НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий Інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«До захисту допущено»
ВО завідувача кафедри
_____ Галина СОЗОННИК
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Аналіз стандартів 3GPP для рішень Інтернету речей»

Виконав (-ла):
студент (-ка) IV курсу, групи ТС-01
Тисак Валентина Вікторівна _____

Керівник:
Доцент кафедри ЕКІР, к.т.н.
Осипчук С.О. _____

Рецензент:
Доцент кафедри ТК НН ІТС, к.т.н., с.н.с.,
Міночкін Д. А. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та інтернету речей»

ЗАТВЕРДЖУЮ
ВО завідувача кафедри
_____ Галина СОЗОННИК
«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Тисак Валентина Вікторівна

1. Тема роботи «Аналіз стандартів 3GPP для рішень Інтернету речей», керівник роботи Осипчук Сергій Олександрович, доцент кафедри ЕКІР, затверджені наказом по університету від «22» травня 2024 р. № 2064-С

2. Термін подання студентом роботи: «14» червня 2024 р.

3. Вихідні дані до роботи

Стандарти 3GPP для рішень Інтернету речей.

Виклики 3GPP для Інтернету речей.

Еволюція технологій IoT.

4. Зміст роботи

Аналіз технологій передавання інформації 3gpp для IoT.

Завдання розвитку і покращення технологій 3gpp.

Розробка і реалізація лабораторної роботи на основі пристроїв зв’язку 3GPP для рішень IoT.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Презентація з наведеними результатами аналізу, в обсязі 11 слайдів (актуальність та мета дослідження, аналіз технологій передавання інформації 3GPP для IoT, аналіз поточних викликів та проблем 3GPP для IoT, огляд сучасних напрямків та інновацій у вдосконаленні 3GPP для IoT, огляд провайдерів і мереж IoT в Україні з використанням стандартів та технологій 3GPP, технічний аналіз модуля зв’язку NB-IoT/Cat-M/EDGE/GPRS/GNSS на SIM7000E до Raspberry Pi, процес налаштування модуля зв'язку SIM7000E NB-IoT HAT до Raspberry Pi, апробація результатів дослідження, висновки).

6. Дата видачі завдання «28» листопада 2023 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної області	08.04.2024-12.04.2024	Виконано
2	Складання плану дипломної роботи	18.04.2024-21.04.2024	Виконано
3	Аналіз джерел на тему дипломної роботи	22.04.2024-17.05.2024	Виконано
4	Детальний аналіз технологій передавання інформації 3GPP для IoT	18.05.2024-22.05.2024	Виконано
5	Написання 1-го розділу дипломної роботи	22.05.2024-23.05.2024	Виконано
6	Дослідження поточних викликів та завдань розвитку і покращення технологій 3GPP	24.05.2024-26.05.2024	Виконано
7	Написання 2-го розділу дипломної роботи	27.05.2024-28.05.2024	Виконано
8	Аналіз джерел інформації для подальшої розробки лабораторної роботи	28.05.2024-29.05.2024	Виконано
9	Написання 3-го розділу дипломної роботи	29.05.2024-02.06.2024	Виконано
10	Оформлення пояснювальної записки	03.06.2024-07.06.2024	Виконано

Студент Валентина ТИСАК

Керівник роботи Сергій ОСИПЧУК

РЕФЕРАТ

Текстова частина дипломної роботи: 72 сторінки, 15 рисунків, 8 таблиць, 23 джерела, та 1 додаток.

Актуальність роботи. У сучасному світі Інтернет речей (IoT) стрімко входить у різні сфери життя, від промисловості до побуту, змінюючи традиційні підходи до збору та обробки даних. Стандарти 3GPP відіграють ключову роль у цьому процесі, надаючи необхідні специфікації для забезпечення надійного та безпечного зв'язку між пристроями IoT. Розробка та оптимізація цих стандартів є актуальною задачею, що вимагає глибокого аналізу та розуміння поточних тенденцій та викликів.

Метою роботи є розробка лабораторного протоколу для налаштування і дослідження рішення IoT на основі модуля зв'язку 3GPP SIM7000E з технологіями передавання даних NB-IoT, Cat-M, EDGE, GPRS, GNSS, та мікроконтролера Raspberry Pi.

Об'єкт дослідження – стандарти та технології 3GPP для побудови рішень IoT.

Предмет дослідження – дослідження і налаштування рішень IoT на основі модуля зв'язку 3GPP SIM7000E та мікроконтролера Raspberry Pi.

3GPP, ІНТЕРНЕТ РЕЧЕЙ, LTE-M, NB-IoT, EC-GSM-IoT, ТЕХНОЛОГІЇ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ.

ABSTRACT

The thesis contains: 72 pages, 15 figures, 8 tables, 23 sources and 1 appendix.

Relevance of the work. In the modern world, the Internet of Things (IoT) is rapidly entering various spheres of life, from industry to domestic use, changing traditional approaches to data collection and processing. 3GPP standards play a key role in this process, providing the necessary specifications to ensure reliable and secure communication between IoT devices. The development and optimization of these standards is a relevant task that requires deep analysis and understanding of current trends and challenges.

The purpose of the work is to develop a laboratory protocol for setting up and studying IoT solutions based on the 3GPP SIM7000E communication module with data transmission technologies NB-IoT, Cat-M, EDGE, GPRS, GNSS, and the Raspberry Pi microcontroller.

