрати завдяки підлозі; b – емпіричний коефіцієнт; $h_п$ – висота підлоги; h_2 і h_1 – висоти антен приймача та передавача; f – частота сигналу.

Враховуючи мобільність абонентів можна отримати залежність частоти сигналу від швидкості руху, так званий ефект Доплера. В мережах Wi–Fi зазвичай з'єднання може бути між двома абонентами безпосередньо, із використанням точки доступу, а також у мережі із багатьма точками доступу та ретрансляторами. У таких ситуаціях абоненти можуть бути стаціонарними та рухомими, і під час руху швидкість передачі може зменшуватись. Отже, залежність частоти сигналу від швидкості абонента записується так:

$$f_{\upsilon} = f\left(\frac{1+\frac{\upsilon_{пр}}{c}}{1-\frac{\upsilon_{пд}}{c}}\right),$$

де $\upsilon_{пр}$ – швидкість передавача сигналу; $\upsilon_{пр}$ – швидкість приймача сигналу; с – швидкість світла.

Також одним із основних параметрів, що впливають на пропускну здатність безпровідного каналу передачі є рівень чутливості приймача. Вона визначає мінімально допустимий рівень сигналу завдяки якому приймач може декодувати інформацію із заданою точністю або заданим рівнем сигнал / шум. У цифрових системах передачі сигнал / шум – відношення енергії сигналу Е на 1 біт інформації до густини потужності шумів ш Р [12]. Тоді, враховуючи побудову каналу на рис. 1 та формулу (2.3), відношення сигнал / шум можна записати так:

$$E / N = \frac{P_{RX}}{(P_{ш} + P_{i})R}, \tag{2.2}$$

де R – швидкість передачі інформації; P_i – потужність інтерференційних завад.

Величина $P_ш$ містить у собі внутрішні шуми приймального тракту і зовнішні шуми, що надходять із каналу передачі на приймальну антену. До шумів у каналі належать шуми, джерелами яких є інші випромінювання на таких самих частотних каналах (побутові пристрої, безпровідні телефони, керуючі пристрої та системи контролю параметрів та інші), а також випромінювання навколишнього середовища (наприклад: температурний атмосферний шум, промисловий шум, космічний шум та інші).

Враховуючи [12], рівень шумів можна визначити за таким виразом:

$$P_{ш} = kT\left[\left(\frac{k_{ш}}{k_{ф}} - 1\right) + \left(\frac{1}{P_0}\sum_{i=1}^{m} P_i - 1\right)\right], \tag{2.3}$$

де k – стала Больцмана; T – температура роботи приймача; $k_{ш}$ – коефіцієнт шуму приймального тракту; $k_{ф}$ – коефіцієнт передачі потужності фідера; P_i – потужність шумів завад $B_m(t)$ середовища передачі; m – кількість завад у середовищі передачі; і P – рівень теплового шуму Землі.

Інтерференція у безпровідних каналах передачі стандарту 802.11 – це сигнали від інших передавачів цього ж стандарту, що використовують однаковий частотний канал або частково перекривають його. При наявності великої кількості безпровідних мереж основним джерелом шуму є інтерференція. На практиці вплив інтерференції виникає при збільшенні навантаження на мережі при передачі великих об'ємів інформації, що використовують такий же частотний канал.

Враховуючи те, що інтерференційних джерел може бути $S_1(t)...S_n(t)$, то загальну потужність цих завад визначимо за таким виразом:

$$P_{iн} = \frac{G_2}{L_{RX}}\sum_{i=1}^{n}\frac{P_{c.c.i}G_{c.c.i}}{G_{ф.i}L_{i.i}L_3}, \tag{2.4}$$

де і L – послаблення в інтерференційному каналі; з L – затухання в антенно–фідерному пристрої інтерференційного передавача; Gφ – послаблення при мінімальній кутовій відстані між антенами, $G_{c.c}$ – коефіцієнт підсилення антени суміжної інтерференційної станції, $P_{c.c}$ – потужність сигналу суміжної станції; n – кількість інтерференційних станцій у межах зони покриття базової станції.

Отже, враховуючи формули (2.2) – (2.4), потужність на вході приймача прийме вигляд:

$$P_{RX} = (E/N)\left(kT\left(\frac{k_{ш}}{k_{ф}} + \frac{1}{P_0}\sum_{i=1}^{n} P_i - 2\right) + \frac{G_2}{L_{RX}}\sum_{i=1}^{m}\frac{P_{c.c.i}G_{c.c.i}}{G_{ф.i}L_{i.i}L_3}\right)R\,.$$

Вишевказаний вираз показує, яку необхідно забезпечити потужність сигналу на вході приймача для забезпечення необхідної швидкості передачі.

Ще однією особливістю стандарту 802.11 є те, що для досягнення високої пропускної здатності використовується багаторівнева квадратурна модуляція. Цей тип модуляції має високу чутливість до параметрів каналу передачі. Використання високих порядків модуляції насамперед потребує жорстких вимог до параметра E / N приймача. Тому у такому випадку можна застосовувати відносний коефіцієнт чутливості:

$$P_в = P_т + k_ш + E/N + K_р \text{ (дб)},$$

де $K_р$ – коефіцієнт запасу виникнення явищ неідеальної побудови приймача.

Одним із методів зменшення залежності швидкості передачі від E / N використовують на практиці технологію прямої корекції помилок (FEC). За такої умови це потребує введення додаткової службової інформації, що з одного боку призтоваруть до зменшення передачі корисної інформації, а з другого – розширення спектру передачі частотного каналу.

2.4 Висновки до розділу

Отже, у цій роботі визначено параметри та проведено аналіз тракту передачі інформації для пари приймач–передавач стандарту 802.11 Wi–Fi, що мають вплив на характеристику пропускної здатності. На основі цього було отримано такі результати:

а) встановлено що у безпровідному каналі основними факторами, що впливають на характеристику передачі є послаблення сигналу у середовищі передачі та наявність інтерференційних завад;

б) запропоновано розширену структуру безпровідного каналу стандарту 802.11, яка враховує шумові та інтерференційні завади, що призводять до зміни та затухання сигналу у тракті передачі.

в) отримано вираз для оцінки потужності сигналу на вході приймача, який дає змогу протоварути оцінку необхідної швидкості передачі, що є базою для розробки ефективних методів оцінки та контролю безпровідних мереж стандарту 802.11 Wi–Fi.

3 РОЗРАХУНОК ПРОДУКТИВНОСТІ МЕРЕЖІ

3.1 Технологія AWS IoT

AWS IoT створює безпечне двостороннє спілкування між пристроями, підключеними до мережі Internet, такими як датчики, виконавчі пристрої, вбудовані мікроконтролери або інтелектуальні пристрої та Cloud AWS. Це дає змогу збирати телеметричні дані з багатьох приладів, а також зберігати та обробляти дані.

AWS IoT складається з таких компонентів:

- Шлюз пристрою. Дає змогу пристроям безпечно та ефективно з’єднуватися з AWS IoT.
- Брокер повідомлень. Створює безпечний механізм для приладів та програм IWT AWS для оприлюднення та отримання повідомлень одне від одного. Для публікації та підписки може підтримуватись протокол MQTT або MQTT через WebSocket, чи інтерфейс HTTP REST.
- Двигун правил. Здійснює обробку повідомлень та спілкування з іншими службами AWS. Може траплятися мова на базі SQL, щоб вибрати дані з корисних інформаційних повідомлень, а потім обробляти та передавати дані інакшим службам, таким як Amazon S3, Amazon DynamoDB та AWS Lambda. Також може підтримуватись брокер повідомлень, щоб повторно висвітлити повідомлення іншим абонентам.
- Служба безпеки та ідентифікації. Створює спільну відповідальність за безпеку. Пристрої мусять зберігати свої облікові дані у безпеці, щоб вдправляти їх до брокера повідомлень. Брокер повідомлень та двигун правил здійснюють функції безпеки AWS для надійного надсилання даних на пристрої або інакші служби AWS.

- Реєстр. Організовує ресурси, пов’язані з усіма пристроями у хмарі. При реєстрації пристрою здійснюється прив’язка до трьох спеціальних атрибутів кожного з них. Є доступ розробити прив’язку сертифікатів та клієнтських ідентифікаторів, аби покращити здатність виявляти та усувати неполадки.

- Реєстр групи. Дає змогу керувати кількома пристроями одночасно, розподіливши їх на групи. Групи також мають містити підгрупи, що здійснює певну ієрархію. Будь–що дії, що створюються на батьківській групі, використовуватимуться до її дочірніх груп, а також до усіх приладів у ньому та в усіх його дочірніх групах. Дозволи, надані групі, будуть здійснюватись до усіх приладів та в усіх його дочірніх групах.

- Цифровий двійник. Документ JSON, що використовується для зберігання та отримання дійсної інформації про стан щодо пристрою. Забезпечує сталі уявлення про пристрої у хмарі. Оновлені дані про стан пристрою можна оприлюднити у службі, а пристрій співзіставить цей стан при підключенні. Пристрої також мусять опублікувати свій поточний стан у тінь для застосування додатками або іншими пристроями.

- Служба автентифікації за замовчуванням. Ви маєте визначити власні авторизатори, що надають змогу керувати вашою власною стратегією автентифікації та авторизації завдяки спеціальній службі автентифікації та функції лямбда. Користувальницькі авторизатори надають змогу AWS IoT перевіряти автентичність приладів та давати дозвіл на операції завдяки автентифікації та стратегій авторизації токенів носіїв. Користувальницькі авторизатори мають реалізовувати різні стратегії автентифікації (наприклад, перевірка JWT, виклик провайдера OAuth тощо) і відновлювати документи політики, що застосовуються шлюзом пристрою для авторизації операцій MQTT.

- Jobs service. Дає змогу визначити набір віддалених операцій, що надсилаються і виконуються на одному або кількох пристроях, підключених до AWS IoT. Наприклад, ви можете ідентифікувати роботу, яка наказує пристроям

завантажити та встановити оновлення програм, перезавантаження, обертання сертифікатів або виконання віддалених способів усунення несправностей. Для здійснення цих операцій необхідно вказати опис віддалених дій, що необхідно виконати, і список цілей, що мають виконувати їх. Цілі можуть бути різними пристроями або групами [18].

3.1.1 Принцип роботи AWS IoT

AWS IoT дає змогу підключеним до мережі Internet пристроям підключитися до Cloud AWS і дає змогу додаткам у хмарі взаємодіяти з пристроями, підключеними до мережі Internet. Звичайні додатки IoT збирають та обробляють телеметрію з приладів або здійснюють доступ користувачам дистанційно керувати пристроєм.

Пристрої сповіщають про стан, публікуючи повідомлення у форматі JSON на теми MQTT. Інша тема MQTT має ієрархічне ім’я, яке ідентифікує пристрій, процес якого оновлюється. Коли повідомлення оприлюднюється у темі MQTT, повідомлення відправляється брокеру повідомлень AWS IoT MQTT, який відповідає за відправлення усіх повідомлень, оприлюднених у MQTT–темі, для усіх клієнтів, підключених до цієї теми.

Зв’язок між пристроєм та AWS IoT захищено завдяки сертифікатам X.509. Сертифікат має бути створено автоматично, або завантажено користувачем. У будь–якому випадку сертифікат мусить бути зареєстрований та активований завдяки AWS IoT, а потім скопійовано на ваш пристрій. Коли ваш пристрій спілкується з AWS IoT, він подає сертифікат AWS IoT як посвідчення.

Користувачем занадаються правила, що визначають одну або кілька дій для здійснення на основі даних у повідомленні. Наприклад, можна оновлювати або задавати дані з таблиці DynamoDB, або запустити певну функцію. Правила

визначають вирази для фільтрування повідомлень. Коли правило синхронізується з повідомленням, двигун правил виконує дію, використовуючи вибрані властивості. Правила також відіграють роль IAM, яка надає AWS IoT доступ на ресурси AWS, використовувані для здійснення дії. Архітектура AWS IoT зображена на рисунку 3.1.

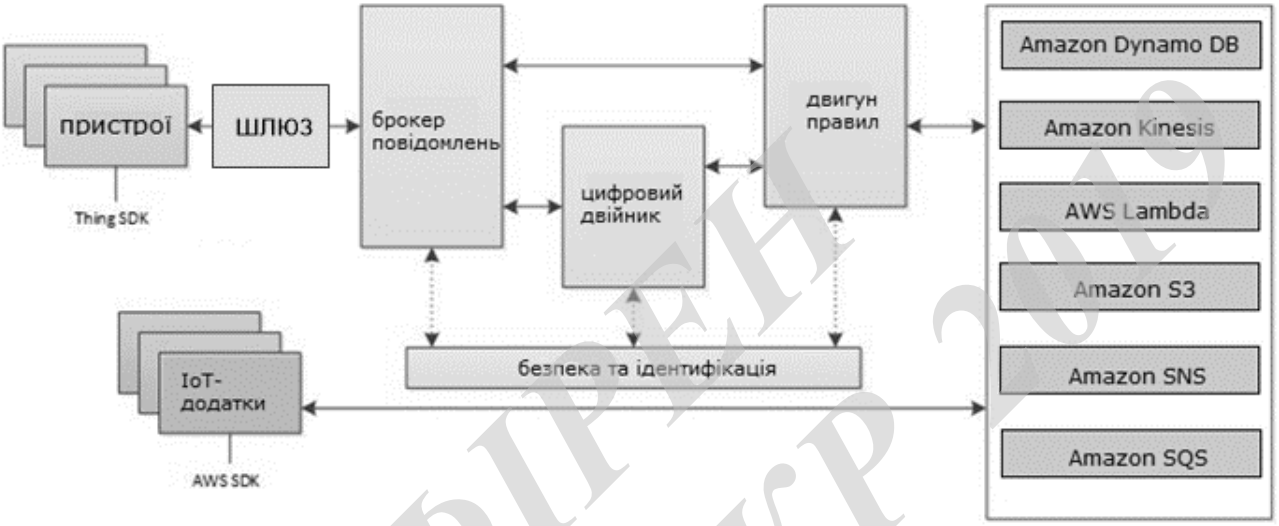


Рисунок 3.1 – Архітектурна будова AWS IoT

Кожен пристрій має цифрового двійника, який зберігає та дістає інформацію про стан. Кожен елемент в інформації про стан має два записи: стан, останній з якого ідентифікується пристроєм, і бажаний стан, запитується програмою. Програма може запитати дійсну інформацію про стан для пристрою. Двійник відповідає на запит, відсилаючи документ JSON з інформацією про стан (повідомляється і за бажанням), метадані та номер версії. Програма може використовувати пристрій, надіславши запит на оновлення свого стану. Цифровий двійник приймає запит на оновлення стану, змінює інформацію про стан та відправляє повідомлення про те, що інформація про стан була змінена. Пристрій приймає повідомлення, оновлює стан і повідомляє про його новий статус [18].

3.1.2 Принцип роботи сервісів на мережі Wi–Fi

Для організації роботи сервісу, насамперед потрібен акаунт AWS. Як тільки AWS IoT Button буде під'єднана до мережі Wi–Fi і отримає виділений для неї сертифікат і приватний ключ, буде здійснено її безпечне підключення до AWS IoT Core. При натисканні кнопка буде оприлюднювати повідомлення у темі. Завдяки сервісу правил AWS IoT можна оптимізувати маршрутизацію подій одиничним, подвійним і тривалим натисканням кнопки до будь–якого сервісу AWS. До того ж, можна налаштувати відсилання повідомлень самому собі через Amazon SNS або зберігання даних про натискання у таблиці Amazon DynamoDB. Можна навіть запрограмувати власну логіку завдяки функції AWS Lambda, написаної на Node.js, Python або Java, а потім налаштувати функцію на підключення до сторонніх сервісів або інших приладів, підключеним до IoT.

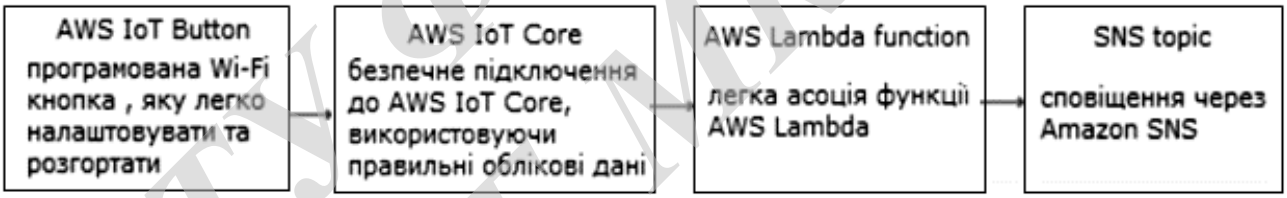


Рисунок 3.2 – AWS IoT. Основні блоки

AWS IoT безпосередньо інтегрується з такими службами AWS:

- Amazon Simple Storage Service – здійснює масштабоване зберігання у Cloud AWS. Сучасні компанії мусять вміти просто та безпечно збирати, зберігати та аналізувати дані у величезному масштабі. Amazon S3 – це об'єкт зберігання, використаний для зберігання та вилучення будь–яких обсягів даних з будь–яких джерел: веб–сайтів і мобільних додатків, корпоративних додатків, а також даних з датчиків або приладів IoT. Сервіс забезпечує надійність зберігання на рівні 99,999999999 % і використовується для зберігання мільйонів прикладних програм, що використовуються в усіх галузях промисловості. S3 відкриває найширші можливості для надання безпеки та

відповідає найсуворішим нормативним вимогам. Сервіс забезпечує клієнтам гнучкість у керуванні даними, здійснюючи оптимізацію витрат, контроль доступу та відповідність вимогам. S3 надає функціональні можливості для здійснення запитів до сервісу без вилучення, що дає змогу використовувати потужні аналітичні інструменти для опосередкованої обробки даних, що зберігаються в S3.