The object of research – 3GPP standards and technologies for building IoT solutions.

The subject of research – study and configuration of IoT solutions based on the 3GPP SIM7000E communication module and the Raspberry Pi microcontroller.

3GPP, INTERNET OF THINGS, LTE-M, NB-IoT, EC-GSM-IoT, INFORMATION TRANSMISSION TECHNOLOGIES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

3GPP	Third Generation Partnership Project
ARIB	Association of Radio Industries and Businesses
ATIS	Alliance for Telecommunications Industry Solutions
CCSA	China Communications Standards Association
ETSI	European Telecommunications Standards Institute
TSDSI	Telecommunications Standards Development Society, India
TTA	Telecommunications Technology Association
TTC	Telecommunication Technology Committee
IoT	Internet of Things
LTE-M	Long-Term Evolution Machine Type Communication
NB-IoT	Narrowband Internet of Things
EC-GSM-IoT	Extended Coverage GSM for the Internet of Things
eMTC	enhanced Machine Type Communication
LPWAN	Low Power Wide Area Network
eGPRS	enhanced General Packet Radio Service
MNO	Mobile Network Operator
MBB	Mobile Broadband
5G	Fifth Generation
5GC	5G Core
5G EPC	5G Evolved Packet Core
NR	New Radio
TDD	Time Division Duplexing
SA	Standalone
URLLC	Ultra-Reliable Low Latency Communications
TSN	Time-Sensitive Networking
EEL	Edge Enabler Layer
EEC	Edge Enabler Client
EES	Edge Enabler Server

ECS	Edge Configuration Server
API	Application Programming Interface
UE	User Equipment
LBO	Local BreakOut
HR	Home Routed
OPG	Operator Platform Group
SA6 WG	Service and System Aspects Working Group 6
PLMN	Public Land Mobile Network
V-PLMN	Visited Public Land Mobile Network
HPLMN	Home Public Land Mobile Network
GSMA	Global System for Mobile Communications Association
ENS	Edge Node Sharing
ECSP	Edge Computing Service Provider
MWC	Mobile World Congress
SAE	System Architecture Evolution
LTE	Long-Term Evolution
SBI	Service-Based Interface
SEPP	Security Edge Protection Proxy
SS7	Signaling System No. 7
AKA	Authentication and Key Agreement
EAP	Extensible Authentication Protocol
SMF	Session Management Function
DN-AAA	Data Network-Authentication, Authorization, and Accounting
NAS	Non-Access Stratum
AMF	Access and Mobility Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
DNN	Data Network Name
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
UDR	Unified Data Repository

AUSF	Authentication Server Function
ARPF	Authentication Repository and Processing Function
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
ME	Mobile Equipment
DU	Distributed Unit
CU	Central Unit
gNB	Next Generation Node B
N3IWF	Non-3GPP Interworking Function
SEAF	Security Anchor Function
AI	Artificial Intelligence
ML	Meta Language
WLAN	Wireless Local Area Network
NAI	Network Access Identifier
V-SMF	Відвідувач Session Management Function
H-SMF	Домашній Session Management Function
IPX	Internetwork Packet Exchange
mMTC	Massive Machine-Type Communications
VR	Virtual Reality
AR	Augmented Reality

ВСТУП

Сучасний світ вже важко уявити без Інтернету речей, він охоплює різні сфери нашого життя, від промисловості до домашнього використання.

Стандарти 3GPP, які включають в себе ряд технологій для підключення IoT пристроїв до мобільних мереж, відіграють ключову роль у цьому контексті. Вони дозволяють пристроям різних виробників взаємодіяти між собою, що є важливим для розвитку IoT.

З розвитком IoT та збільшенням кількості пристроїв, які потребують підключення до мережі, значимість стандартів 3GPP стрімко зростає. Вони впливають на різні аспекти IoT, включаючи ефективність, надійність та безпеку комунікацій. Однак, окрім усіх переваг, які надає IoT, перед розробниками з'являється ряд викликів та складностей, які потребують вирішення.

Метою дипломної роботи є розробка лабораторного протоколу для налаштування і дослідження рішення IoT на основі модуля зв'язку 3GPP SIM7000E з технологіями передавання даних NB-IoT, Cat-M, EDGE, GPRS, GNSS, та мікроконтролера Raspberry Pi. А також проведення детального аналізу стандартів 3GPP для рішень Інтернету речей, з акцентом на оцінку їх впливу на розвиток та інтеграцію IoT-технологій. Робота спрямована на вивчення історії та еволюції 3GPP, огляду ключових стандартів, та аналізу їх ролі у стільниковому зв'язку для IoT. Дослідження також охоплює виклики та завдання, пов'язані з розвитком та оптимізацією цих технологій, включаючи безпеку, енергоспоживання та масштабування мережі, а також розглядає сучасні напрямки та інновації.

1 АНАЛІЗ ТЕХНОЛОГІЙ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ 3GPP ДЛЯ IOT

1.1 Історія розвитку 3GPP

Історія розвитку 3GPP (3rd Generation Partnership Project) є невід'ємною частиною сучасного світу інтернету речей. Об'єднуючи сім організацій з розробки стандартів телекомунікацій (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), відомих як "організаційні партнери", 3GPP створює стабільне середовище для своїх членів, де вони можуть виробляти звіти та специфікації, які визначають технології 3GPP.

«The Third Generation Partnership Project (3GPP) - це колаборація між організаціями зі стандартизації телекомунікацій для розробки специфікацій технологій мобільного зв'язку» [1]. «У рамках 3GPP існують різні технічні специфікації, які охоплюють різні аспекти мобільного зв'язку, включаючи Інтернет речей (IoT)» [1].

Специфікації, розроблені 3GPP, є фундаментом для стандартів Інтернету речей (IoT). Вони відіграють ключову роль у визначенні технологій, що лежать в основі IoT, та відкривають широкі можливості для різноманітних IoT-рішень. Ці специфікації дозволяють реалізувати найрізноманітніші сценарії використання IoT, включаючи розумні міста, промисловий Інтернет речей, розумні будинки та багато іншого. Вони відкривають двері до світу, де мільярди пристроїв можуть спілкуватися та взаємодіяти один з одним, створюючи безліч нових можливостей.

1.2 Огляд стандартів 3GPP для IoT: LTE-M NB-IoT, EC-GSM-IoT

Стандарти 3GPP для IoT, включаючи LTE-M, NB-IoT та EC-GSM-IoT, відкривають нові можливості для розвитку Інтернету речей. Вони надають широкий спектр можливостей для підключення пристроїв та служб, від простих до складних, від низькопотужних до високопродуктивних. Ці стандарти відіграють ключову роль у формуванні майбутнього IoT, відкриваючи нові горизонти для інновацій та технологічного прогресу. Завдяки їх гнучкості та

адаптивності, вони можуть задовольнити потреби широкого спектра застосувань IoT, від промислових до споживчих. Завдяки цим стандартам, ми можемо очікувати більш зв’язане та інтелектуальне майбутнє для IoT.

Специфікації 3GPP IoT були розроблені для того, аби задовольнити конкретні вимоги пристроїв IoT, які часто мають інші потреби для спілкування порівняно з традиційними мобільними пристроями. Стандарти 3GPP IoT були розроблені з урахуванням унікальних характеристик пристроїв IoT. Однією з ключових особливостей є низьке енергоспоживання, як правило, пристрої IoT працюють від батареї і повинні забезпечувати тривалу автономну роботу без необхідності частої її заміни. Щодо обміну даними, багато IoT-додатків передбачають нерегулярну передачу невеликих обсягів даних, тому швидкість передачі даних часто є невеликою. Що стосується покриття, пристрої IoT можуть бути розташовані в складних або віддалених місцях, тому вони вимагають кращого покриття, ніж традиційні мобільні пристрої. Специфікації 3GPP IoT визначають набір протоколів, які включають фізичний рівень для опису характеристик середовища бездротової передачі, рівень каналу даних для опису процесу упаковки даних і передачі через фізичний рівень мережі, мережевий рівень для адресації, маршрутизації та пересилання пакетів даних, а також рівень програми, який визначає взаємодію між програмами [1].

Безпека є важливим елементом в IoT, і стандарти 3GPP IoT не лише визнають це, але й включають в себе різні функції для забезпечення конфіденційності, цілісності та автентичності даних, які обмінюються між пристроями та мережами. Це означає, що вони надають захист від несанкціонованого доступу та зловмисного використання даних, що є критично важливим для забезпечення надійності та довіри до систем IoT [1].

3GPP, пропонує ряд унікальних технологій, включаючи LTE-M, NB-IoT та EC-GSM-IoT. Кожна з цих технологій має свої особливості, що робить їх відмінно підходящими для різних застосувань в рамках IoT. Давайте детальніше розглянемо кожну з цих технологій.

Long-Term Evolution Machine Type Communication (LTE-M, або LTE-MTC), є типом малопотужної технології радіозв'язку глобальної мережі. Ця технологія розроблена 3GPP для міжмашинного зв'язку та Інтернету речей (IoT). LTE-M включає eMTC (enhanced Machine Type Communication, «розширений зв'язок машинного типу»), також відома як LTE Cat-M1 [2]. eMTC підтримує високу швидкість передачі даних до 1 Мбіт/с, що робить його ідеальним для застосувань IoT, яким потрібна висока пропускна здатність. Він також може співіснувати з іншими службами LTE в межах однієї смуги пропускання, що робить його гнучким рішенням для розгортання в різних мережевих умовах.

Narrowband Internet of things, (NB-IoT), є стандартом радіотехнології глобальної мережі малої потужності (LPWAN), який був розроблений 3GPP, для забезпечення широкого спектру стільникових послуг [3]. Ця специфікація була заморожена у версії 13 3GPP, відомої як LTE Advanced Pro, у червні 2016 року. NB-IoT зосереджується на покритті всередині приміщень, низькій вартості, тривалому терміні служби батареї та високій щільності з'єднання. Цей стандарт використовує підмножину стандарту LTE, однак обмежує пропускну здатність однією вузькою смугою 200 кГц [3]. NB-IoT відрізняється своєю здатністю до роботи в трьох різних режимах: автономному, в охоронній смузі та внутрішньосмуговому. Це робить NB-IoT надзвичайно гнучким для різних сценаріїв розгортання. Крім того, NB-IoT має ще нижчу вартість пристрою, ніж eMTC, що робить його більш доступним для масового розгортання.