• Amazon DynamoDB – надає керовану базу даних NoSQL. це швидкий і гнучкий сервіс баз даних NoSQL. Він використовується для будь–яких додатків, що вимагають постійної роботи із затримкою не більше кількох мілісекунд на будь–який масштаб. Ця повністю керована обласна база даних підтримує роботу на базі документів та пар «ключ–значення». Гнучка модель даних, постійна продуктивність та автоматичне масштабування пропускної здатності роблять цей сервіс відмінною платформою для мобільних та інтернет–додатків, ігор, реклами, IoT та багатьох інших додатків. Amazon DynamoDB Accelerator (DAX) – це абсолютно керований високоактивний кеш пам’яті, який дає змогу зменшити час відгуку DynamoDB з мілісекунд до мікросекцій навіть при обробці мільйонів запитів у секунду.

• Amazon Kinesis – дає змогу в реальному часі оформляти потокові дані у масовому масштабі. Завдяки Amazon Kinesis можна просто збирати, обробляти й аналізувати потокові дані у режимі теперішнього часу, щоб своєчасно отримувати аналітичні результати і миттєво реагувати на нову інформацію. Надані службою Amazon Kinesis основні можливості надають змогу економічно обробляти поточні дані на будь–якому масштабі, а також здійснюють гнучкість при виборі інструментів, що оптимально відповінадають вимогам програми. Amazon Kinesis дає змогу в режимі теперішнього часу збирати такі дані, як відео– та аудіопотоки, додатки журналів, події навігації користувачів по веб–сайтам і телеметричні дані мережі Internet для машинного навчання, аналізу та інших додатків. Amazon Kinesis надає доступ обробляти й аналізувати дані за часом поступу й реагувати швидко, а не чекати, поки усі дані будуть зібрані, щоб здійснити їх обробку.

• AWS Lambda – запускає ваш код на віртуальних серверах від Amazon EC2 у відповідь на події. AWS Lambda дає змогу відкривати програмні коди без виділення серверів та керування ними. За допомогою Lambda можна запускати вірогідно будь–що види програм і серверних сервісів, водночас виконувати що–небудь операції адміністрації не необхідно. Просто завантажте програмний код, і Lambda гарантує усі ресурси, потрібні для його виконання та масштабування, з високим ступенем доступності. Можна здійснити автоматичний запуск програмного коду з інших сервісів AWS або безпосередньо з будь–якого мобільного або веб–додатка.

• Amazon Simple Notification Service – це гнучка, повністю керована служба надсилання повідомлень по моделі «публікація–підписка» та повідомлення для мобільних приладів, що дає змогу координувати доставку повідомлень для підписаних кінцевих точок і клієнтів. Завдяки SNS можна надсилати повідомлення більшій кількості отримувачів, включаючи розподілені системи та сервіси, а також мобільні пристрої. Сервіс дає змогу надійно відправляти повідомлення з усіма кінцевими точками при будь–якому масштабі. Розпочати роботу з SNS можна за кілька хвилин, використовуючи Консоль управління AWS, інтерфейс командного рядка AWS або AWS SDK всього з трьома простими API. SNS дає змогу ігнорувати складності та додаткові витрати, пов’язані з обслуговуванням виділеної ПО та інфраструктури для надсилання повідомлень, а також з керуванням такими.

• Amazon Simple Queue Service – зберігає дані у черзі, що необхідно завантажити, використовуючи додатки. Служба простої черги Amazon (SQS) – повністю керована послугами повідомлень, що дає змогу легко ізолювати та масштабувати мікросервіси, що розподілені системи та безсерверні додатки. Одна із сучасних рекомендацій по розробці ПО – створення архітектури, у щой кожний інший компонент розв’язання виконує свою ідентифіковану задачу. Такий підхід дає змогу підвищити масштабність та надійність готової системи. SQS дає змогу легко та економічно відокремити компоненти обласного додатка та розрахувати їх роботу. За допомогою SQS можна надсилати, зберігати та

отримувати повідомлення компонентів програмного забезпечення у будь–якому масштабі без втрати повідомлень і необхідності забезпечити сталу доступність інших сервісів [18].

3.2 Фактори, що впливають на продуктивність Web–служб

Досліджуються фактори, що впливають на продуктивність Web–служб, а також здійснюється методика розробки простих кількісних моделей для найкращого вибору протоколу по критерію продуктивності, що прямопропорційне числу користувачів. Web–служба – це послуга, що висвітлюється через Internet, яка виконує задані завдання або виробляє транзакції [29]. Web–служби містять модульну структуру і є самодостатніми модулями, що можна зобразити, опублікувати і виконати через Internet. Web–служба може бути бізнес–процесом, додатком і навіть обчислювальним ресурсом. До прикладів Web–служб можна віднести усе, починаючи з послуг електронних платежів і закінчуючи послугами розповсюдження вмісту та зберігання інформації. Web–служби можна автоматично викликати з додатків, а не тільки з браузерів.

Бізнес стає залежнішим від використання Web–служб, тому їх робочі характеристики (тобто продуктивність) стають дуже необхідними. Чим більше інформації і послуг можна взяти від компанії, тим більше запитів він отримує. А чим більше запитів отримує Web–служби, тим більша вірогідність, що користувачі занадто довго чекатимуть відгуку на свій запит. І тоді, переважно, Web–користувачі (можливі покупці) будуть незадоволені і будуть відмовлятися від отримання послуг.

Час відгуку і пропускна здатність – це два найважливіші показники продуктивності Web–систем. Зазвичай під пропускною спроможністю Web–служби мають на увазі швидкість обслуговування запитів, що вимірюється

кількістю операцій в секунду. Через велике розмаїття розмірів запитуваних Web–об’єктів, пропускну здатність також вимірюють у бітах в секунду (біт / с, bps).

Незважаючи на те, що затримка установки зв’язку має вплив на сприйняття користувачами сайту, водночас вона є нетривалим, одноразово діючим фактором продуктивності сайту, тобто він вимірюється один раз на запит і не відображає щость усього сеансу [18].

Отже, до найчастіше використовуваних показників продуктивності Web–служб належать:

- пропускна здатність, запитів / с;
- пропускна здатність, Мбіт / с;
- час відгуку при наскрізний передачі даних;
- навантаження центрального процесору;

3.3 Опис системи та розрахунок пропускної здатності

В офісному центрі користуються певним товаром, на який прикріплено кнопку Amazon Dash. Коли закінчується товар, користувач натискає кнопку. Сповіщення надсилається на смартфон адміністратора. Адміністратор зі свого боку проходить багатофакторну автентифікацію, вибирає зручну дату і час та підтверджує замовлення. У цифровому двійнику кнопки «зашита» вся потрібна інформація: починаючи від цифрового ідентифікатора, закінчуючи складом та специфікацією необхідного товару.

Запит обробляється сервером, та надсилається кур’єру. Коли товар відправлений, менеджер підтверджує оплату і після цього відбувається оплата.

Аналіз було проведено на реалізації сервісу IoT, що розгорнутий на інфраструктурі Amazon, який може бути здійснений на транспортному рівні протоколом MQTT чи HTTP.

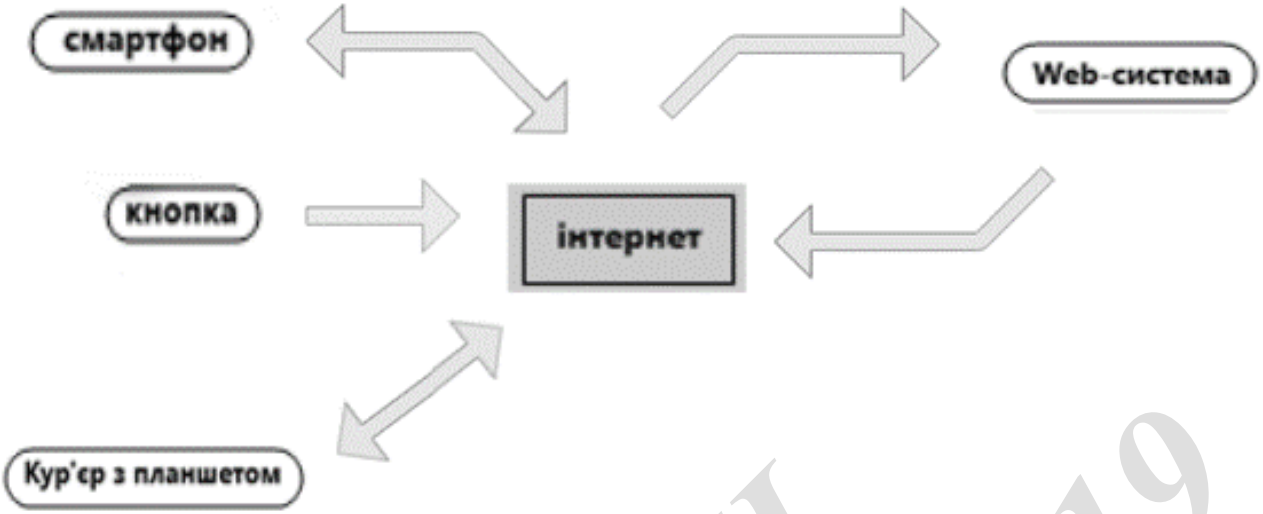


Рисунок 3.3 – Схематичне відображення процесу

Нижче наведено типи запитів, що беруть участь у повному циклі від натискання кнопки, до підтвердження замовлення:

1. 1 тип – замовлення.
2. 2 тип – підтвердження замовлення.
3. 3 тип – багатофакторна автентифікація.
4. 4 тип – підтвердження доставки.
5. 5 тип – оплата замовлення.

Кожен з приведених типів може мати різний об’єм даних. Нижче приведено об’єм інформації простого цифрового двійника та детального.

а) простий варіант (10 В):

1) ідентифікаційний номер.

б) детальний (2 kB):

2) ідентифікаційний номер.
3) назва.
4) тип товару.
5) склад товару.
6) дата виготовлення.
7) адреса.

8) об’єм.

9) державні норми.

10) вимоги до товару

У таблицях 3.1 та 3.2 наведено розміри повідомлень для різних типів запитів.

Таблиця 3.1 – Варіації розміру повідомлень при використанні HTTP

	Тип запиту	1	2	3	4	5
Розміри повідомлень, Біт	Варіант 1	1290	5290	10290	3290	100290
	Варіант 2	2290	7290	12290	6290	110290
	Варіант 3	6290	12290	16290	10290	120290
	Варіант 4	8290	15290	17290	12290	140290
	Варіант 5	9290	18290	19290	14290	165290
	Варіант 6	11290	20290	22290	17290	170290
	Варіант 7	16290	25290	24290	20290	200290
	Варіант 8	20290	30290	26290	28290	250290
	Варіант 9	36290	50290	30290	33290	260290
	Варіант 10	40290	77290	33290	100290	270290

Таблиця 3.2 – Варіації розміру повідомлень при використанні MQTT

	Тип запиту	1	2	3	4	5
Розміри повідомлень, Біт	Варіант 1	1002	5002	12002	3002	100002
	Варіант 2	2002	7002	12002	6002	110002
	Варіант 3	6002	12002	16002	10002	120002
	Варіант 4	8002	15002	17002	12002	14002
	Варіант 5	9002	18002	19002	14002	165002
	Варіант 6	11002	20002	22002	17002	170002
	Варіант 7	16002	25002	24002	20002	200002
	Варіант 8	20002	3002	26002	28002	250002
	Варіант 9	36002	50002	30002	33002	260002
	Варіант 10	40002	77002	33002	100002	270002

Мережевий трафік містить пульсуючий характер [20]. "Пульсуючий" означає, що дані перенадаються випадково, з надвисокими швидкостями, що перевищують середні швидкості у 8–10 випадкув [21]. Також вважається, що мережевий трафік існує у кількох масштабах часу. Припустимо, що фірма обслуговує 1000000 клієнтів. Кожен клієнт здійснює замовлення товару 1 раз на тиждень. Навантаження має піковий характер. Замовлення відбуваються з 06:00 до 09:00 та з 18:00 до 22:00. З цього слідує, що кожного дня тривалість замовлень складає 7 годин.

Пропускна здатність сервера, виражена у запитах / с, складатиме:

$$\frac{1000000}{7*7*3600} = 5{,}66\frac{запитів}{с}, \quad (3.1)$$

Однак, цей показник не дає ніякого уявлення щодо пропускної здатності мережі, що здійснюється у період спостереження і не дає представлення про розміри типів запитів. Отже, для оцінки пропускної здатності мережі чи мережевого адаптера необхідно розрахувати пропускну здатність в Біт / с.

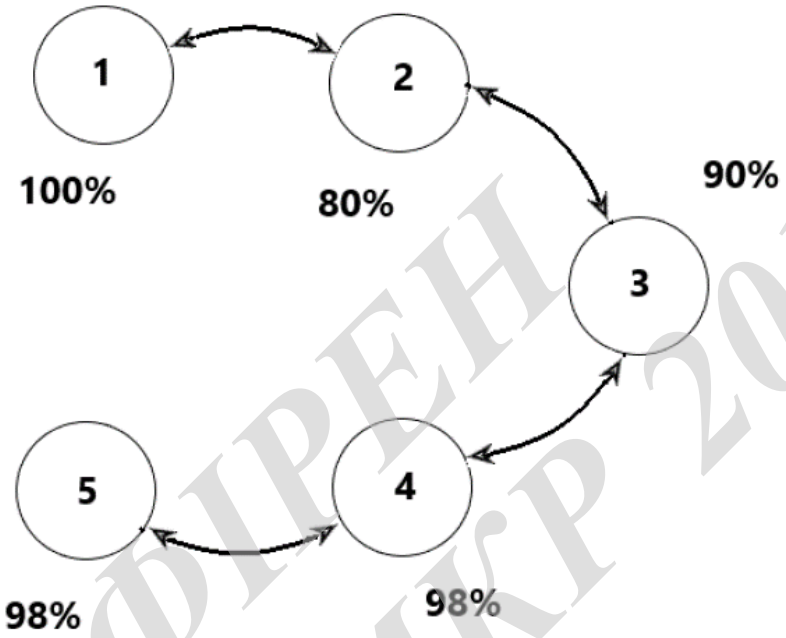


Рисунок 3.4 – Ймовірності виконання запитів

На рисунку 3.4 наведено вірогідність того, що кожен з типів запитів відбудеться.

Щоб визначити, яку частку складає кожен з типів в усій передачі, проведемо такі розрахунки:

$$\frac{1}{1+0.8+(0.8*0.9)+(0.8*0.9*0.98)+(0.8*0.9*0.98*0.98)} = 0.255, \quad (3.2)$$

$$\frac{0.8}{1+0.8+(0.8*0.9)+(0.8*0.9*0.98)+(0.8*0.9*0.98*0.98)} = 0.204, \quad (3.3)$$

$$\frac{(0.8*0.9)}{1+0.8+(0.8*0.9)+(0.8*0.9*0.98)+(0.8*0.9*0.98*0.98)} = 0.184, \quad (3.4)$$

$$\frac{(0.8*0.9*0.98)}{1+0.8+(0.8*0.9)+(0.8*0.9*0.98)+(0.8*0.9*0.98*0.98)} = 0.180, \quad (3.5)$$

$$\frac{(0.8*0.9*0.98*0.98)}{1+0.8+(0.8*0.9)+(0.8*0.9*0.98)+(0.8*0.9*0.98*0.98)} = 0.177, \quad (3.6)$$

Розрахуємо пропускну здатність для кожного типу запиту:

$$\text{Пропускна здатність} = \frac{\text{загальна кількість запитів} * \text{частка кожного з типів} * \text{середній розмір}}{\text{час спостереження}}, \quad (3.7)$$

Розрахунки для усіх типів першого варіанту:

$$\frac{1000000*0,255*(1290*8)}{176400} = 14918,3\ [Біт/с], \quad (3.8)$$

$$\frac{1000000*0,204*(5290*8)}{176400} = 48941,5\ [Біт/с], \quad (3.9)$$

$$\frac{1000000*0,184*(10290*8)}{176400} = 85866,67\ [Біт/с], \quad (3.10)$$

$$\frac{1000000*0,180*(3290*8)}{176400} = 26857,14\ [Біт/с], \quad (3.11)$$

$$\frac{1000000*0,177*(100290*8)}{176400} = 805049,00\ [Біт/с], \quad (3.12)$$

Загальна пропускна здатність – це сума пропускних здатностей для кожного з типів:

$$\text{Загальна пропускна здатність} = 14918,37 + 48941,5 + 85866,67 + \\ + 26857,14 + 805049 = 981632,7\ [\text{Біт / с}] \quad (3.13)$$

Отже пропускна здатність для першого варіанту складає 981,633 Кбіт / с ;

Розрахунки для інших варіантів виконані за аналогією в Excel, результати наведені у таблицях 3.3 та 3.4

Таблиця 3.3 – Пропускна здатність при використанні HTTP

	Тип запиту	1	2	3	4	5	Σ
Пропускна здатність, Біт / с HTTP	Варіант1	14918,37	48941,5	85866,67	26857,14	805049	981632,7
	Варіант2	26482,99	67444,9	102556	51346,94	885321,1	1133152
	Варіант3	72741,5	113703,4	135934,7	84000	965593,2	1371973
	Варіант4	95870,75	141458,5	144279,4	100326,5	1126137	1608072
	Варіант5	107435,4	169213,6	160968,7	116653,1	1326818	1881089
	Варіант6	130564,6	187717	186002,7	141142,9	1366954	2012381
	Варіант7	188387,8	233975,5	202692,1	165632,7	1607770	2398458
	Варіант8	234646,3	280234	219381,4	230938,8	2009131	2974332
	Варіант9	419680,3	465268	252760,1	271755,1	2089403	3498867
	Варіант10	465938,8	715063,9	277794,1	818693,9	2169675	4447166

Таблиця 3.4 – Пропускна здатність при використанні MQTT

	Тип запиту	1	2	3	4	5	Σ
Пропускна здатність, Біт / с MQTT	Варіант1	11587,76	46277,01	83463,4	24506,12	802737,1	968571,4
	Варіант2	23152,38	64780,41	100152,7	48995,92	883009,3	1120091
	Варіант3	69410,88	111038,9	133531,4	81648,98	963281,4	1358912
	Варіант4	92540,14	138794	141876,1	97975,51	1123826	1595012
	Варіант5	104104,8	166549,1	158565,4	114302	1324506	1868027
	Варіант6	127234	185052,5	183599,5	138791,8	1364642	1999320
	Варіант7	185057,1	231311	200288,8	163281,6	1605458	2385397
	Варіант8	231315,6	277569,5	216978,1	228587,8	2006819	2961270
	Варіант9	416349,7	462603,5	250356,8	269404,1	2087091	3485805
	Варіант10	462608,2	712399,5	275390,8	816342,9	2167363	4434104

Таблиця 3.5 – Загальна пропускна здатність при використанні MQTT

	Тип запиту	MQTT	HTTP	Δ
Пропускна здатність, Біт / с	Варіант1	968571,4	981632,7	1,013485
	Варіант2	1120091	1133152	1,011661
	Варіант3	1358912	1371973	1,009611
	Варіант4	1595012	1608072	1,008188
	Варіант5	1868027	1881089	1,006992
	Варіант6	1999320	2012381	1,006533
	Варіант7	2385397	2398458	1,005475
	Варіант8	2961270	2974332	1,004411
	Варіант9	3485805	3498867	1,003747
	Варіант10	4434104	4447166	1,002946

Рисунок 3.5 – Відношення загальної пропускної здатності

З отриманих результатів можна підсумувати, що мережеве з'єднання мусить мати мінімальну пропускну здатність 5 Мбіт / с, рекомендовано 10 Мбіт / с. А при збільшенні розмірів запитів, різниці між протоколами майже немає. Тому при великих файлах варто використовувати HTTP, бо він не вимагає додаткових налаштувань при розгортанні. При передачі запитів, та відповідей невеликих розмірів, краще використовувати MQTT.

3.4 Середній час відгуку

Визначення затримок, та "вузьких місць" має істотне значення для того, щоб робити зміни у програмному забезпеченні, модернізації обладнання або установки, здійснюючи швидкісні лінії передачі даних. Затримки можна розкласти на 3 масштабні складові:

1. Процесор. Центральний процесор здійснює обробку даних з приладів, а також за ініціалізацію зв'язку.

2. Мережа. Мережа породжує затримки під час відправки інформації від клієнта до сервера і назад, від сервера до клієнта. Ці затримки є функціями різних компонентів на відстані між клієнтом і сервером, таких як модеми, маршрутизатори, лінії передачі, мости і комутатори.

3. Сервер. Час перебування на сервері, R' Server – це час, що витрачається на здійснення запиту. Воно включає у себе час обробки і час очікування на різних складових сервера, таких як процесор, диск і мережевий адаптер.

Коли запитуваний документ не міститься у кеші клієнта, час відгуку R на запит являє собою суму часу перебування запитів на усіх ресурсах:

$$R_{miss}=R'_{CPU}+R'_{Network}+R'_{Server}, \quad (3.14)$$

де R'_{CPU} – час обробки процесором.

$R'_{Network}$ – час передачі в мережі.

R'_{Server} – час перебування на сервері.

Розглянемо середній час відгуку для наведених протоколів. Уявімо, що документи не кешуються. Середній час перебування на сервері (R' Server) – 3,6 с, а час, затрачений процесором на обробку отриманих даних (R' CPU) – 0,3 с. Пропускна здатність мережі складає 100 Мбіт / с.

Час передачі у мережі ($R'_{Network}$) відповідає розміру даних у бітах, поділеному на пропускну здатність мережі. Визначимо розрахунки для першого варіанта. Розрахунки для інших варіантів було здійснено у програмі Excel, результати зображено у таблиці 3.6.

$$R'_{Network(HTTP)} = \frac{120450*8}{100000000} = 0{,}009639, [c] \quad (3.15)$$

$$R'_{Network(MQTT)} = \frac{119010*8}{100000000} = 0{,}009521, [c] \quad (3.16)$$

$$R_{miss(HTTP)} = 0.009639 + 0.3 + 3.6 = 3{,}909636, [c] \quad (3.17)$$

$$R_{miss(MQTT)} = 0.009521 + 0.3 + 3.6 = 3{,}909521\ [c] \quad (3.18)$$

$$\Delta = \frac{R_{miss(HTTP)}}{R_{miss(MQTT)}}; \quad (3.19)$$

$$\Delta = \frac{3{,}909636}{3{,}909521} = 1.000029467 \quad (3.20)$$

Таблиця 3.6 – Середній час відгуку

Протокол	MQTT	HTTP	Δ
Варіант1	3,9095	3,9096	1,000029467
Варіант2	3,9109	3,9110	1,000029456
Варіант3	3,9131	3,9132	1,000029439
Варіант4	3,9153	3,9154	1,000029423
Варіант5	3,9180	3,9181	1,000029403
Варіант6	3,9192	3,9193	1,000029394
Варіант7	3,92280	3,9229	1,000029367
Варіант8	3,92832	3,9284	1,000029326
Варіант9	3,9327	3,9328	1,000029293
Варіант10	3,94160	3,9417	1,000029227

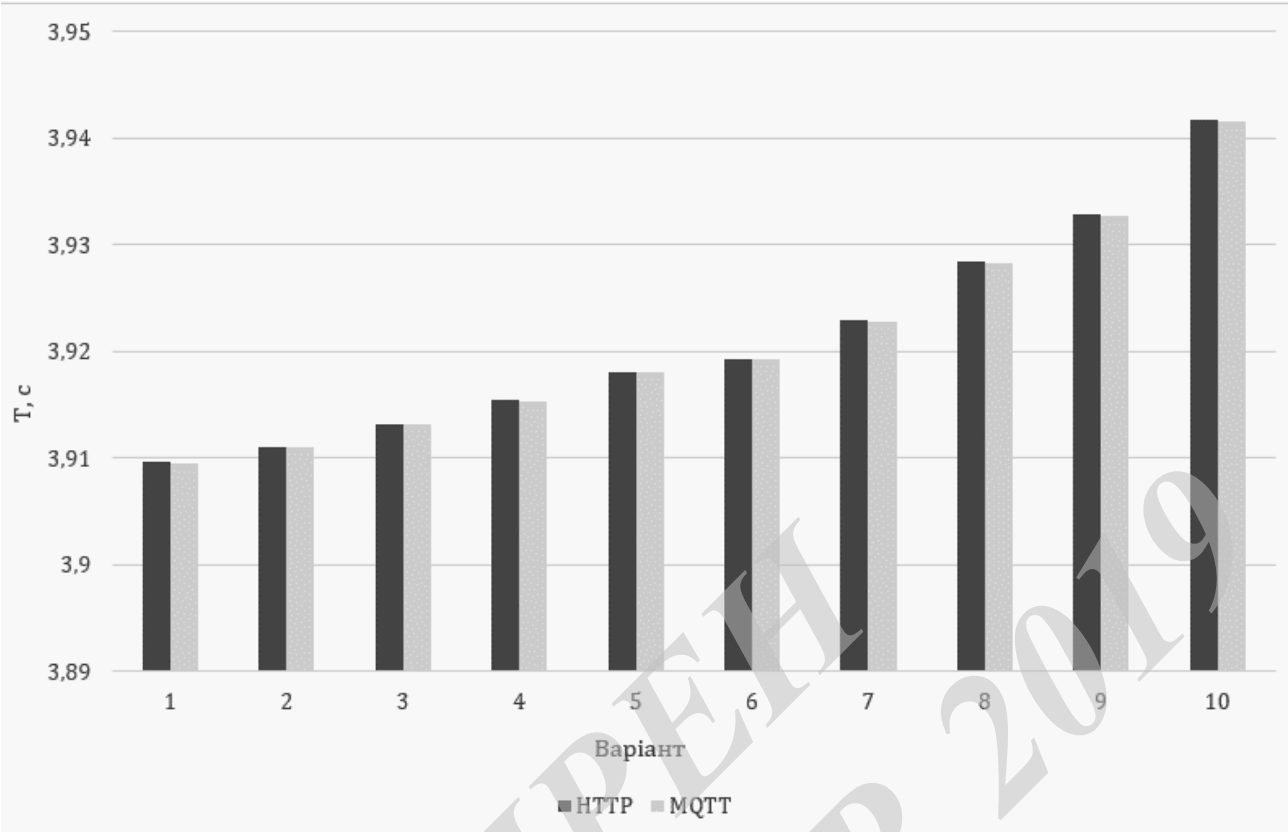


Рисунок 3.6 – Порівняння середнього часу відгуку для протоколів

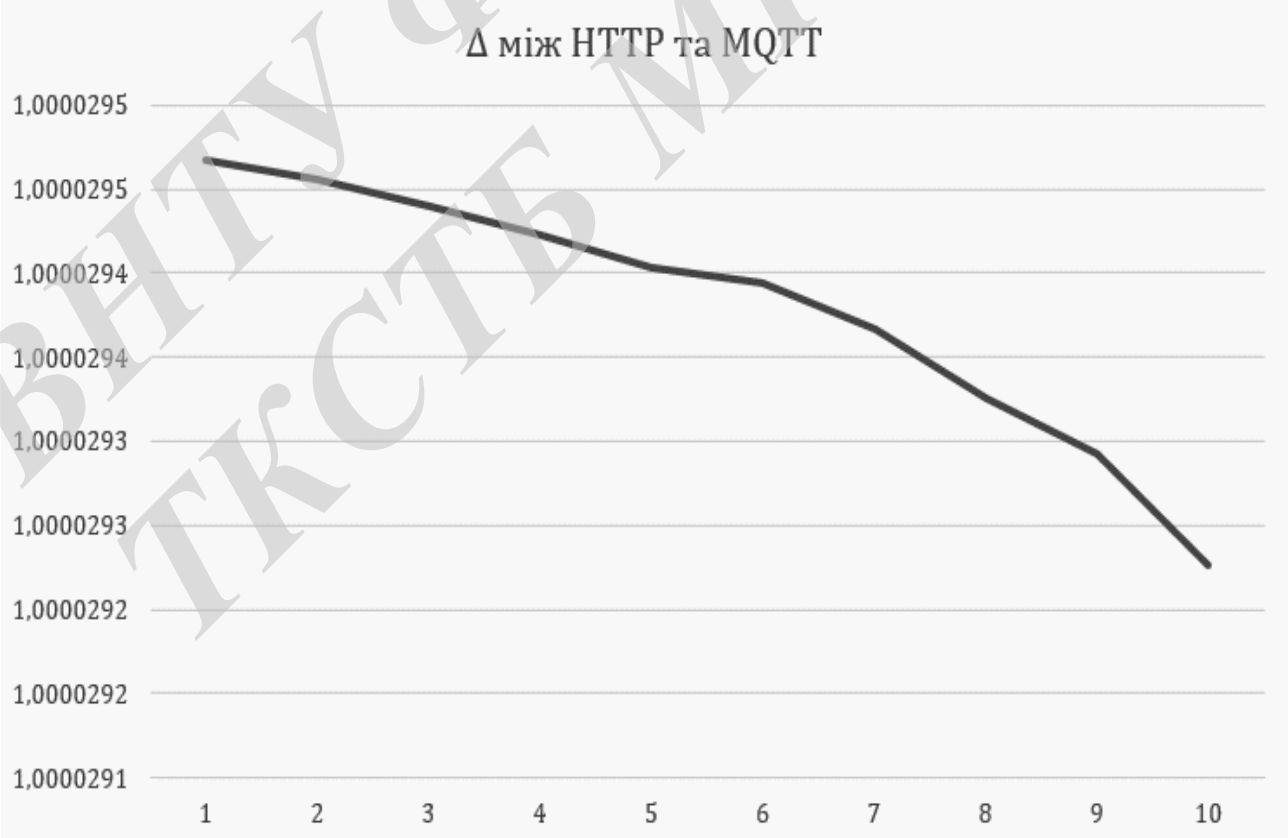


Рисунок 3.7 – Відношення середнього часу відгуку

3.5 Пропускна спроможність при використанні кешуючого проксі–сервера

Проксі–сервер, кеш і сервер дзеркального відображення – це три технології, що передбачаються для поліпшення характеристик продуктивності і безпеки Web. Згадані технології призначені для зменшення часу доступу до Web–документів, збільшення пропускної здатності мережі, необхідної для передачі Web–документів, потреби у серверах, що містять найпопулярніші документи, а також підвищення безпеки електронних служб [21].

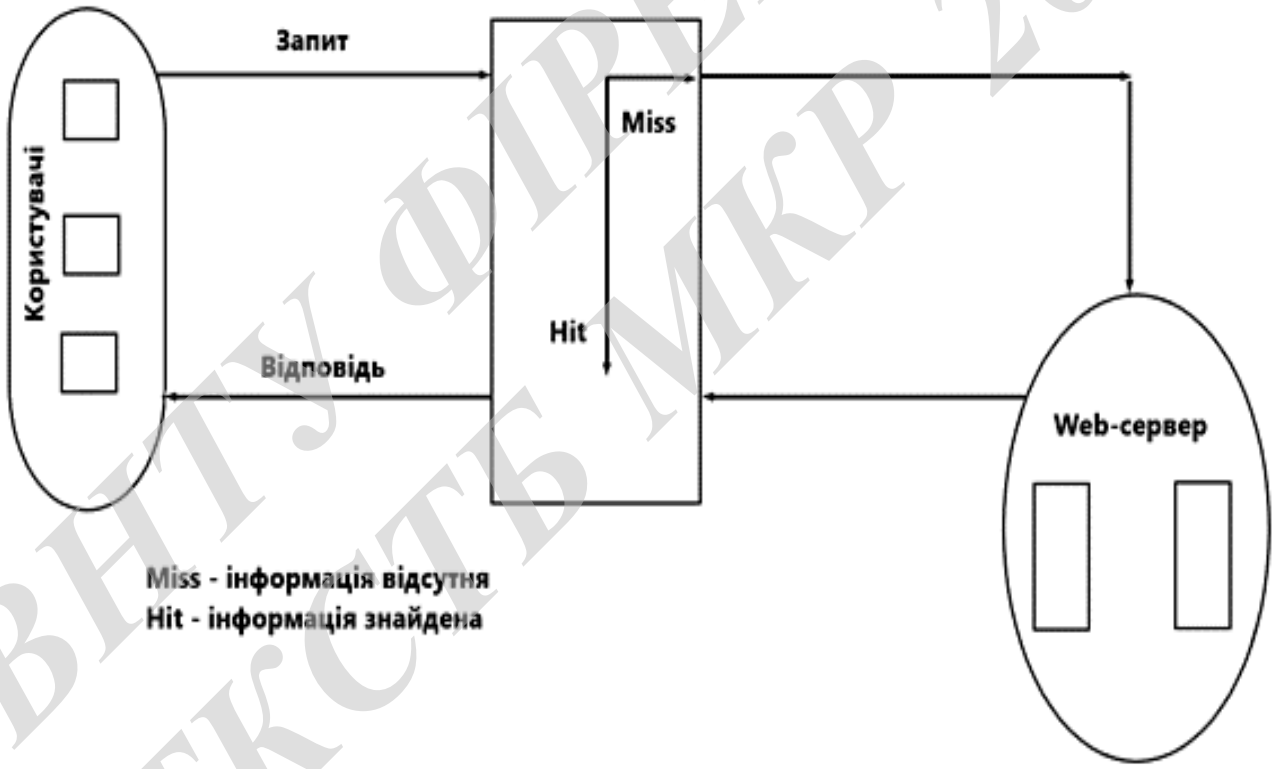


Рисунок 3.8 – Архітектура проксі–сервера

Проксі–сервер являє собою особливий тип Web–сервера. Він має змогу виступати як і серверу, так і клієнту (див. рис. 3.8). Проксі–сервер працює як агент, що зображає сервер для клієнта і клієнта для сервера. Проксі–сервер отримує запити від клієнтів і направляє їх на Web–сервери. Як тільки проксі–

сервер приймає відповіді від віддалених серверів, він пересилає їх клієнтам. Спочатку проксі–сервери були дійсні для надання доступу в Web користувачам з приватних мереж, що могли здійснювати доступ в Internet тільки через брандмауер.

Проксі–сервер робить набагато більше, ніж просто комутує відповіді. Проксі–сервери для Web можуть бути оптимізовані так, щоб кешувати прийняті відповіді, стаючи, у такий спосіб, кешуючими проксі–серверами. У великих розподілених інформаційних системах, подібних World Wide Web, кешування – це доступ до високої продуктивності. Основна ідея кешування досить–таки примітивна: зберегти необхідні документи у місцевих файлах або проксі–серверах для можливого використання. Отже, відпадає необхідність у завантаженні документа при пізнішому його запиті. Кешування зтоваруть до мінімуму час доступу завдяки максимально близькому розташуванню даних до їх споживачів. Отже, кешування збільшує швидкість доступу і зменшує мережевий трафік, оскільки часто запитуваний документ повертається з найближчого кешу швидше, ніж з віддалених серверів. До того ж, кешування зменшує навантаження на сервер і збільшує коефіцієнт готовності завдяки дублюванню документа на кількох серверах [24].