Extended coverage GSM IoT (EC-GSM-IoT) - це технологія широкого діапазону з низьким споживанням енергії, стандартизована 3GPP для використання в ліцензованому спектрі. EC-GSM-IoT, яка базується на eGPRS, розроблена як стільникова система з високою пропускною здатністю, великим радіусом дії, низьким споживанням енергії та низькою складністю для підтримки Інтернету речей (IoT). EC-GSM-IoT, у свою чергу, пропонує розширене покриття з максимальними втратами зв'язку 164 дБ, що робить його ідеальним для застосувань IoT в складних умовах покриття. Він також підтримує велику

кількість пристроїв, приблизно 50 000 на комірку, що робить його відмінним вибором для масового розгортання IoT-пристроїв [4].

На Таблиці 1 представлені детальні характеристики стандартів, включаючи eMTC (LTE Cat M1), NB-IoT та EC-GSM-IoT. Ця таблиця надає глибокий аналіз кожного стандарту, враховуючи такі параметри, як зона покриття, швидкість передачі даних, ширина смуги радіочастот та інші технічні характеристики.

Таблиця 1.1 – Технічні характеристики стандартів: eMTC (LTE Cat M1), NB-IOT та EC-GSM-IoT [5]

	eMTC (LTE Cat M1)	NB-IOT	EC-GSM-IoT
Розгортання	У межах LTE	У межах та за межами LTE, автономний	У межах GSM
Зона покриття*	155.7 дБ	164 дБ для автономного, FFS для інших	164 дБ, з потужністю 33 дБм 4 дБ, з потужністю 23 дБм
Завантаження	OFDMA, інтервал тона 15 кГц, Турбо-код, 16 QAM, 1 Rx	OFDMA, інтервал тона 15 кГц, TBCC, 1 Rx	TDMA/FDMA, GMSK та 8PSK (опціонально), 1 Rx
Відвантаження	SC-FDMA, інтервал тона 15 кГц, Турбо-код, 16 QAM	Однотонове, інтервали тона 15 кГц та 3.75 кГц	TDMA/FDMA, GMSK nf 8PSK (опціонально)
Ширина смуги	1,08 МГц	180 кГц © 3GPP 2012	200кГц на канал. Типова система пропускна здатність 2.4МГц [менше пропускна здатність до 600 кГц вивчали в межах Rel-13]
Пікова швидкість (DL/UL)	1 Мбіт/с для DL та UL	DL: ~250 кбіт/с UL: ~250 для багатотонового, ~20 кбіт/с для однотонового	Для DL та UL (з використанням 4 часових слотів): ~70 кбіт/с (GMSK), ~240 кбіт/с (8PSK)
Дуплексування	FD та HD (тип B), FDD та TDD	HD (тип B), FDD	HD, FDD
Енергозбереження	PSM, зовн. I-DRX, C-DRX	PSM, зовн. I-DRX, C-DRX	PSM, зовн. I-DRX
Клас енергоспоживання	23 дБм, 20 дБм	23 дБм, решта TBD	33 дБм, 23 дБм

1.3 Стільниковий зв’язок для IoT

Сучасні глобальні мережі, що базуються на стандартах 3GPP, забезпечують взаємозв’язок між пристроями та людьми, перетинаючи кордони. Різні сектори економіки, такі як домашня електроніка, автомобільна індустрія, залізничний транспорт, гірнича промисловість, комунальні послуги, медицина, аграрний сектор, виробництво та логістика, вже використовують переваги стільникового IoT. У 2020 році, кількість стільникових IoT-підключень перевищила 1 мільярд, а компанія Ericsson очікує, що до 2025 року ця цифра зросте до 5 мільярдів [6]. З появою 5G, більшість індустрій розглядають можливості стільникового зв’язку для радикальної зміни своїх бізнес-моделей. У деяких регіонах держава стимулює розвиток IoT, надаючи різні пільги для підтримки сталого розвитку, інновацій та економічного зростання.

Оператори мобільного зв’язку (MNO), які вже мають успіх у сфері мобільного широкосмугового доступу (MBB), також мають унікальну можливість створювати нові цінності в сегменті IoT, використовуючи свої регіональні та глобальні ресурси. В той же час, IoT вимагає значно більшої різноманітності у використанні, ніж MBB. Для того, щоб максимально використати інвестиції, операторам необхідно постійно оновлювати стільникові мережі, щоб відповідати зростаючим потребам IoT у широкому спектрі індустрій [6].

Щодо бездротового з’єднання, існують чотири основні категорії вимог, які можна виділити у різних секторах. Ericsson розробила чотири ключові сегменти IoT-підключень: Massive IoT, Broadband IoT, Critical IoT та Industrial Automation IoT. Кожен з цих сегментів відповідає на потреби численних сценаріїв використання в різних галузях.

Сучасні 4G мережі обслуговують Massive IoT за допомогою технологій Cat-M та NB-IoT, а також Broadband IoT через LTE. З розвитком 5G, Massive IoT з Cat-M/NB-IoT стає ще доступнішим, а Broadband IoT отримує нові можливості завдяки 5G радіо та мережевим інноваціям. 5G мережі, з їх високою надійністю та мінімальними затримками, відкривають двері для Critical IoT, який вимагає

надзвичайно точного та своєчасного зв’язку. Щоб інтегрувати 5G мережі з промисловими Ethernet-базованими комунікаційними системами, 3GPP розробив стандарти для додаткових функцій, які полегшать підключення для Industrial Automation IoT.