Розрахуємо, яке значення пропускної здатності можна нівелювати, використовуючи кешуючий проксі–сервер.

$$\text{Економія пропускної здатності} = \text{Пропускна здатність} * \\ * \text{Результативність} * \% \text{ кешованого трафіку}, \quad (3.21)$$

Протокол HTTP завбачає кешування даних, що дає змогу знівелювати частину пропускної здатності мережі. У цілях аналізу показника кешування, розглянемо ситуацію, коли результативність складає 68 % і 42 % всього трафіку можна знівелювати, використовуючи кешування. Пропускна здатність HTTP складає 4,4471 Мбіт / с, а MQTT – 4.434 Мбіт / с.

$$\text{Економія ПЗ} = 4{,}4471 * 0{,}42 * 0{,}60 = 1{,}12 \text{ [Мбіт / с]}, \quad (3.22)$$

$$\text{Пропускна здатність} = 4{,}4471 - 1{,}12 = 3{,}327 \text{ [Мбіт / с]}, \quad (3.23)$$

Оскільки протокол MQTT не використовує кешування, то використання HTTP буде переважати у розмірі:

$$4{,}434 - 3{,}327 = 1{,}107 \text{ [Мбіт / с]}, \quad (3.24)$$

Рисунок 3.9 – Порівняння пропускної здатності протоколів при використанні кеш–серверу

3.6 Розрахунок використання ЦП серверу додатків при обробці запитів

Сервер додатків (application server) являє собою програмне забезпечення, виконує усі прикладні операції між споживачами, і базою даних компанії.

Загалом, сервер додатків отримує запит клієнта, виконує деяку бізнес–логіку і взаємодіє з сервером транзакцій і / або сервером бази даних. Зазвичай, сервери додатків використовують такі характеристики:

1) зберігають і виконують логіку додатків, написаних різними мовами програмування (наприклад, Java, C або C++);

2) керують великими обсягами транзакцій з серверними базами даних;

3) забезпечують сумісність з усіма існуючими мережевими стандартами, включаючи HTTP, HTML, XML, CGI, Netscape Server API (NSAPI), Microsoft Internet Server API (ISAPI) і Java;

4) працюють з більшістю популярних Web–серверів, браузерів і систем управління базами даних.

Сервери додатків мають бути реалізовані кількома різними способами: у вигляді CGI–сценаріїв, FastCGI–сценаріїв, Java–сервлетів, серверних додатків і серверних сценаріїв [22].

Уявімо, що Web–сервіс отримує приблизно 20 відвідувань в секунду. 0,8 запитів проходять усі етапи. Кожна з цих транзакцій генерує HTTP – запити (CGI–сценарії), що виконуються на Web–сервері. Необхідно знати навантаження на центральний процесор, що створюється сценаріями. Навантаження, що викликається HTTP – запитом було змодельовано нижченаведеним прикладом. Середня потреба в обслуговуванні ЦП HTTP – запитом (D_{cpu}^{HTTP}) складає 12 мс. Використовуючи закон для забезпечення в обслуговуванні, отримуємо:

$$U_{cpu}^{HTTP}=X_{HTTP}*D_{cpu}^{HTTP}, \quad (3.25)$$

де X_{HTTP} – пропускна здатність сервера в HTTP – запитах, виконаних за секунду,

U_{cpu}^{HTTP} – використання ЦП, що пов’язане з виконанням HTTP – запитів.

Інтенсивність вхідного потоку ($ccccc$) може бути розрахована, як:

$$\lambda_{HTTP} = 20 * 0.8 = 16\ [CGI\text{–запитів / с}], \quad (3.26)$$

Вважаємо, що поток постійний $XHTTP = \lambda HTTP$. Отже:

$$U_{cpu}^{HTTP} = 16 * 0.012 = 19\ \%, \quad (3.27)$$

З отриманих результатів ми бачимо, що на обробку HTTP – запит витрачається 19 % ЦП.

Розглядаючи MQTT, використовуються Java–сервлети. Сервлет, що підключається до теми MQTT, і пересилає усі повідомлення, що він отримує через WebSocket. Згідно статистики, сервлети на 30 % менш ресурсномісткі, ніж CGI–додатки. Потреби в обслуговуванні ЦП зі сторони сервлетів складає:

$$D_{cpu}^{MQTT} = D_{cpu}^{HTTP} * 0.7 = 12 * 0.7 = 8.4\ [\text{мс}], \quad (3.28)$$

Використовуючи формулу (3.25), отримаємо:

$$U_{cpu}^{HTTP} = 16 * 0.0084 = 13\ \%, \quad (3.29)$$

Отримані результати наглядно демонструють, що Java–сервлети (MQTT) знижують використання ЦП з 19 % до 13 %.

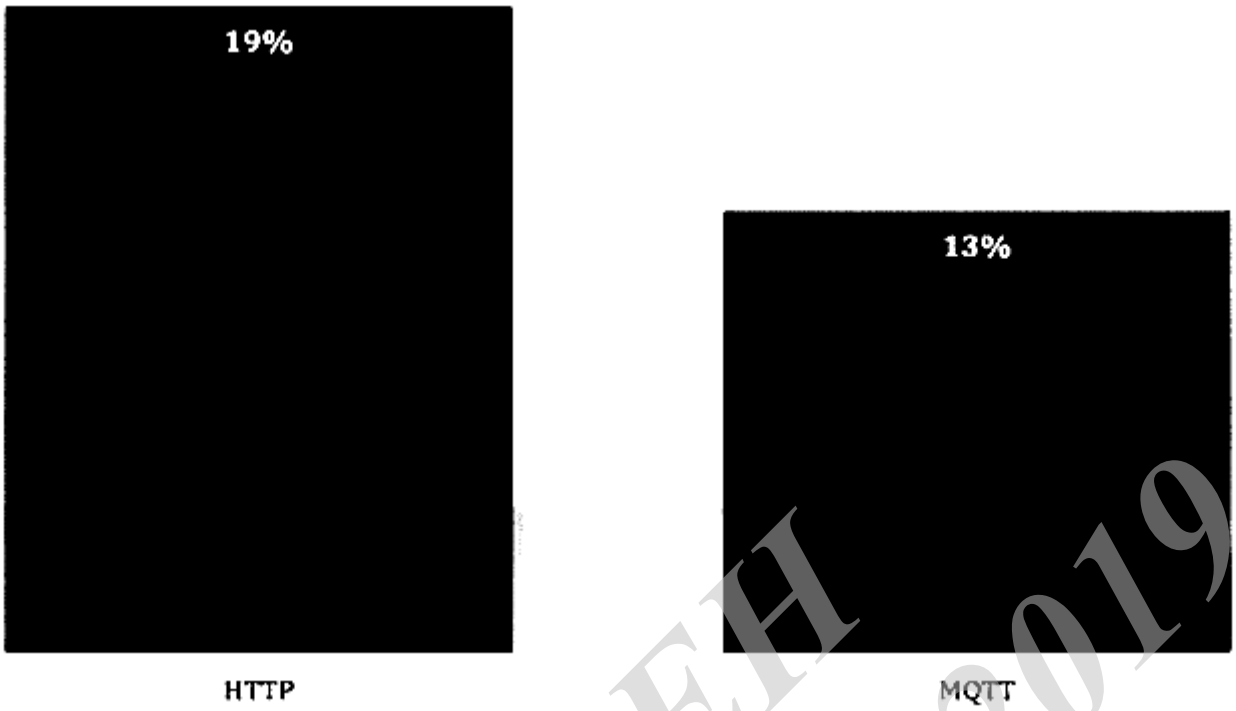


Рисунок 3.10 – Використання ЦП серверу, при обробці запитів

3.7 Час обслуговування в різних мережах

Повідомлення від клієнта до сервера мусить пройти через кілька рівнів протоколу та може отримуватись через одну або більшу кількість мереж (рис. 3.11).

Рисунок 3.11 – З’єднання між клієнтом і сервером

Повідомлення від клієнта до Web–сервера має пройти через три мережі з швикостями 10 Мбіт / с, 100 Мбіт / с, і 16 Мбіт / с відповідно. Повідомлення, що відтворюються додатком, мусять пройти через стек протоколів, що включають, принаймні, транспортний протокол (TCP чи UDP), Internet–протокол (IP) та мережевий протокол. Протокольні об'єкти кожного рівня спілкуються між собою завдяки обміну протокольними одиницями обміну (ProtocolDataUnit, PDU), що складаються із заголовка та сфери даних [23].

Протокольні одиниці обміну по–різному називаються у різних протоколах і зазвичай відводять максимально можливий розмір під сфера даних. На мережевому рівні максимальний розмір сфери даних носить назву максимального розміру блоку корисного навантаження пакету (maximumtransmissionunit, MTU). Для мережі першого ISP (InternetServiceProvider) MTU = 1 500 байт, для мережі другого ISPMTU = 4 472 байт, а для мережі третього ISP MTU = 4 444 байт.

Отже, маршрутизатори мають фрагментувати дейтаграми при переході до мережі з нижчим значенням MTU. Фрагменти збираються заново на рівні Internet–протокола (IP) на хості місця призначення.

Кожен рівень протоколу притоваруть свій власний заголовок, а іноді й хвіст (тобто заключну частину). Час обслуговування повідомлення мережею – це час, потрібний на передачу цього повідомлення через мережу. Згаданий час прямопропорційний відношенню кількості байт, необхідних для передачі повідомлення, включаючи заголовок та хвіст (службова інформація) до пропускної здатності мережі. Розмір заголовка протоколу залежить від протоколів, що використовуються та від фрагментації повідомлення, яка може знадобитися на мережевому рівні.

Для зображення методики розрахунку часу обслуговування повідомлення мережею, наведемо кілька прикладів.

Приклад перший:

Клієнт на рис. 3.12 посилає 300–байтний запит Web–серверу та отримує 10 000–байтну відповідь. Взаємодія між клієнтом та сервером виконується через TCP–з'єднання.

Запит від клієнта до сервера знаходиться в сфери даних TCP–сегмента, який відсилається в сфера даних IP–дейтаграми. IP–дейтаграма інкапсулюється Ethernet, кадрами по ступеню її проходження по мережам. Отже, до 300–байтного запиту дописується 20–байтний TCP–заголовок. 20–байтний IP–заголовок плюс 2 байт заголовка MQTT в мережі 1, та 18 байт – у мережі 3. Тобто 300–байтний запит перетворюється в 342–байтовий кадр (= 300 + 20 + 20 + 2) у мережі 1 та 2 і в 358–байтний кадр (= 300 + 20 + 20 + 18) у мережі 3. Час на передачу кадру по мережі дорівнює розміру кадру в бітах, поділеному на пропускну спроможність мережі (в біт / с). Відповідно, час передачі для кадрів, що містять клієнтський запит, в мережах 1, 2 та 3, відповідно, складає:

$$\frac{342\times8}{10000000} = 0{,}000273,[\text{с}], \tag{3.30}$$

$$\frac{342\times8}{100000000} = 0{,}00002736,[\text{с}], \tag{3.31}$$

$$\frac{358\times8}{16000000} = 0{,}000179,[\text{с}], \tag{3.32}$$

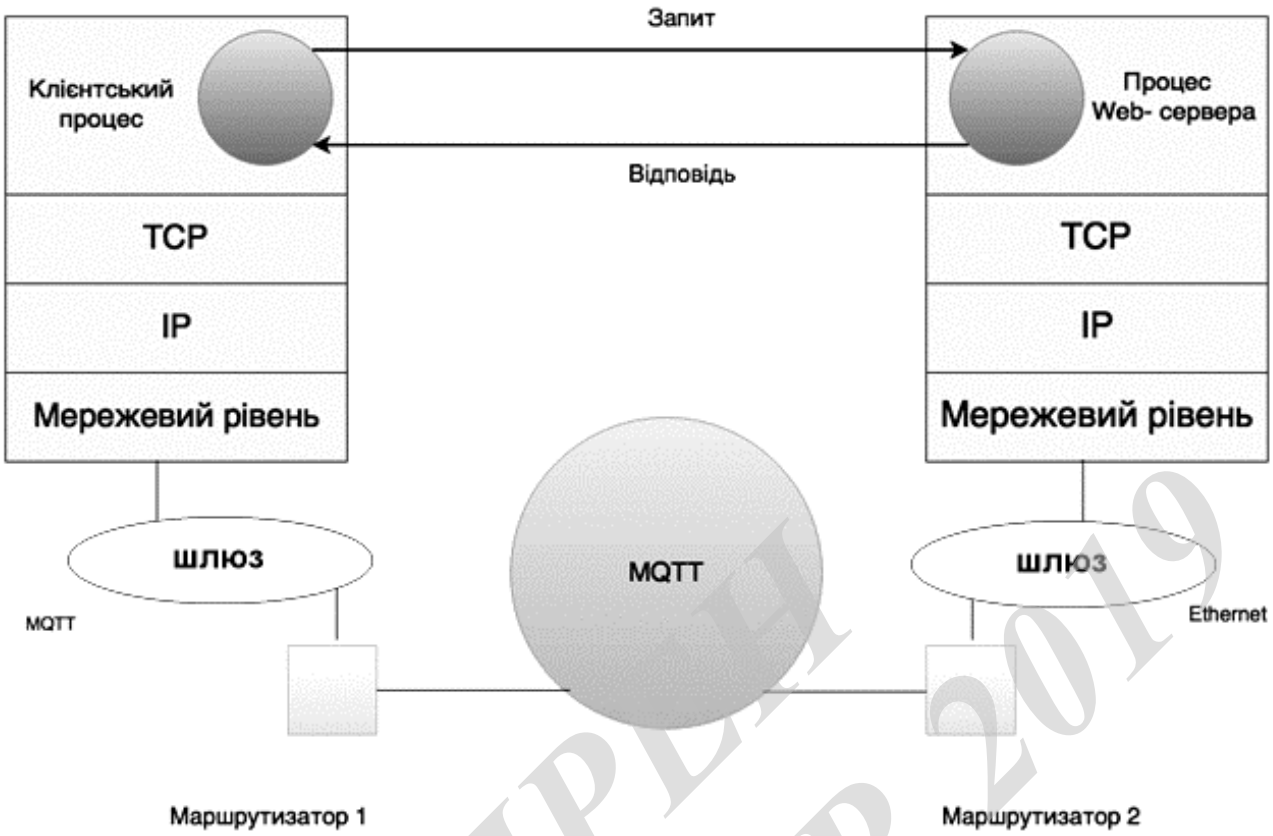


Рисунок 3.12 – Взаємодія між клієнтом та сервером

Приклад другий:

Клієнт на рис. 3.11. посилає 10 000–байтний запит Web–серверу.

Отже, до 10 000–байтного запиту дописується 20–байтний TCP–заголовок. 20–байтний IP–заголовок плюс 2 байт заголовкаMQTTв мережі 1, та 18 байт – у мережі 3. Тобто 10 000–байтний запит перетворюється в 10042–байтовий кадр (= 10000 + 20 + 20 + 2) в мережі 1 та 2 і в 10058–байтний кадр (= 10000 + 20 + 20 + 18) в мережі 3. Відповідно, час передачі для кадрів, що мають клієнтський запит, у мережах 1, 2 та 3, відповідно, складає:

$$\frac{10042\times8}{10000000} = 0{,}008033,[\text{с}], \tag{3.32}$$

$$\frac{10042\times8}{10000000} = 0{,}00080336,[\text{с}], \tag{3.33}$$

$$\frac{10058\times8}{10000000} = 0{,}005029,[\text{с}], \tag{3.34}$$

Приклад третій:

Клієнт на рис. 3.11. посилає 50–байтний запит Web–серверу. Тобто 50–байтний запит змінюється в 92–байтовий кадр (= 50 + 20 + 20 + 2) у мережі 1 та 2 і в 108–байтний кадр (= 50 + 20 + 20 + 18) у мережі 3. Відповідно, час передачі для кадрів, що включають клієнтський запит, у мережах 1, 2 та 3, відповідно, складає:

$$\frac{92\times8}{10000000} = 0{,}0000736,[\text{с}], \tag{3.35}$$

$$\frac{92\times8}{10000000} = 0{,}00000736,[\text{с}], \tag{3.36}$$

$$\frac{108\times8}{10000000} = 0{,}000054,[\text{с}], \tag{3.37}$$

Розглянемо ситуацію, коли замість MQTT використовується HTTP, при відповідних запитах довжиною 300, 10 000, 50 байт. Середня довжина заголовку HTTP складає 290 байт. Отже, до 300–байтного запиту дописується 20–байтний TCP–заголовок. 20–байтний IP–заголовок плюс 290 байт заголовка HTTP в мережі 1, та 18 байт – у мережі 3. Тобто 300–байтний запит перетворюється у 630–байтовий кадр (= 300 + 20 + 20 + 290) в мережі 1 та 2 і у 648–байтний кадр (= 300 + 20 + 20 + 18+290) у мережі 3.