Підключення Massive IoT орієнтовано на з’єднання великої кількості доступних пристроїв з обмеженою пропускною спроможністю, які зазвичай рідко здійснюють передачу або отримання даних. Ці пристрої часто встановлюються у місцях зі складними умовами для радіозв’язку, де потрібне високоякісне покриття, і частіше за все вони живляться виключно від акумулятора [6].

Технології LTE-M та NB-IoT співіснують з LTE в мережах 4G з 2017 року і задовольняють стандарти 5G, встановлені ITU та 3GPP для широкомасштабного машинного зв’язку [6]. LTE-M адаптує LTE для машинного зв’язку, надаючи підтримку для простих у використанні пристроїв, відомих як Cat-M. NB-IoT є самостійною технологією радіодоступу, яка базується на стандартах LTE. У 2020 році, понад 120 комерційних мереж по всьому світу підтримували NB-IoT та Cat-M, обслуговуючи мільйони користувачів [6]. Очікується, що до 2025 року кількість підключень перевищить 2,5 мільярда. Комерційні застосування охоплюють широкий спектр пристроїв, таких як лічильники, сенсори та трекери, які використовуються у багатьох секторах, включаючи комунальні послуги, автомобілебудування, транспорт, логістику, сільське господарство, виробництво, охорону здоров’я, складське господарство та гірничодобувну промисловість.

«На ринку представлені два основних типи модемів Cat-M/NB-IoT: одномодові модеми NB-IoT, які ідеально підходять для дуже дешевих пристроїв, та двомодові модеми Cat-M1/NB-IoT, які можуть бути використані у більш широкому спектрі застосувань з недорогими пристроями» [6]. Двомодовий модем об’єднує переваги обох технологій, забезпечуючи оптимальну пропускну спроможність, покриття, мобільність, голосову підтримку та точність позиціонування.

Дворежимні пристрої зазвичай використовують режим Cat-M1 у зоні покриття Cat-M1 і можуть перемикатися на доступ NB-IoT, коли знаходяться поза

зоною покриття Cat-M1. Cat-M1 має два режими розширення покриття (CE) у стандарті 3GPP: обов'язковий режим CE A (до 10 дБ CE) і додатковий режим CE B (до 20 дБ CE, нарівні з NB-IoT) [6]. Коли використовується режим CE B, переваги Cat-M1 у продуктивності знижуються через основний компроміс між покриттям та пропускною спроможністю. Режим CE B вимагає значного використання спектральних ресурсів. Враховуючи, що дворежимний модем може переключатися на NB-IoT і використовувати захищені діапазони NB-IoT у ситуаціях з дуже слабким покриттям, комерційна вигода від використання режиму CE B відсутня.

Cat-M1 та NB-IoT сприяють поступовій еволюції до мереж 5G, завдяки динамічному спільному використанню спектру, дворежимний 5G Cloud Core та неперервній стандартизації в рамках 3GPP. NR розширюється на нові частотні діапазони 5G, а також на існуючі частотні діапазони 4G, де функціонують Cat-M1, NB-IoT та LTE. Завдяки динамічному спільному використанню спектру, всі ці технології ефективно співіснують, як це зображено на рисунку 1.1. [6].

Дворежимний 5G Cloud Core складається з 5GC та 5G EPC. Існуючі та нові Cat-M1/NB-IoT пристрої можуть підключатися до 5G EPC. У 3GPP Rel-16 також передбачена можливість підключення пристроїв Cat-M/NB-IoT, сумісних з Rel-16, до 5GC, проте це може бути складним для ринку Massive IoT, що чутливий до витрат, через збільшену складність і розподіл ринку [6].

В свою чергу, Broadband IoT використовує можливості MBB для IoT, надаючи значно вищі швидкості передачі даних і менші затримки порівняно з Massive IoT, а також пропонуючи додаткові функції для IoT, такі як збільшений час роботи від батареї, розширене покриття, покращену швидкість передачі даних у висхідному напрямку та більш точне визначення місцезнаходження пристроїв.

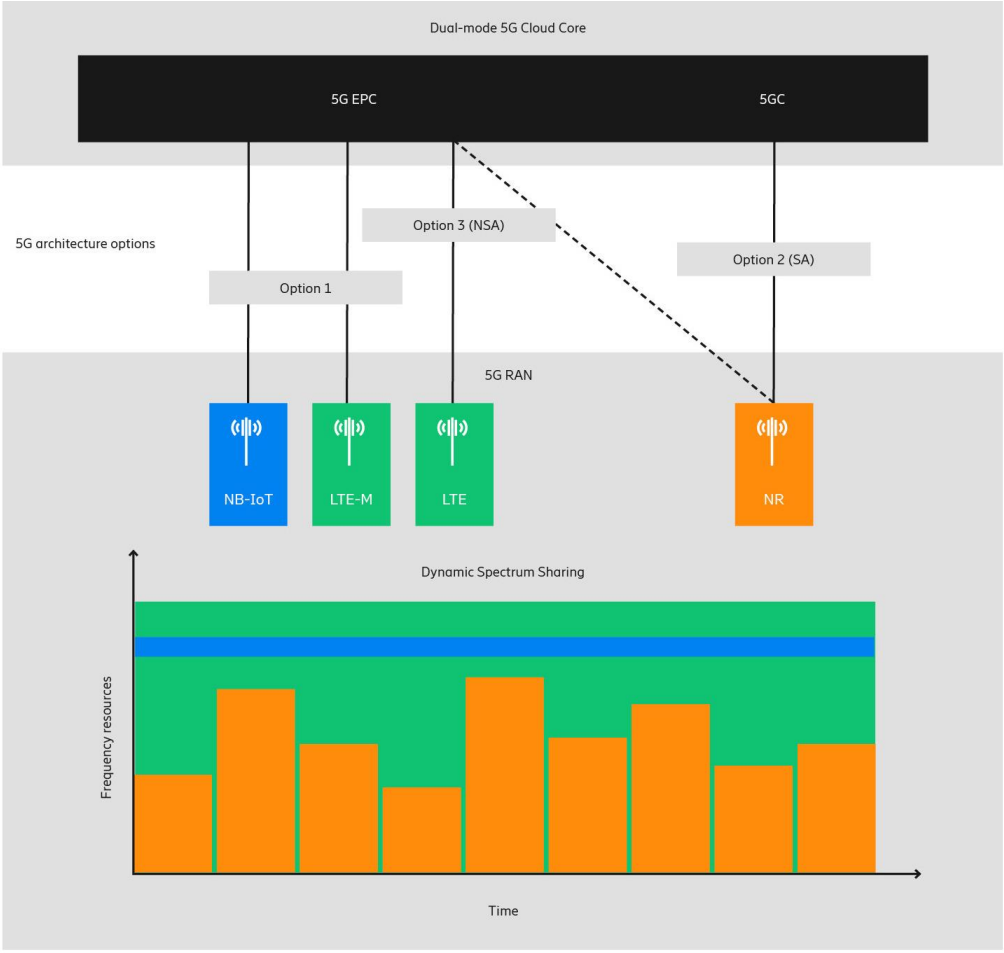

Рисунок 1.1 – Технології доступу різних сфер IoT [6]

У LTE існує багато категорій пристроїв (LTE Cat-1 і вище) з великою пропускною спроможністю, які підходять для широкого спектру застосувань. LTE забезпечує швидкість передачі даних до Гбіт/с і затримку RAN (максимальних зусиль) близько 10 мс (час проходження в обидва боки). З введенням 5G NR у старих і нових спектрах, Broadband Інтернет речей налаштований на досягнення швидкостей десятків Гбіт/с. Покриття однієї базової станції може бути розширене, якщо послабити вимоги до швидкості передачі даних і затримки, наприклад, пристрій LTE може динамічно перемикатися між LTE і LTE-M в залежності від покриття. Термін служби батареї пристрою може бути значно збільшений завдяки використанню особливостей трафіку користувача. Точність визначення місцезнаходження пристроїв у мережі може бути покращена за допомогою NR, оскільки точність зазвичай залежить від ширини смуги пропускання сигналу, а NR може працювати у значно ширшій смузі, ніж LTE [6].

При використанні методології розробки через тестування (TDD), пропускна спроможність висхідного та низхідного напрямків залежить від конфігурації TDD. Зазвичай мобільні оператори повинні домовлятися про загальну статичну конфігурацію TDD, щоб уникнути перешкод. Сучасні конфігурації TDD часто оптимізовані для низхідних каналів зв'язку для використання MBB. Однак, зі зростанням використання IoT у висхідному напрямку, мобільним операторам може знадобитися переглянути угоди щодо TDD, щоб знайти оптимальний баланс між пропускною спроможністю висхідного та низхідного напрямків і низькою затримкою. Автономна 5G (SA) (варіант 2 на рисунку 1.1.) є довгостроковою цільовою архітектурою та ідеальним вибором для сценаріїв із потребами у локалізованому покритті, таких як локальні промислові розгортання, у короткостроковій перспективі з точки зору продуктивності та складності. Для розширення можливостей використання NR, 3GPP Rel-17 планує впровадити підтримку менш складних модемів з функціями енергозбереження, працюючи над NR пристроями з обмеженими можливостями [6].

Critical IoT був розроблений для time-critical communication. Воно гарантує доставку даних в рамках встановлених граничних затримок. Цей тип з'єднання використовує передові можливості 5G для забезпечення високої надійності та низької затримки з різними швидкостями передачі даних. Надійність у цьому контексті означає ймовірність успішної доставки даних протягом заданого часового інтервалу. На відміну від Broadband IoT, який пропонує низьку затримку на рівні "найкращих зусиль", Critical IoT здатен доставляти дані з гарантованими рівнями затримки навіть у перевантажених мережах.