Час передачі клієнтського запиту складатиме:

$$\frac{630\times8}{10000000} = 0{,}000504,[\text{с}] \tag{3.38}$$

$$\frac{630\times8}{10000000} = 0{,}0000504,[\text{с}] \tag{3.39}$$

$$\frac{648\times8}{10000000} = 0{,}000324,[\text{с}] \tag{3.40}$$

Проведемо аналогічні розрахунки для запиту розміром 10 000 байт та 50 байт. 50–байтний запит перетворюється у 380–байтний в мережі 1 та 2, та в 398–байт в мережі 3.

$$\frac{380\times8}{10000000} = 0{,}000304,[\text{с}] \quad (3.41)$$

$$\frac{380\times8}{10000000} = 0{,}0000304,[\text{с}] \quad (3.42)$$

$$\frac{398\times8}{10000000} = 0{,}000199,[\text{с}] \quad (3.43)$$

Запит розміром 10 000 байт, шляхом додавання заголовків перетвориться у 10330–бітовий в мережах 1 і 2, та у 10348–байтний у мережі 3. Час обслуговування складатиме відповідно:

$$\frac{10330\times8}{10000000} = 0{,}008264,[\text{с}] \quad (3.44)$$

$$\frac{10330\times8}{10000000} = 0{,}0008264,[\text{с}] \quad (3.45)$$

$$\frac{10348\times8}{10000000} = 0{,}005174,[\text{с}] \quad (3.46)$$

На рис. 3.13 показано порівняльну характеристику часу обробки повідомлення запиту розміром 300 байт.

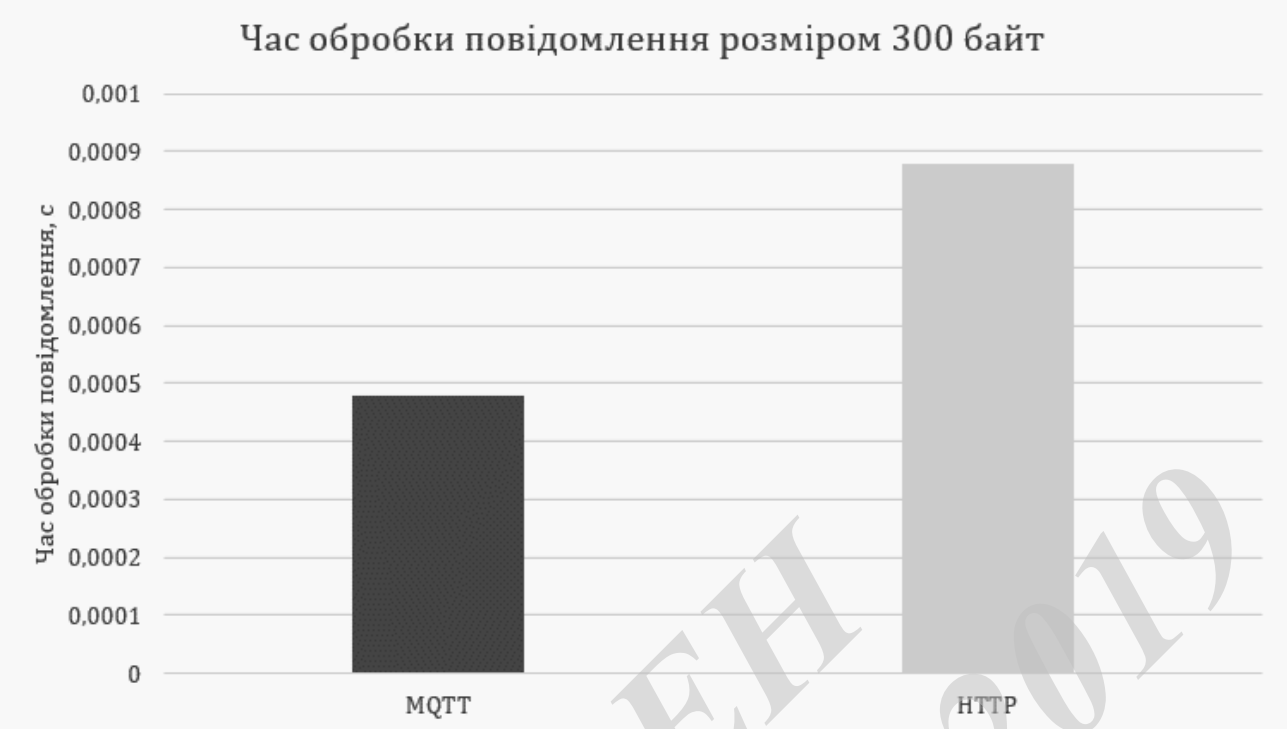


Рисунок 3.13 – Час обробки повідомлення розміром 300 байт

На рис. 3.14 зображено порівняльну характеристику часу обробки повідомлення запиту розміром 10 000 байт.

На рисунку 3.15 зображено порівняльну характеристику часу обробки повідомлення запиту розміром 50 байт.

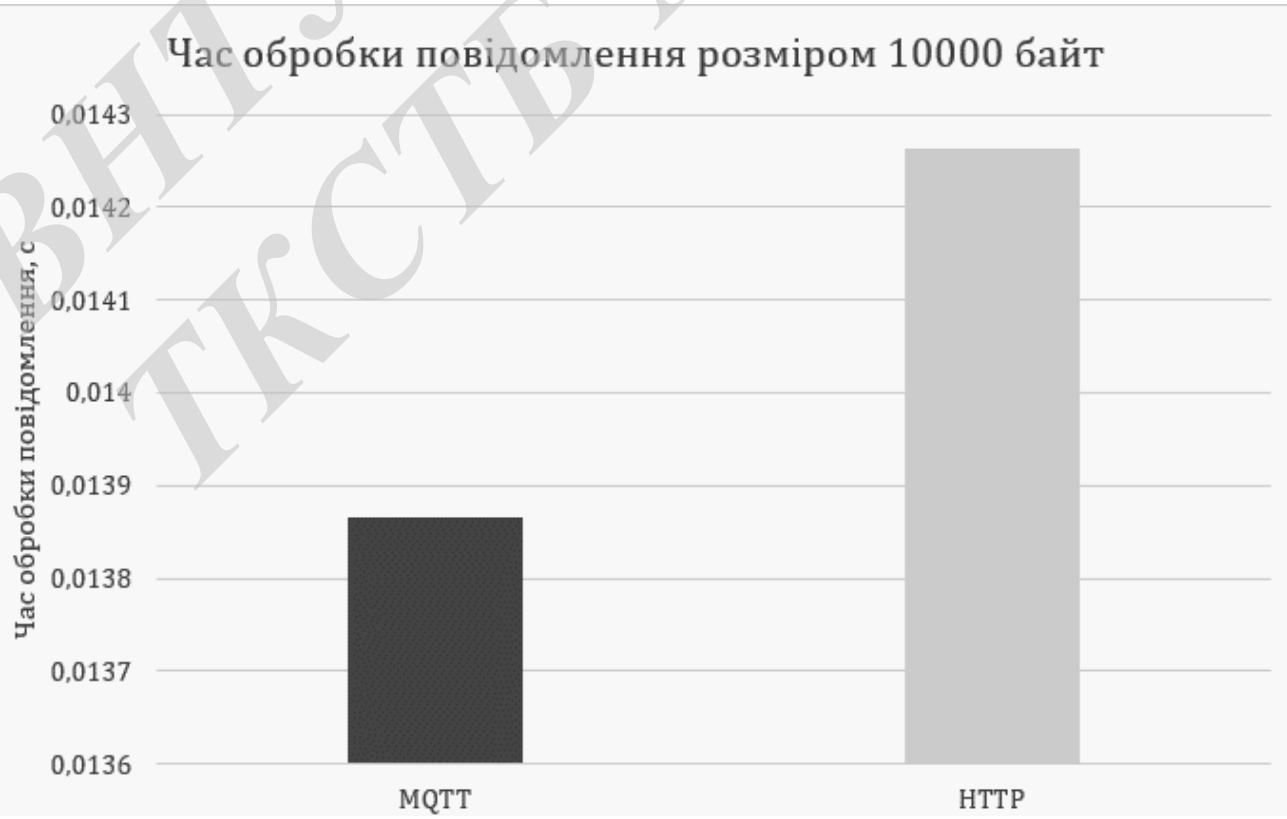


Рисунок 3.14 – Час обробки повідомлення розміром 10 000 байт

Рисунок 3.15 – Час обробки повідомлення розміром 50 байт

У таблиці 3.7 наведено узагальнені результати розрахунків часу обробки запитів.

Таблиця 3.7 – Час обробки запитів

Час обробки запитів			
Розмір повідомлення	Назва мережі	MQTT	HTTP
50 (байт)	ISP1 (10Мбіт / с)	7.36 × 10−5 (с)	30.40 × 10−5 (с)
	ISP2 (100Мбіт / с)	0.0736 × 10−5 (с)	3.04 × 10−5 (с)
	ISP3 (16Мбіт / с)	5.4 × 10−5 (с)	53.34 × 10−5 (с)
300 (байт)	ISP1 (10Мбіт / с)	27.3 × 10−5 (с)	50.40 × 10−5 (с)
	ISP2 (100Мбіт / с)	2.73 × 10−5 (с)	5.04 × 10−5 (с)
	ISP3 (16Мбіт / с)	17.9 × 10−5 (с)	32.40 × 10−5 (с)
10 000 (байт)	ISP1 (10Мбіт / с)	803.3 × 10−5 (с)	826.40 × 10−5 (с)
	ISP2 (100Мбіт / с)	80.33 × 10−5 (с)	82.40 × 10−5 (с)
	ISP3 (16Мбіт /с)	502.9 × 10−5 (с)	517.4 × 10−5 (с)

Тепер розглянемо відповідь сервера клієнту. Нехай після встановлення TCP–з'єднання встановлений MSS (максимальний розмір сегмента), який дорівнює 1 460 байт. Це означає, що серверу необхідно відправити клієнту 7 TCP–сегментів, щоб передати свою 10 000–байтну відповідь. Перші 6 сегментів будуть мати кожен 1 460–байтний блок даних плюс 20–байтний TCP–заголовок. Останній сегмент буде мати блок даних довжиною 1 240 байт (≈ 10 000 – 6 х 1 460). По мірі руху відповіді від сервера до клієнта, до кожного сегменту додадуться ще IP–заголовок і заголовок кадра відповідної мережі.

Розрахуємо час обслуговування для відповіді у мережах 1, 2 і 3. Почнемо з мережі 3, Ethernet. Кожен із перших 6 сегментів згенерує 1518–байтний кадр

(з них 1460 байт буде відведено на дані, 20 байт – TCP–заголовок, 20 байт – на IP–заголовок і 18 байт – на службову інформацію кадра Ethernet).

Останній сегмент згенерує 1298–байтний кадр. Отже, час обслуговування для відповіді у мережі 3 складе:

$$\frac{(6\times1518+1298)\times8}{16000000} = 0{,}005203, [\text{с}]$$

Розмір заголовку кадра і смуга пропускання мережі 1 та 2 відрізняються від відповідних значень для мережі 3. Отже, час обслуговування для відповіді складатиме:

$$\frac{(6\times(1460+20+20+2)+(1240+20+20+2))\times8}{10000000} = 0{,}008235, [\text{с}]$$

$$\frac{(6\times(1460+20+20+2)+(1240+20+20+2)\times8)}{100000000} = 0{,}000823, [\text{с}]$$

$$\frac{(6\times(1460+20+20+18)+(1240+20+20+18)\times8)}{16000000} = 0{,}00337, [\text{с}]$$

Час обслуговування 100 000–байтної відповіді:

$$\frac{(69\times(1460+20+20+2)+(720+20+20+2))\times8}{10000000} = 0{,}08352, \ [\text{с}]$$

$$\frac{(69\times(1460+20+20+2)+(720+20+20+2))\times8}{100000000} = 0{,}008352, [\text{с}]$$

$$\frac{(69\times(1460+20+20+18)+(720+20+20+18)\times8)}{16000000} = 0{,}05276, [\text{с}]$$

Час обслуговування 5 000–байтної відповіді:

$$\frac{(4\times(1460+20+20+2)+(620+20+20+2))\times8}{10000000} = 0{,}005336, [\text{с}]$$

$$\frac{(4\times(1460+20+20+2)+(620+20+20+2))\times8}{100000000} = 0{,}0005336, [\text{с}]$$

$$\frac{(4\times(1460+20+20+18)+(620+20+20+18)\times 8)}{16000000} = 0{,}003375, [\text{с}]$$

Розрахуємо час обслуговування для відповіді в мережах 1, 2 і 3, при використанні протоколу HTTP.

Час обслуговування 10 000–байтної відповіді:

$$\frac{(6\times(1460+20+20+290)+(1240+20+20+290))\times 8}{10000000} = 0{,}010608, [\text{с}]$$

$$\frac{(6\times(1460+20+20+290)+(1240+20+20+290))\times 8}{100000000} = 0{,}001061, [\text{с}]$$

$$\frac{(6\times(1460+20+20+18)+(1240+20+20+18)\times 8)}{16000000} = 0{,}00663, [\text{с}]$$

Час обслуговування 100 000–байтної відповіді:

$$\frac{(69\times(1460+20+20+290)+(720+20+20+290))\times 8}{10000000} = 0{,}100824, [\text{с}]$$

$$\frac{(69\times(1460+20+20+290)+(720+20+20+290))\times 8}{100000000} = 0{,}010082, [\text{с}]$$

$$\frac{(69\times(1460+20+20+308)+(720+20+20+308)\times 8)}{16000000} = 0{,}06315, [\text{с}]$$

Час обслуговування 5 000–байтної відповіді:

$$\frac{(4\times(1460+20+20+7)+(620+20+20+7))\times 8}{10000000} = 0{,}007744, [\text{с}]$$

$$\frac{(4\times(1460+20+20+2)+(620+20+20+2))\times 8}{100000000} = 0{,}000774, [\text{с}]$$

$$\frac{(4\times(1460+20+20+18)+(620+20+20+18)\times 8)}{16000000} = 0{,}00484, [\text{с}]$$

На рис. 3.16. зображено порівняльну характеристику часу обробки повідомлення відповіді розміром 10 000 байт.

На рис. 3.17 зображено порівняльну характеристику часу обробки повідомлення відповіді розміром 100 000 байт.

На рис. 3.18 зображено порівняльну характеристику часу обробки повідомлення відповіді розміром 5000 байт.

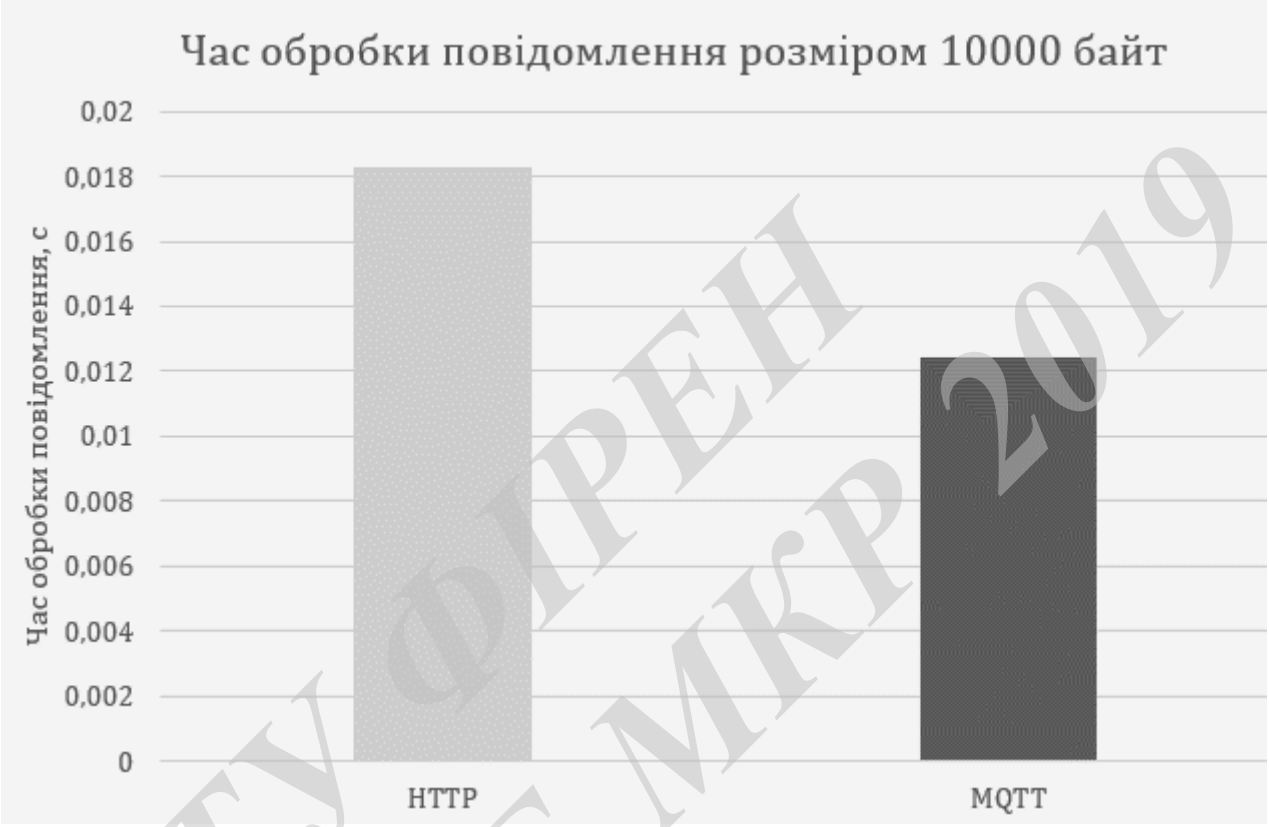


Рисунок 3.16 – Час обробки повідомлення розміром 10 000 байт

Рисунок 3.17 – Час обробки повідомлення розміром 100 000 байт

Рисунок 3.18 – Час обробки повідомлення розміром 5000 байт

Зазначимо, що оскільки MSS менше або дорівнює MTU для усіх мереж, то фрагментувати повідомлення не необхідно. Сучасні IP–стандарти рекомендують хосту джерела повідомлення визначати мінімальне значення MTU по тракту передачі даних до вибору початкового розміру дейтаграми. Це дасть змогу уникати фрагментації з подальшою зборкою повідомлення та прискорює обробку пакетів на проміжних маршрутизаторах і хості місця призначення.

3.8 Висновки до розділу

В 3 розділі було запропоновано методологію розрахунку продуктивності мережі.

Проведено аналіз сервісу IoT, розгорнутого на інфраструктурі AWS Amazon, що може бути реалізованим на транспортному рівні, протоколам MQTT чи HTTP.

AWS IoT забезпечує безпечне двостороннє спілкування між пристроями, підключеними до Internet, такими як датчики, виконавчі пристрої, вбудовані мікроконтролери або інтелектуальні пристрої та Cloud AWS. Це дає змогу збирати телеметричні дані з кількох приладів, а також зберігати та аналізувати їх.

Запропонований метод складається з таких розрахунків:

1) Розрахунок пропускної здатності для 5 типів запитів, та різних розмірів повідомлень. Отримані результати демонструють, що для передачі маленьких повідомлень краще використовувати протокол MQTT. При передачі великих файлів, краще HTTP, бо він не потребує додаткових налаштувань при розгортанні.

2) Середній час відгуку. З отримах результатів, бачимо, що різниці між протоколами майже не існує.

3) Пропускна здатність мережі при використанні кешуючого проксі–сервера. Для протокола MQTT такий сервер не передбачений. Для протокола HTTP виграш в пропускній здатності складає 1,107 Мбіт / с.

4) Розрахунок використання ЦП серверу є важливим пунктом, бо це один з ключових елементів мережі та всієї системи. При використанні протоколу HTTP використання ресурсів ЦП склало 19 %, а при MQTT – 13 %.

5) Під час розрахунку часу обслуговування в мережах, було розраховано час, що витрачався на обробку запитів, для повідомлень розміром 300, 50 та 10 000 байт, для двох протоколів (MQTTі AMQP). Також було розраховано час відповіді для повідомлень розміром 5 000, 10 000 та 100 000 байт відповідно. Отримані результати наведені у таблицях 3.1, та 3.2.

4 ЕКОНОМІЧНА ЧАСТИНА

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

ВИСНОВКИ

1) Розглянуто основні поняття технології «Інтернету речей», IoT (Internet of Things). Інтернет речей складається з чотирьох основних рівнів, таких як: рівень сенсорів і сенсорних мереж, рівень шлюзів і мереж, сервісний рівень, рівень додатків.

2) Досліджено значення цифрового двійника в архітектурі IoT та аналіз його складових блоків. Цифровий двійник складається з набору різних інфокомунікаційних технологій, що забезпечують функціонування Інтернету речей, і його архітектура показує, як ці технології пов'язані один з одним. Зв'язок між фізичним та цифровим світами, який демонструє рис.1 підкреслює глибокий потенціал цифрового двійника: тисячі датчиків, що приймають безперервні, нетривіальні вимірювання, що транслюються на цифрову платформу, яка, у свою чергу, виконує аналіз в режимі реального часу для оптимізації бізнес–процесу.

3) Безпека і стійкість Інтернету речей – це ефективність оцінки ризиків та їх усунення. Безпека в IoT унікальна, тому що луди повинні довіряти технології. Унікальність полягає в тому, що повинна відбуватися ідентифікація, аутентифікація, зберігання та обробка інформації, в тому числі і фінансової. Також повинна забезпечуватись безпека доставки товарів, мультифакторна аутентифікація, автоматична фіксація передачі прав від одного контрагента до другого.

4) Досліджено методи інтеграції технології IoT з блокчейн. Шляхом використання блокчейна, стає можливим здійснювати мікроплатежі за рамками P2P–розрахунків публічного блокчейна. У контрольованій мережі приватного блокчейна, ми впроваджуємо Машинну Валюту для двосторонніх договорів і платежів між елементами цифрового двійника і, тим самим сприяємо більш доступним, надійним і безпечним процесам.

5) Проведено аналіз сервісу IoT, розгорнутого на інфраструктурі AWS Amazon, та розроблено методологію розрахунку продуктивності мережі. Запропонований метод складається з наступних розрахунків:

1. Розрахунок пропускної здатності для 5 типів запитів, та різних розмірів повідомлень. Отримані результати демонструють, що для передачі маленьких повідомлень краще використовувати протокол MQTT. При передачі великих файлів, краще HTTP, бо він не потребує додаткових налаштувань при розгортанні.

2. Середній час відгуку. З отримах результатів, бачимо, що різниці між протоколами майже не існує.

3. Пропускна здатність мережі при використанні кешуючого проксі–сервера. Для протокола MQTT такий сервер не передбачений. Для протокола HTTP виграш в пропускній здатності складає 1,107 Мбіт / с.

4. Розрахунок використання ЦП серверу являється важливим пунктом, бо це один з ключових елементів мережі та всієї системи. При використанні протоколу HTTP використання ресурсів ЦП склало 19%, а при MQTT – 13%.

5. Під час розрахунку часу обслуговування в мережах, було розраховано час, що витрачався на обробку запитів, для повідомлень розміром 300, 50 та 10 000 байт, для двох протоколів (MQTTі AMQP). Також було розраховано час відповіді для повідомлень розміром 5 000, 10 000 та 100 000 байт відповідно.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Виробнича безпека, що її розглядає охорона праці, має велике значення для працюючих тому, що саме вона контролює фізичний стан працівника, що не може не позначитись на його житті, здоров'ї, а також результативності праці в тому числі і у галузі радіоелектроніки.

У даному розділі наводиться аналіз небезпечних, шкідливих [1] та уражаючих для людини та навколишнього середовища факторів, що виникають при проведенні дослідження бездротових мереж стандарту 802.11 для концепції "Інтернет речей". Тут висвітлюються, зокрема, технічні рішення з гігієни праці та виробничої санітарії, визначення попереднє КПО для верхнього природного освітлення, технічні рішення з промислової та пожежної безпеки при проведенні дослідження, безпека в надзвичайних ситуаціях.

5.1 Гігієна праці та виробнича санітарія

5.1.1 Мікроклімат та склад повітря робочої зони

Вибираємо для приміщення для проведення дослідження бездротових мереж стандарту 802.11 для концепції "Інтернет речей", категорію важкості робіт за фізичним навантаженням – легка Іа.

Відповідно до [2] допустимі показники температури, відносної вологості та швидкості руху повітря в робочій зоні для теплого та холодного періодів року приведені у таблиці Х.1 додатку Х.

При опроміненні менше 25% поверхні тіла людини, допустима інтенсивність теплового опромінення сладає 100 Вт/м^2.

Вміст шкідливих речовин в повітрі робочої зони не повинен перевищувати гранично допустимих концентрацій (ГДК) у повітрі робочої зони та підлягає

систематичному контролю для запобігання можливості перевищення ГДК, значення яких для роботи з ЕОМ наведено в таблиці Х.2 додатку Х.

При роботі з ЕОМ джерелом зараження повітря є також іонізація молекул речовин, які знаходяться у повітрі. Рівні позитивних та негативних іонів мають відповідати [4] і наведені в таблиці Х.3 додатку Х.

Для забезпечення необхідних за нормативами показників мікроклімату і складу повітря робочої зони передбачено такі заходи: у приміщенні повинна бути розміщена система опалення для холодного і кондиціонування для теплого періодів року; застосування вентиляції, яка видаляє забруднення або нагріте повітря з приміщення, а також за допомогою неї контролюється швидкість руху повітря і вологість.

5.1.2 Виробниче освітлення

З метою забезпечення гігієнічних раціональних умов на робочих місцях значні вимоги висуваються до кількісних та якісних показників освітлення.

З погляду задач зорової роботи в приміщенні, в якому проводиться робота з дослідження бездротових мереж стандарту 802.11 для концепції "Інтернет речей", відповідно до [3] визначаємо, що вони відповідають IV розряду зорових робіт. Приймаємо контраст об’єкта з фоном – великий, а характеристику фону – середню, яким відповідає підрозряд *г*.

Нормовані значення коефіцієнта природного освітлення (КПО) і мінімальні значення освітленості при штучному освітленні приведені в таблиці Х.4 додатку Х.

Оскільки приміщення розташоване в місті Вінниця (2-га група забезпеченості природним світлом), а вікна розташовані за азимутом 135°, то за таких обставин КЕО визначатиметься за формулою [3, 4]

$$e_N = e_н m_N \ [\%], \qquad (5.1)$$

де $e_н$ – табличне значення КЕО для бокового освітлення, %;

m_N – коефіцієнт світлового клімату;

N – порядковий номер групи забезпеченості природним світлом.

Підставляючи відомі значення одержимо нормовані значення КПО для бокового та суміщеного освітлення:

$$e_{N.б} = 2 \cdot 0{,}85 = 1{,}7\ (\%);$$

$$e_{N.с} = 1{,}2 \cdot 0{,}85 = 1{,}02\ (\%).$$

Для встановлення нормативних значень показників освітлення запропоновано: при недостатньому природному освітлені в світлу пору доби доповнення штучним завдяки використанню газорозрядних ламп з утворенням системи суміщеного освітлення; застосування загального штучного освітлення у темну пору доби.

Розміри приміщення (м): 7 × 5 × 3,3. Освітлення комбіноване симетрично розташованими світловими прорізами у покритті, розміри яких (м): 2,1 × 1,9. Висота від підлоги до підвіконня – 0,8 м. Остіклення подвійне, плетіння металеві. Конфронтуючі будинки відсутні. Кількість світлових прорізів у покритті n = 2.

Оскільки приміщення знаходиться в м. Вінниця (2-га група забезпеченості природним світлом), а світлові пройми орієнтовані за азимутом 135°, то для таких умов КПО буде рівним [2]:

$$e_{N.верх} = e_{н.верх}\, m_N\ [\%]; \qquad (5.2)$$

$$e_{N.верх} = 5 \cdot 0{,}85 = 4{,}25\ (\%).$$

Природне освітлення забезпечується необхідними архітектурно-будівельними рішеннями – положенням світлових пройм в покритті.

Розрахункове значення коефіцієнта природної освітленості визначається за формулою [3]:

$$e_П = \frac{nS_В\tau_З r_1 100}{K_З \eta_В S_П K_{БУД}} \text{ [\%]}, \quad (5.2)$$

де n – кількість світловими прорізами у покритті;

$S_В$, $S_П$ – площа світлового прорізу у покритті та підлоги відповідно, м^2;

$\tau_З$ – загальний коефіцієнт світлопропускання;

r_1 – коефіцієнт, що враховує підвищення КПО при комбінованому освітлені завдяки світлу, яке відбивається від поверхонь приміщень;

$K_З$ – коефіцієнт запасу (для виробничих приміщень $K_З$ = 1,3...1,5);

$\eta_В$ – світлова характеристика світлових прорізів у покритті;

$K_{БУД}$ – коефіцієнт, що враховує затінення вікон будівлями, які розташовані напроти.

Площу кожного світлового прорізу в покритті визначимо за формулою

$$S_В = H_В B_В \text{ [м}^2\text{]}, \quad (5.3)$$

де $H_В$, $B_В$ – висота та ширина світлового прорізу у покритті відповідно, м.

Площа стелі рівна площі підлоги і визначається за формулою

$$S_{стелі} = S_П = L_П B_П \text{ [м}^2\text{]}, \quad (5.4)$$

де $L_П$, $B_П$ – довжина та ширина підлоги відповідно, м.

Визначимо загальний коефіцієнт світлопропускання за формулою:

$$\tau_З = \tau_1\ \tau_2\ \tau_3\ \tau_4\ \tau_5, \quad (5.5)$$

де τ_1 – коефіцієнт світлопропускання матеріалу;

τ_2 – коефіцієнт, що враховує втрати світла у віконній рамі;

τ_3 – коефіцієнт, що враховує втрати світла у несучих конструкціях (при боковому освітленні $\tau_3 = 1$; при верхньому – $\tau_3 = 0{,}8\text{-}0{,}9$);

τ_4 – коефіцієнт, що враховує втрати світла у сонцезахисних пристроях;

τ_5 – коефіцієнт, що враховує втрати світла у захисній сітці, яка встановлюється під ліхтарями (при суміщеному освітленні приймається рівним 0,9; при природному 1).

Для одинарного остіклення вибираємо $\tau_1 = 0{,}9$. Для дерев'яного виду віконних рам $\tau_2 = 0{,}75$. Для верхнього освітлення приймаємо $\tau_3 = 0{,}85$. Оскільки сонцезахисні пристрої не використовуються, то приймаємо $\tau_4 = 1$. Для природного освітлення приймаємо $\tau_5 = 1$.

Після підстановки відомих значень у формули (5.3, …, 5.5) отримаємо

$$S_B = 2{,}1 \cdot 1{,}9 = 4 \text{ (м}^2\text{)};$$

$$S_{стелі} = S_П = 7 \cdot 5 = 35 \text{ (м}^2\text{)};$$

$$\tau_З = 0{,}9 \cdot 0{,}75 \cdot 0{,}85 \cdot 1 \cdot 1 = 0{,}57.$$

Приймаємо коефіцієнт запасу $K_З = 1{,}3...1{,}5 = 1{,}4$.

Для визначення коефіцієнту r_1 необхідно знайти середній коефіцієнт відбиття приміщення за формулою:

$$\rho_{СР} = \frac{\rho_{стелі} S_{стелі} + \rho_{стін} S_{стін} + \rho_П S_П}{S_{стелі} + S_{стін} + S_П}, \qquad (5.6)$$

де $\rho_{стелі}$, $\rho_{стін}$, $\rho_п$ – коефіцієнти відбиття стелі, стін та підлоги відповідно;

$S_{стелі}$, $S_{стін}$, $S_п$ – площа стелі, стін, та підлоги відповідно, м^2.

Приймаємо $\rho_{стелі} = 0{,}725$; $\rho_{стін} = 0{,}7$; $\rho_п = 0{,}25$.

Площу стін визначимо за формулою

$$S_{стін} = H_{стіни}(2L_П + 2B_П)\ [м^2], \qquad (5.7)$$

де $H_{стіни}$ – висота стіни, м.

Після підстановки відомих значень у формули (5.7, 5.6) отримаємо

$$S_{стін} = 3{,}3 \cdot (2 \cdot 7 + 2 \cdot 5) = 79{,}2\ (м^2);$$

$$\rho_{ср} = \frac{0{,}725 \cdot 35 + 0{,}7 \cdot 79{,}2 + 0{,}25 \cdot 35}{35 + 79{,}2 + 35} = 0{,}6003.$$

Для визначення коефіцієнту r_1 необхідно також визначити співвідношення

$$B_п / h;\ l / B_п;\ L_п / B_п, \qquad (5.8)$$

де h – висота від рівня умовної робочої поверхні до верхнього краю світлового прорізу у покритті, м;

l – відстань розрахункової точки до зовнішньої стіни, м.

Знайдемо висоту від рівня умовної робочої поверхні до верхнього краю світлового прорізу у покритті за формулою:

$$h = H_{стіни} - h_р - (H_{стіни} - H_В - h_П) = H_В + h_П - h_р\ [м], \qquad (5.9)$$

де $h_р$ = 0,8 м – висота робочої поверхні.

Розрахункову точку приймаємо на відстані 1 м від стіни, протилежної від світлового прорізу у покритті

$$l = B_п - 1\ [м]. \qquad (5.10)$$

Після підстановки відомих значень у формули (5.10, 5.11) отримаємо

$$l = 5 - 1 = 4 \text{ (м)};$$

$$h = 2{,}1 + 0{,}8 - 0{,}8 = 2{,}1 \text{ (м)}.$$

Таким чином, співвідношення, необхідні для визначення коефіцієнту r_1 дорівнюють $B_n / h = 5 / 2{,}1 = 2{,}38$; $l / B_n = 4 / 5 = 0{,}8$; $L_n / B_n = 7 / 5 = 1{,}4$.

За отриманими значеннями і величиною $\rho_{ср}$ вибираємо коефіцієнт $r_1 = 7{,}86$. Світлову характеристику світлових прорізів у покритті вибираємо за значеннями співвідношень L_n / B_n; B_n / h, для яких $\eta_B = 13{,}8$.

Оскільки конфронтуючі будинки відсутні, то $K_{БУД} = 1$.

Отже, розрахункове значення коефіцієнта природної освітленості становить

$$e_n = \frac{2 \cdot 4 \cdot 0{,}57 \cdot 7{,}86 \cdot 100}{1{,}4 \cdot 13{,}8 \cdot 35 \cdot 1} = 5{,}3 \text{ (\%)}.$$

Оскільки $e_П = 5{,}3$ % > $e_N = 4{,}25$ %, то природна освітленість в даному приміщенні є достатньою.

5.1.3 Виробничі віброакустичні коливання

Зважаючи на те, що при використанні пристроїв крім усього іншого устаткування застосовується обладнання, робота якого супроводжується шумом та вібрацією, необхідно передбачити захист від шуму та вібрації.

Визначено, що приміщення, в якому відбувається робота з дослідження бездротових мереж стандарту 802.11 для концепції "Інтернет речей" може мати робочі місця із шумом та вібрацією, що створюється вентиляторами блоку живлення комп’ютера та кулерами мікропроцесора, відеоадаптера.

З метою запобігання травмуванню працюючих під дією шуму він підлягає нормуванню. Головним нормативом стосовно промислового шуму, діючим на

території нашої країни, є [5], у відповідності з яким допустимі рівні звукового тиску, рівні звуку і еквівалентні рівні шуму на робочих місцях в промислових приміщеннях не повинні перевищувати значень, які приведені в таблиці Х.5 додатку Х. Норми виробничих вібрацій наведені в таблиці Х.6 додатку Х для локальної вібрації.