Для того, аби задовольнити вимоги Critical IoT, можливо, доведеться підвищити стандарти затримки та надійності для всіх компонентів, включаючи мережі, пристрої та додатки. Загальна наскрізна затримка в мережі складається з суми окремих затримок, що виникають на рівні радіо, транспорту та базової мережі, і загальна надійність не може перевищувати надійність найслабшої ланки в цьому ланцюгу. Critical IoT може вимагати значних ресурсів спектру для досягнення високої надійності та низької затримки. NR працює на ширшому

діапазоні частот з більшою пропускною спроможністю та більшими можливостями порівняно з LTE, що робить NR ідеальною технологією для таких застосувань. LTE може не отримати подібних покращень для Critical IoT через ряд причин, включаючи обмеження комерційного використання, постійне розширення можливостей NR URLLC в рамках 3GPP, прогрес NR та можливість оновлення програмного забезпечення на існуючих LTE сайтах до NR (використовуючи LTE спектральні діапазони) [6].

Оператори мобільного зв'язку, які володіють гнучким спектром, мають унікальні можливості для надання покриття Critical IoT. Це стосується не тільки масштабних розгортань, але й локальних промислових застосувань. Технологія NR дозволяє використовувати URLLC у всіх частотних діапазонах 5G, як FDD, так і TDD. Приклади комбінацій спектральних діапазонів разом з ключовими характеристиками, такими як пропускна здатність URLLC та охоплення, демонструють можливості для широкого кола користувачів, а також для локальних потреб. Оскільки смуга пропускання на частотах нижче 1 ГГц є обмеженою, її рекомендується використовувати для найважливіших глобальних користувачів. Використання TDD може призводити до затримок в RAN, які залежать від шаблонів передачі TDD, і це особливо важливо на частотах нижче 6 ГГц.

Industrial Automation IoT прагне до безперешкодної інтеграції мобільного зв'язку в існуючу провідну промислову інфраструктуру, яка вже використовується для складної автоматизації в реальному часі. Він включає можливості для інтеграції систем 5G з Ethernet реального часу та Time-Sensitive Networking (TSN), які є ключовими для мереж промислової автоматизації.

Мобільний зв'язок надає значні переваги у мобільності, гнучкості, зниженні витрат та цифровізації порівняно з традиційними провідними з'єднаннями. У деяких випадках, промислові системи можуть переходити від провідних до бездротових мереж поступово, залежно від потреб окремих компонентів системи. Навіть у зоні покриття 5G, деякі елементи можуть залишатися підключеними через кабель через специфічні вимоги, такі як висока продуктивність, яка

перевищує поточні можливості 5G, або через довгий життєвий цикл обладнання. Тому важливо, щоб 5G підтримувала інтеграцію з існуючою провідною інфраструктурою, яка продовжує розвиватися [6].

Різні промислові сектори, такі як гірничодобувна промисловість, комунальні послуги, будівництво, порти та нафтогазовий сектор, використовують провідні мережі для розширеної автоматизації. Існує кілька промислових Ethernet рішень, таких як PROFINET, EtherCAT, Sercos, EtherNet/IP, Powerlink і Modbus, які підтримують детермінований зв’язок для автоматизації в реальному часі. 3GPP стандартизував підтримку Ethernet сеансів у Rel-15 і ввів стиснення заголовків Ethernet у Rel-16 для підвищення спектральної ефективності. Надійна доставка даних з гарантованими затримками забезпечується за допомогою 5G URLLC, який підтримується критичним IoT. З Rel-16, 5G віртуальну мережу можна налаштувати через 5G систему, яка надає послуги типу 5G LAN (наприклад, VLAN), підтримуючи підключення на вимогу від UE до UE, багатоадресні та широкомовні приватні комунікації в рамках однієї віртуальної мережі 5G [6].

Для подолання проблем фрагментованого ринку промислових Ethernet, з’явився загальний відкритий стандарт - Ethernet з підтримкою TSN. TSN розроблено для задоволення різноманітних вимог QoS, включаючи детерміновані та найкращі затримки. TSN був стандартизований IEEE, а його профіль для промислової автоматизації розробляється спільно IEC та IEEE. Для забезпечення інтеграції 5G з TSN, 3GPP стандартизували набір функцій у Rel-16 як частину Industrial IoT робочого елемента.

1.4 Перспективи розвитку та інтеграції технологій 3GPP для IoT

3GPP продовжує розвивати свої стандарти, щоб відповідати змінним вимогам IoT. Це включає постійні зусилля з покращення ефективності, зменшення затримки та підвищення підтримки різноманітних додатків IoT. З появою додатків 5G можна очікувати, що споживання даних поступово зростатиме в кілька разів порівняно з мережами попереднього покоління. Деякі

додатки 5G мають низьку затримку як вимогу KPI. Щоб зменшити затримку та, таким чином, покращити взаємодію з користувачем. Edge computing є важливою функцією, яка поступово наближає обчислювальні ресурси до кінцевих користувачів.

Граничні обчислення підтримуються в мережах 3GPP завдяки впровадженню можливостей периферійних обчислень у системній архітектурі 5G (3GPP TS 23.501). Для подальшої підтримки системної архітектури 3GPP також представив Edge Enabler Layer (EEL) у 3GPP TS 23.558 у Rel-17, щоб дозволити програмам краще використовувати можливості Edge-обчислень 3GPP. EEL визначає можливості конфігурації та розгортання додатків на межі та дає змогу обладнанню користувача (UE) виявляти та використовувати програми на межі [7].

«EEL складається з Edge Enabler Client (EEC), Edge Enabler Server (EES) і Edge Configuration Server (ECS). EEL надає API для підтримки таких можливостей, як надання послуг, реєстрація, виявлення сервера додатків, доступ до EAS і підтримка безперервності обслуговування» [7].