З метою покращення віброакустичного клімату в приміщенні запропоновано такі заходи: оздоблення стін спеціальними перфорованими плитами, панелями з метою шумопоглинання; передбачено використовувати в приміщені штори із щільної тканини.

5.1.4 Виробничі випромінювання

Величина напруженості електромагнітного поля на робочих місцях з персональними комп'ютерами мають не перевищувати граничнодопустимі, які складають 20 кВ/м. Експозиційна доза рентгенівського випромінювання на відстані 0,05 м від екрана до корпуса монітора при будь-яких положеннях регулювальних пристроїв не повинні перевищувати $7{,}74 \cdot 10^{-12}$ Кл/кг, що відповідає потужності еквівалентної дози 0,1 мБер/год (100 мкР/год) згідно [14].

З метою забезпечення захисту і досягнення нормативних рівнів випромінювань потрібно застосовувати приекранні фільтри, локальні світлофільтри та інші засоби захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат.

5.2 Технічні рішення щодо промислової та пожежної безпеки при проведенні дослідження

Сучасний етап розвитку техніки, автоматизації розробок та досліджень характеризується широким використанням на робочому місці ЕОМ. Наявність

великої кількості прикладних програм сприяє тому, що ЕОМ є основним робочим інструментом інженера в галузі радіотехніки.

5.2.1 Безпека щодо організації робочих місць

Робочі місця з відеодисплейним терміналом зобов'язані розташовуватись на відстані не менше ніж 1,5 м від стіни з віконними прорізами, від інших стін – на відстані 1 м, одне від одного на відстані не менше як 1,5 м. У випадку розміщення робочих місць потрібно виключити можливість прямого засвічування екрану джерелом природного освітлення. Робоче місце доцільно розташовувати таким чином, щоб природне освітлення знаходилось збоку, переважно з лівого [7].

Розташовувати відеодисплейний термінал на робочому місці необхідно так, щоб поверхня екрана повинна знаходитись на віддалі 400-700 мм від очей працівника. Висота робочої поверхні столу при виконанні роботи сидячи повинна налаштовуватись у межах 680-800 мм. Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною не менше як 500 мм, глибиною на рівні колін не менше 450 мм та на рівні витягнутої ноги не менше як 650 мм [8].

5.2.2 Електробезпека

Причинами ураження електричним струмом у даному приміщенні можуть бути: робота під напругою під час проведення ремонтних робіт, несправність устаткування, випадковий дотик до металевих частин, що опинилися під напругою або струмоведучих частин. У відповідності до [9] це приміщення відноситься до приміщень із підвищеною небезпекою ураження електричним струмом через наявність високої (понад 75 %) відносної вологості. Тому безпека експлуатації електрообладнання має забезпечуватись комплексом заходів, що передбачають використання ізоляції струмовідних елементів, захисних блокувань, захисного заземлення та ін [10].

5.2.3 Пожежна безпека

Відповідно до [11] приміщення, в якому проводиться робота з дослідження бездротових мереж стандарту 802.11 для концепції "Інтернет речей", відноситься до категорії пожежної небезпеки Б. Це приміщення відноситься до 2-го ступеня вогнестійкості, в якому приміщення знаходяться в будівлі з несучими та огороджувальними конструкціями з природних або штучних кам’яних матеріалів, бетону, залізобетону із застосуванням листових і плитних негорючих матеріалів.

Мінімальні межі вогнестійкості конструкцій приміщення, що розглядається наведені в таблиці Х.7. В таблиці Х.8 приведено протипожежні норми проектування будівель і споруд.

Вибираємо, що приміщення, де проводиться робота з дослідження, має бути оснащене двома вогнегасниками, пожежним щитом, ємністю з піском [12].

5.3 Безпека у надзвичайних ситуаціях

……..

Висновки до розділу

Під час написання цього розділу було опрацьовано такі питання охорони праці та безпеки в надзвичайних ситуаціях, як технічні рішення з гігієни праці та виробничої санітарії, визначення попереднє КПО для верхнього природного освітлення, технічні рішення з промислової та пожежної безпеки при проведенні дослідження бездротових мереж стандарту 802.11 для концепції "Інтернет речей", безпека у надзвичайних ситуаціях.

Література

1. ГОСТ 12.0.003-74.ССБТ. Опасные и вредные производственные факторы. Классификация.
2. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень.
3. ДБН В.2.5-28-2006. Природне і штучне освітлення.
4. Пособие по расчету и проектированию, естественного, искусственного и совмещенного освещения НИИСФ – М.: Стройиздат. 1985. – 384 с.
5. ДСН 3.3.6-037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку.
6. ДСН 3.3.6.039-99. Державні санітарні норми виробничої та загальної вібрацій.
7. ГОСТ 12.2.032-78. ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования.
8. Методичні вказівки до опрацювання розділу "Охорона праці та безпека в надзвичайних ситуаціях" в дипломних проектах і роботах студентів спеціальностей, що пов’язані з функціональною електронікою, автоматизацією та управлінням / Уклад. О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2012. – 64 с.
9. ДНАОП 0.00-1.21-98 Правила безпечної експлуатації електроустановок споживачів. – К. : Держнаглядохоронпраці, 1998. – 382 с.
10. ДБН В.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд.
11. ДБН В.1.1.7-2002. Пожежна безпека об’єктів будівництва.
12. НАПБ Б.03.001-2004. Типові норми належності вогнегасників.
13. СНиП 2.09.02-85. Противопожарные нормы проектирования зданий и сооружений.
14. Норми радіаційної безпеки України (НРБУ-97), МОЗ України. – К., 1997.

Додаток Х

Нормовані значення виробничих факторів

Таблиця Х.1 – Допустимі показники мікроклімату

Період року	Категорія робіт	Температура повітря, °С для робочих місць		Відносна вологість повітря, %	Швидкість руху повітря, м/с
		постійних	непостійних		
Холодний	Іа	21-25	18-26	75	≤0,1
Теплий		22-28	20-30	55 при 28°С	0,1-0,2

Таблиця Х.2 – ГДК шкідливих речовин [4]

Назва речовини	ГДК, мг/м^3	Агрегатний стан	Клас небезпеки
Озон	0,1	Пара	4
Оксиди азоту	5	Пара	2
Пил	4	Аерозоль	2

Таблиця Х.3 – Число іонів в 1 см^3 повітря приміщення під час роботи на ЕОМ

Рівні	Мінімально необхідні	Оптимальні	Максимально допустимі
позитивний	400	1500-3000	50000
негативний	600	3000-5000	50000

Таблиця Х.4 – Нормативні значення коефіцієнта природного освітлення і мінімальні освітленості для штучного освітлення

Характеристика зорової роботи	Найменший розмір об'єкта розрізнення, мм	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фону	Штучне освітлення, лк		Природне освітлення (верхнє), КПО, %	Природне освітлення (бокове), КПО, %	Суміщене освітлення (бокове), КПО, %
						При комбінованому освітленні	При загальному освітленні			
Високої точності	0,3-0,5	III	г	великий	середній	400	200	5	2	1,2

Таблиця Х.5 – Допустимі рівні шуму та еквівалентні рівні звуку

Рівні звукового тиску в дБ в октавних полосах із середньо-геометричними частотами, Гц									Рівні звуку і еквівалентні рівні звуку, дБА
31,5	63	125	250	500	1000	2000	4000	8000	
86	71	61	54	49	45	42	40	38	50

Таблиця Х.6 – Нормовані рівні віброприскорення [6]

Гранично допустимі рівні віброприскорення, дБ, в октавних полосах із середньо-геометричними частотами, Гц								Коректовані рівні віброприскорення, дБА
8	16	31,5	63	125	250	500	1000	
73	73	79	85	91	97	103	109	76

Таблиця Х.7 – Мінімальні межі вогнестійкості приміщення [11]

Ступінь вогнестійкості будівлі	Стіни				Колони	Східчасті майданчики	Плити та інші несучі конструкції	Елементи покриття	
	Несучі та східчасті клітки	Самонесучі	Зовнішні несучі	Перегородки				Плити, прогони	Балки, ферми
2	REI 120 М0	REI 60 М0	E 15 М0	EI 15 М0	R 120 М0	R 60 М0	REI 45 М0	REI 15 М0	R 30 М0

Примітка. R – втрати несучої здатності; E – втрати цілісності; I – втрати теплоізолювальної спроможності; M – показник здатності будівельної конструкції поширювати вогонь (межа поширення вогню); M0 – межа поширення вогню дорівнює 0 см.

Таблиця Х.8 – Протипожежні норми проектування будівель і споруд [13]

Об’єм приміщення, тис. м	Категорія пожежної небезпеки	Ступінь вогнестійкості	Відстань, м, для щільності людського потоку в загальному проході, осіб/м^2			Кількість людей на 1 м ширини евакуаційного виходу	Протипожежні розриви, м, для ступеня їх вогнестійкості			Найбільша кількість поверхів	Площа поверху в межах пожежного відсіку, м^2, для кількості поверхів		
			до 1	2-3	4-5		I,II	III	IV,V		1	2	3 і більше
до 15	Б	2	40	25	15	45	9	9	12	6	н.о.	–	–

Примітки: н.о. – не обмежується.

5.3 Безпека у надзвичайних ситуаціях. Дослідження стійкості роботи бездротової мережі в умовах дії загрозливих чинників НС

У елементній базі радіоелектронної апаратури (РЕА) під дією іонізуючих випромінювань ймовірна зміна ледве не всіх електричних і експлуатаційних характеристик, що залежить від протікання процесів іонізації та порушення структури матеріалів.

Під час електромагнітного імпульсу можуть спостерігатись високі імпульси струмів і напруг в провідниках та кабелях зв'язку, електропередач, систем обчислювальних машин та автоматичних систем управління, антенах радіостанцій тощо.

5.3.1 Дослідження стійкості роботи бездротової мережі в умовах дії іонізуючих випромінювань

Початкові дані: рівень радіації через 1 год після аварії P_{1max} = 5,43 Р/год; максимальне значення часу, протягом якого повинна працювати апаратура t_{pmax} = 5000 год; коефіцієнт ослаблення радіації $K_{осл}$ = 1; час початку опромінення t_n = 1 год.

За критерій стійкості роботи приймаємо максимальне значення експозиційної дози, при якому РЕА бездротової мережі буде працювати з потрібною якістю протягом часу напрацювання на відмову.

Дослідження стійкості роботи проводимо в такій послідовності:

Проводимо аналіз приладу і визначаємо радіоелектронні елементи елементи, від яких залежить його функціонування.

Визначаємо граничні значення експозиційних доз, при яких в елементах можуть виникнути зворотні зміни, але елемент ще буде працювати. Дані заносимо в табл. 5.1.

Таблиця 5.1 – Максимально допустимі експозиційні дози елементів РЕА

№	Елементи РЕА пристрою	$Д_{зв.і}$, Р	$Д_{зв}$, Р
1	Діоди 1N4004	10^5	10^4
2	Резистори МЛТ	10^6	
3	Конденсатори СР-13.020	10^6	
4	Транзистори 2SA1271	10^4	
5	Мікросхеми TPIC6B595	10^5	

За мінімальним значенням $Д_{зв.і}$ визначаємо границю стійкості роботи РЕА бездротової мережі в цілому. Це значення заносимо в табл. 5.1.

Граничне значення дози:

$$Д_{гр} = Д_{зв} \cdot К_{осл} \text{ [Р]}; \quad (5.9)$$

$$Д_{гр} = 10^4 \cdot 1 = 1 \cdot 10^4 \text{ (Р)}.$$

Можлива доза опромінення елементної бази в заданих умовах складає

$$Д_М = \frac{2P_{1max}(\sqrt{t_к} - \sqrt{t_п})}{К_{осл}} \text{ [Р]}; \quad (5.10)$$

$$Д_м = \frac{2 \cdot 5{,}43 \cdot (\sqrt{5000} - \sqrt{1})}{1} = 757{,}06 \text{ (Р)}.$$

Оскільки $Д_м$ = 757,06 Р < $Д_{гр}$ = 1 · 10^4 Р, то апаратура бездротової мережі працюватиме протягом потрібного гарантійного часу стійко із заданим рівнем надійності.

5.3.2 Дослідження стійкості роботи бездротової мережі в умовах дії електромагнітного імпульсу

Початкові дані: $E_В$ = 10,93 кВ/м; $U_ж$ = 12 ± 5% В; $l_Г$ = 0,45 м; $l_В$ = 0,22 м.

За критерій стійкості роботи РЕА в цих умовах приймаємо коефіцієнт безпеки:

$$K_в = 20\lg\frac{U_д}{U_{в(г)}} \geq 40 \text{ [дБ]}, \quad (5.11)$$

де $U_д$ – допустимі коливання $U_ж$;

$U_{в(г)}$ – напруга наведення в вертикальних (горизонтальних) струмопровідних частинах.

Визначаємо горизонтальну складову напруженості електромагнітного поля за формулою

$$E_г = 10^{-3} E_в \text{ [кВ/м]}, \quad (5.12)$$

де $E_В$ – вертикальна складова напруженості електромагнітного поля, кВ/м.

Визначаємо вертикальну та горизонтальну напруги наведення на струмопровідних частинах РЕА за формулами:

$$U_в = E_г l_в \text{ [В]}; \quad (5.13)$$

$$U_г = E_в l_г \text{ [В]}, \quad (5.14)$$

де $l_в$, $l_г$ – довжини вертикальної та горизонтальної струмопровідних частин РЕА відповідно, м.

Розраховуємо допустиме коливання напруги живлення:

$$U_д = U_ж + \frac{U_ж}{100} N \text{ [В]}, \quad (5.15)$$

де $U_{ж}$ – робоча напруга живлення, В;

N – допустимі коливання напруги, %.

Підставляючи відомі значення у формули (5.12, …, 5.15, 5.11) одержимо

$$E_{г} = 10^{-3} \cdot 10{,}93 = 0{,}01093 \text{ (кВ/м)};$$

$$U_{в} = 0{,}01093 \cdot 1000 \cdot 0{,}22 = 2{,}4046 \text{ (В)};$$

$$U_{г} = 10{,}93 \cdot 1000 \cdot 0{,}45 = 4918{,}5 \text{ (В)};$$

$$U_{д} = 12 + \frac{12}{100} \cdot 5 = 12{,}6 \text{ (В)};$$

$$K_{бв} = 20\lg\frac{12{,}6}{2{,}4046} = 13{,}3 \text{ (дБ)};$$

$$K_{бг} = 20\lg\frac{12{,}6}{4918{,}5} = -53{,}8 \text{ (дБ)}.$$

Так як ($K_{бв}$ = 13,3 дБ) < ($K_{бном}$ = 40 дБ) і ($K_{бг}$ = -53,8 дБ) < ($K_{бном}$ = 40 дБ), то робота бездротової мережі є нестійкою до дії електромагнітного імпульсу.

5.3.3 Розробка превентивних заходів по підвищенню стійкості роботи бездротової мережі в умовах дії НС

Найбільш ефективним способом підвищення збільшення стійкості роботи РЕА є екранування системи або її елементів. З цією метою проводиться розрахунок екрану. Розраховуємо перехідне затухання енергії електричного поля стальним екраном:

$$A = K_{бном} - K_{бмін} \text{ [дБ]}; \qquad (5.16)$$

$$A = 40 - (-53{,}8) = 93{,}8 \text{ (дБ)},$$

де $K_{бном}$ – номінальний коефіцієнт безпеки ($K_{бном}$ = 40 дБ);

$K_{бмін}$ – мінімальний розрахунковий коефіцієнт безпеки.

Товщину захисного екрану знаходимо за формулою:

$$t = \frac{A}{k\sqrt{f}} \text{ [см];} \qquad (5.17)$$

$$t = \frac{93,8}{5,2 \cdot \sqrt{15000}} = 0,147 \text{ (см)} = 1,47 \text{ (мм)},$$

де k – коефіцієнт, який для стального екрана дорівнює 5,2;

f – найбільш характерна частота (f = 15000 Гц).

Підвищення стійкості роботи бездротової мережі можна досягти через посилення найбільш слабких елементів і ділянок системи, а також завчасним проведенням комплексу інженерно-технічних, технологічних та організаційних заходів, що спрямовані на максимальне зменшення дії уражаючих чинників і створення умов для відновлення працездатності пристрою.

Висновки: Таким чином в даному розділі нами було розглянуто такі питання охорони праці, як технічні рішення з гігієни праці та виробничої санітарії, технічні рішення з промислової та пожежної безпеки.

Також, в цьому підрозділі нами було досліджено стійкість роботи бездротової мережі в умовах дії загрозливих чинників надзвичайних ситуацій. Із дослідження дії електромагнітного імпульсу на стійкість роботи бездротової мережі можна зробити висновок, що система РЕА виявилася нестійкою в роботі. Використання екранування РЕА значно збільшує її стійкість в умовах впливу електромагнітного імпульсу.

СПИСОК ЛІТЕРАТУРИ

1. Інтернет Речей. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Інтернет_речей

2. Росляков А. В. ІНТЕРНЕТ РЕЧЕЙ: Навчальний посібник / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. Самара: ПГУТИ, 2015. 136 с.

3. D. Evans, “The Internet of things: How the next evolution of the Internet is changing everything,” CISCO, San Jose, CA, USA, White Paper, 2011.

4. L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

5. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future Internet: The Internet of Things architecture, possible applications and key challenges,” inProc. 10th Int. Conf. FIT, 2012, pp. 257–260.

6. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

7. P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, “Survey of Internet of Things technologies for clinical environments,” in Proc. 27th Int. Conf. WAINA, 2013, pp. 1349–1354.

8. D. Yang, F. Liu, and Y. Liang, “A survey of the Internet of Things,” in Proc. 1st ICEBI, 2010, pp. 358–366.

9. Industry 4.0 and the digital twin/ 2017. URL: https://www2.deloitte.com/insights/us/en/focus/industry–4–0/digital–twin–technology–smart–factory.html#endnote–11

10. J. Gantz and D. Reinsel, “The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east,” IDC iView: IDC Anal. Future, vol. 2007, pp. 1–16, Dec. 2012.

11. Васильков А. Микрокомпьютеры для интернета вещей: от умного дома к поумневшему окружению / А. Васильков / Компьютерра, 14 июня 2013 г.

12. Вишневский В. Mesh–сети стандарта IEEE 802.11s. технологи и реализация / В. Вишневский, Д. Лаконцев, А. Сафонов, С. Шпилев / Первая миля. 2008. № 2–3. С. 26–31.

13. Восков Л. С. Web вещей – новый этап развития интернета вещей / Л. С. Восков, Н. А. Пилипенко / Качество. Инновации. Образование. 2013. № 2. С. 44–49.

14. Гайкович Г. Ф. Стандартизация в области промышленных сетей. Развитие беспроводных стандартов для АСУ ТП / Г. Ф. Гайкович / Электронные компоненты. 2009. № 1. С. 48–53.

15. Гиббс М. Интернет вещей – не только для «умных» / М. Гиббс / Сети / network world. 2013. № 3.

16. Архитектура безопасности "Интернета вещей". 2018. URL: https://docs.microsoft.com/ru–ru/azure/iot–suite/iot–security–architecture

17. Эталонная архитектура безопасности интернета вещей (IoT). URL: https://www.anti–malware.ru/practice/solutions/iot–the–reference–security–architecture–part–1

18. Доктор Гринспен Гидеон, «Приватный мультиблокчейн – Технический документ» Coin Sciences, http://www.multichain.com/download/MultiChain–White–Paper.pdf, (2014).

19. AWS IoT Button URL: https://aws.amazon.com/ru/iotbutton/

20. V. A. F. Almeida, D. A. Menasc.e, R. Riedi, F. P. Ribeiro, R. Fonseca, and W. Meira Jr., "Analyzing Web Robots and their Impact on Caching," Proc. Sixth

Workshop on WebCa ching and Content Distribution, Boston, Massachusetts, June 20–22, 2001.

21. V. A. F. Almeida, D. A. Menasce, R. Riedi, F. P. Ribeiro, R. Fonseca, and W. Meira Jr., "Characterizing and Modeling Robot Workload on E–Business. Sites," Proc. 2001 ACM SIGMETRICS Conf. Measurement Comput. Syst., ACM, Boston, Massachusetts, June 16–20, 2001.

22. V .A. F. Almeida, A. Bestavros, M. Crovella, and A. Oliveira, "Characterizing Reference Locality in the WWW," Fourth Int. Conf. Parallel Distrib. Inform. Syst. (PDIS), IEEE Comput. Soc, Dec. 1996, Miami Beach, Florida, pp. 92–103.

23. J. M. Almeida, V. A. F. Almeida, and D. Yates, "Measuring the Behavior of a World–Wide Web Server," Proc. Seventh Conf. High Perform. Networking (HPN), IFIP, Apr. 1997, pp. 57–72.

24. M. Arlitt and C. Williamson, "Web Server Workload Characterization: the Search for Invariants," Proc. 1996 ACM SIGMETRICS Conf. Measurement Comput. Syst., Philadelphia, Pennsylvania, May 1996, pp. 126–137.

25. T. Berners–Lee, R. Cailliau, H. Nielsen, and A. Pecret, "The World Wide Web," Comm. ACM, vol. 37, no. 8, pp. 76–82, Aug. 1994.

Додаток А

(обов’язковий)

ВНТУ

ЗАТВЕРДЖУЮ

Зав.кафедри ТКСТБ ВНТУ,

канд. техн. наук, професор

Г.Г.Бортник

. “__” _____ 2019 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

МЕТОДИ ПОБУДОВИ БЕЗПРОВІДНИХ МЕРЕЖ СТАНДАРТУ 802.11 ДЛЯ КОНЦЕПЦІЇ "ІНТЕРНЕТ РЕЧЕЙ"

08-34.МКР.001.00.000 ТЗ

Керівник роботи

к.т.н., доц. кафедри ТКСТБ ВНТУ

Михалевський Д. В.

Виконавець: ст. гр. ТТК-18м

Бондарев М. В.

Вінниця-2019

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “02” 10 2019 року № 254 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 02.09.2019 р.

Дата закінчення: 18.12.2019 р.

2 МЕТА І ПРИЗНАЧЕННЯ МКР

Метою даної магістерської кваліфікаційної роботи є аналіз методів побудови безпровідних мереж стандарту 802.11 для концепції "інтернет речей".

Задачами магістерської кваліфікаційної роботи є:

- розробка технічного завдання;
- аналіз параметрів стандарту 802.11 wi–fi;
- оцінка параметрів безпровідного каналу;
- опис системи та розрахунок пропускної здатності;
- розрахунок продуктивності мережі

Об’єкт дослідження є пропускна здатність каналів у безпровідних мережах стандарту 802.11

Предмет дослідження є методи побудови безпровідних мереж стандарту 802.11 для концепції "інтернет речей".

Основними завданнями роботи є:

- техніко-економічне обґрунтування доцільності даної розробки;
- аналіз параметрів стандарту 802.11 wi–fi;
- оцінка параметрів безпровідного каналу;
- аналіз пропускної здатності мережі;
- аналіз економічної ефективності проведеної розробки;

- дослідження питань безпеки життєдіяльності.

Розроблений в ході виконання метод побудови мережі IP дозволить розв'язати допустимий потік повідомлень для оптимальної пропускної здатності в мережі IP на основі стандарту IEEE 802.11.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Робота базується на дисертації аналізу IoT «Аналіз архітектури побудови мереж для реалізації концепції Internet of Things», яка виконувалась у КПІ у 2017-2018 н. р. Під час підготовки магістерської кваліфікаційної роботи будуть використані матеріали цієї роботи.

Список використаних джерел розробки:

3.1 Михалевський Д. В. Оцінка параметрів безпровідного каналу передачі інформації стандарту 802.11 wi-fi. «Информационно-управляющие системы» 2014 – 5с.

3.2 ---------

3.3 ----------

3.4

3.5 Положення про кваліфікаційну роботу у Вінницькому національному технічному університеті / Уклад. О. Н. Романюк, Р. Р. Обертюх, Т. О. Савчук, Л. П. Громова – Вінниця : ВНТУ, 2015 – 27 с.

3.6 Кухарчук В.В., Ігнатенко О.Г., Обертюх Р.Р. Методичні вказівки до оформлення дипломних проектів (робіт) для студентів всіх спеціальностей.- В.: ВДТУ, 2002.

3.7 Козловський В.О. Техніко-економічні обгрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – В.: ВДТУ, 2003.

3.8 ДСТУ 3008-2015. Інформація та документація, звіти у сфері науки і техніки.- К.: ДП «УкрНДНЦ», 2016.

3.9 Разработка и оформление конструкторской документации радиоэлектронной аппаратуры. Справочник. Под ред. Э.Т.Романычевой.- М: Радио и связь, 1989.

3.10 Бортник Г.Г., Васильківський М.В. Методичні вказівки до підготовки магістерських кваліфікаційних робіт для студентів спеціальності «Телекомунікації та радіотехніка» усіх форм навчання - Вінниця:ВНТУ, 2018.- 50 с.

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра телекомунікаційних систем та телебачення, студент групи ТТК-18м Бондарев М. В.

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати дослідження методів побудови безпровідних мереж стандарту 802.11 для концепції "інтернет речей"

Технічні вимоги, яким повинна відповідати розробка, наступні:

- стандарт мережі IEEE 802.11 wi-fi;
- діапазон частот 2,4 ГГц;
- пропускна здатність 11 000 кбіт/сек;
- кількість можливих варіантів потоку повідомлень 10

При розробці ІКМ слід максимально використовувати стандартні та уніфіковані деталі.

6 ЕТАПИ МКР І ТЕРМІНИ ЇХ ВИКОНАННЯ

№	Назва та зміст етапу	Термін виконання		Очікувані результати	Звітна документ-тація
		початок	закінчення		
1.	Розробка технічного завдання (ТЗ)	02.09.2019р.	06.09.2019р.	Розроблене ТЗ	Додаток А
2.	Техніко-економічне обґрунтування розробки (ТЕО)	09.09.2019р.	13.09.2019р.	Розроблене ТЕО	Вступ. Розділ 1.
3.	Аналіз параметрів стандарту 802.11 wi–fi	16.09.2019р.	04.10.2019р.	Проведений аналіз	Розділ 2
4.	Оцінка параметрів безпровідного каналу; опис системи та розрахунок пропускної здатності	07.10.2019р	25.10.2019р.	Розроблений метод	Розділ 3
6.	Аналіз економічної ефективності	11.11.2019р.	15.11.2019р.	Економічна частина МКР	Розділ 4
7.	Охорона праці та безпека в надзвичайних ситуаціях	18.11.2019р.	22.11.2019р.	Частина ОТ та БНС	Розділ 5
8.	Оформлення пояснювальної записки (ПЗ) та графічної частини	25.11.2019р.	29.11.2019р.	Оформлена документація	ПЗ та графічна частина
9.	Нормоконтроль, попередній захист, рецензування МКР	02.12. 2019р.	06.12.2019р.	Позитивні відзиви	Відзив. Рецензія
10.	Захист МКР ЕК		18.12. 2019р.	Позитивний захист	Протокол ЕК

7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть досліджені:

- структура IoT;
- пропускна здатність мережі;
- економічна частина МКР;
- розділ ОП та БНС;

Результати, отримані в процесі виконання даної роботи, будуть впроваджені в галузі телекомунікацій:

- Регіональний Центр експлуатації телекомунікаційної мережі України шляхом впровадження широкосмугового ІКМ;

- ПАТ "Укртелеком" шляхом впровадження нових методик контролю характеристик ІКМ.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується підвищення точності та розширення частотного діапазону ІКМ.

8 МАТЕРІАЛИ, ЯКІ ПОДАЮТЬ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ ТА ПІД ЧАС ЕТАПІВ

За результатами виконання МКР до ЕК подаються пояснювальна записка, графічна частина МКР, відгук і рецензія.

9 ПОРЯДОК ПРИЙМАННЯ МКР ТА ЇЇ ЕТАПІВ

Поетапно результати виконання МКР розглядаються керівником роботи та обговорюються на засіданні кафедри.

Захист магістерської кваліфікаційної роботи відбувається на відкритому засіданні ЕК.

10 ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

Документація, що розробляється в процесі виконання досліджень повинна містити:

- техніко-економічне обґрунтування розробки;

- аналіз параметрів стандарту 802.11 wi–fi;
- опис системи та розрахунок пропускної здатності;
- розрахунок продуктивності мережі
- економічну частину та розділ БЖД і ЦЗ;
- рекомендації щодо подальшого використання результатів.

11 ВИМОГИ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У зв’язку з тим, що інформація не є конфіденційною, заходи з її технічного захисту не передбачаються.

Додадки

Додаток А

(обов’язковий)

Сфери застосування технології IP

Додаток Б

(обов’язковий)

Структура безпровідного каналу Wi–Fi

Додаток В

(обов’язковий)

Архітектурна будова AWS IoT

Додаток Г

(обов’язковий)

Сфери застосування технології IP

Додаток Д

(обов’язковий)

Стек протоколу BlueTooth та пікомережі

Додаток Е

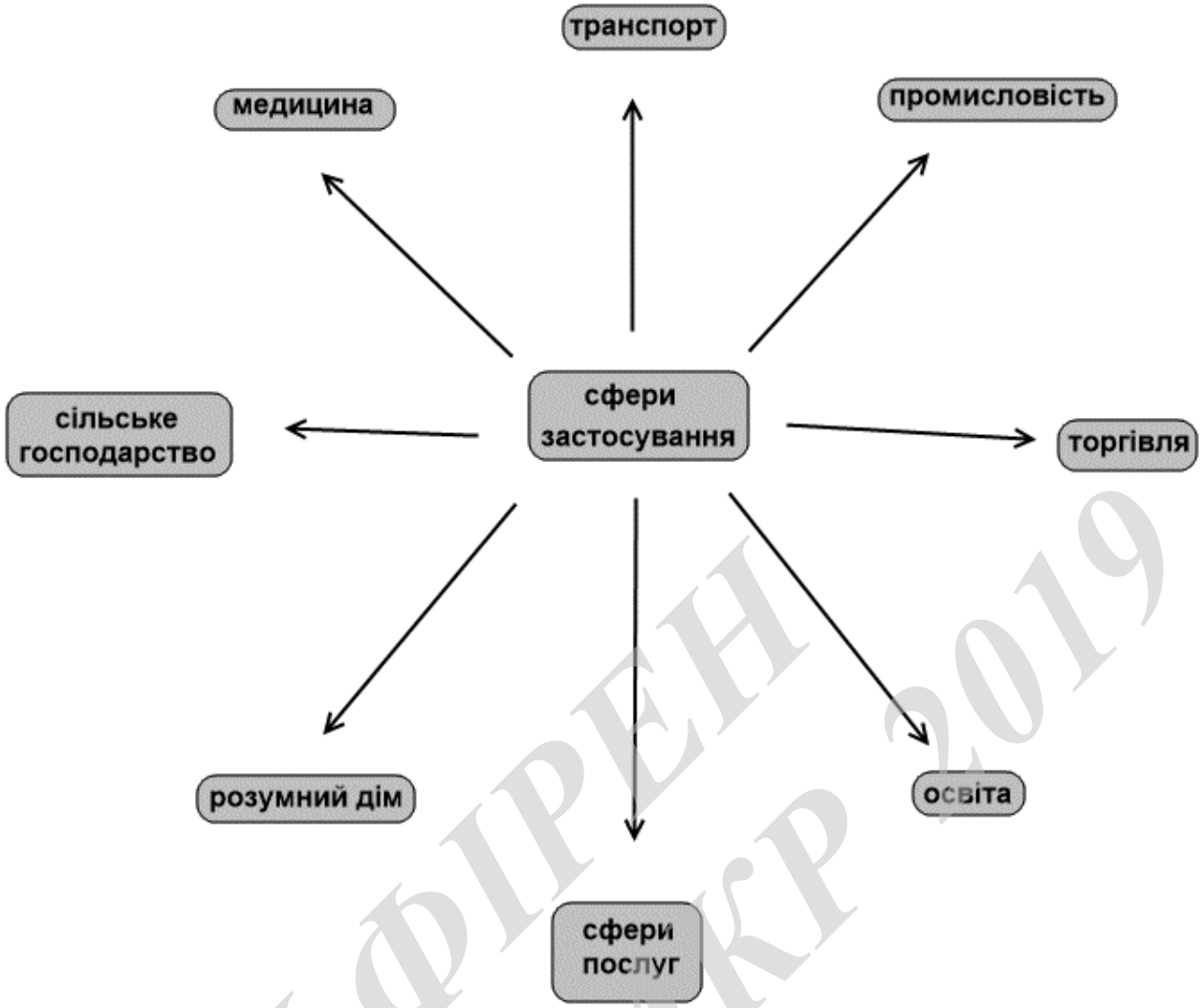
(обов’язковий)

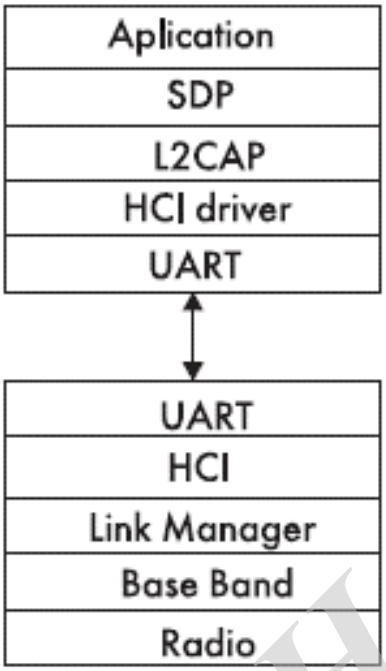
Взаємодія між клієнтом та сервером

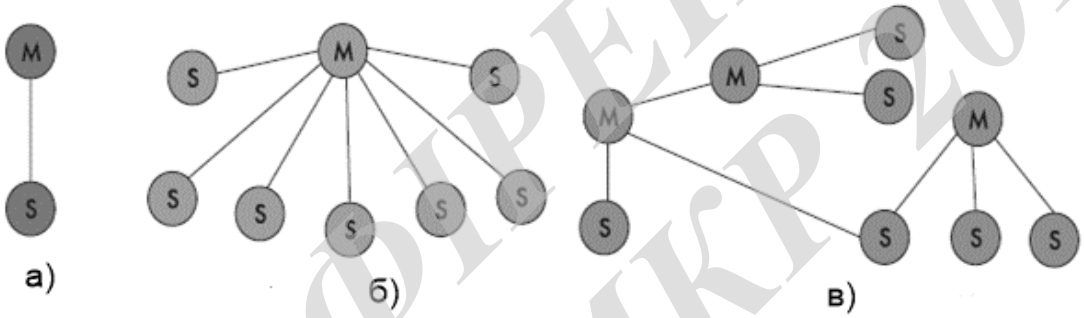
Додаток Ж

(обов’язковий)

Відношення загальної пропускної здатності







а) б) в)