Для підтримки UE, які перебувають у роумінгу, EEL покладається на ECS, доступні як у HPLMN, так і в VPLMN. EEC в UE отримує послуги EEL від ECS у відвідуваній PLMN (V-ECS) і EES від відвідуваної PLMN (V-EES). Контрольна точка EDGE-10 використовується для взаємодії між H-ECS і V-ECS. Контрольна точка EDGE-4 використовується для взаємодії між EEC і V-ECS у V-PLMN, а також між EEC і H-ECS у H-PLMN [7].

Дві моделі роумінгу підтримуються для граничних додатків:

- Архітектура роумінгу локального підключення (LBO); коли сеанс LBO PDU використовується для маршрутизації трафіку EDGE-4 між EEC і H-ECS; і
- Архітектура роумінгу Home Routed (HR); коли сеанс HR PDU використовується для маршрутизації трафіку EDGE-4 між EEC і H-ECS [7].

Для того, щоб підтримувати можливості роумінгу та об’єднання, ECS можна додатково розширити для підтримки функцій сховища, які називаються ECS-ER, які використовуються в процедурах роумінгу та об’єднання. Однією з

важливих послуг у федерації операторів є спільний доступ до межових вузлів (ENS). ENS — це сценарій, у якому партнерська платформа оператора (OP) ділиться своїми обчислювальними ресурсами для провідної OP. Провідний OP розгортає програму на спільному ресурсі на основі вимог постачальника послуг програми. В такому випадку оператор, що надає OP, також вважається ECSP.

Прогнозується, що майбутнє розширення стандарту 3GPP 5G (Rel-19) включатиме зовнішній IoT в 6G, що дозволить збільшити кількість підключень від мільярдів до трильйонів пристроїв. IoT відкриває можливості для нових джерел прибутку, а також може бути корисним для кінцевих користувачів. Компанія Wiliot представила свої IoT Pixels на MWC 2022. Цей пристрій IoT Pixels можна приєднати до будь-якого виробу і живити його за допомогою перетворених хвиль навколишньої енергії, що дозволяє забезпечити видимість в ланцюгах постачання в режимі реального часу, відстежувати умови (наприклад, температуру) і рівень запасів у режимі реального часу, замість щоденних оновлень для ефективних поставок [8].

1.5 Висновки до розділу 1

В цьому розділі було розглянуто та проаналізовано основні технології передавання інформації 3GPP для IoT.

Було з’ясовано, що специфікації, створені 3GPP, служать основою для стандартів Інтернету речей. Вони є важливим елементом у формуванні технологій IoT і надають широкі можливості для створення різних рішень в області IoT. Навколишній Інтернет речей можна використовувати для відстеження таких дрібниць, як їжа, одяг і ліки, а не дорогих об’єктів, що містять ці окремі активи. Він використовує недорогі всюдисущі радіостанції та не покладається на сканування вручну, але автоматично відчуває речі поблизу та автоматизує підключення, а не покладається на портативні сканери. Радіоприймачі в телефонах, автомобілях, побутовій техніці та іншому обладнанні будуть

модернізовані, щоб забезпечувати енергією та зчитувати сигнали смарт-тегів розміром з поштову марку, які не працюють від батареї.

З цього розділу стало відомо, що стандарти 3GPP, такі як LTE-M, NB-IoT та EC-GSM-IoT, відіграють важливу роль у розвитку Інтернету речей, пропонуючи гнучкість та високу адаптивність для різноманітних IoT-застосувань. Вони забезпечують не тільки широке покриття та низьке енергоспоживання, але й високий рівень безпеки для даних, що обмінюються між пристроями та мережами.

Також, в цьому розділі було вказано, що мобільні оператори мають важливі можливості для трансформації різних секторів завдяки стільниковому Інтернету речей, який інтегрований у мережу 5G. Чотири ключові сегменти IoT - Massive IoT, Broadband IoT, Critical IoT та Industrial Automation IoT - забезпечують комплексний підхід до розвитку IoT, пропонуючи масштабованість, економічну ефективність та високий рівень надійності.

Враховуючи, що в першому розділі було проаналізовано ключові технології 3GPP для IoT та їх значення для розвитку Інтернету речей, у другому розділі ми зосередимося на виявленні та аналізі основних проблем і викликів, які стоять перед цими технологіями. Ми розглянемо питання безпеки, оптимізації споживання енергії та масштабування мережі IoT, а також оцінимо сучасні напрямки та інновації, що можуть сприяти подальшому удосконаленню стандартів 3GPP для IoT.

2 ЗАВДАННЯ РОЗВИТКУ І ПОКРАЩЕННЯ ТЕХНОЛОГІЙ 3GPP

2.1 Аналіз поточних викликів та проблем 3GPP для IoT

2.1.1 Аналіз проблем безпеки в IoT

Технологія 5G являє собою новітній крок у розвитку мобільних комунікацій, і є наступником системи 4G, або системи архітектурної еволюції/довгострокової еволюції (SAE/LTE). Архітектура безпеки 5G була спеціально розроблена з метою забезпечення рівня безпеки, який не поступається 4G, але при цьому інтегрована в новітню 5G систему. Враховуючи широкий спектр потенційних загроз, таких як атаки на радіоінтерфейси, сигнальні та користувацькі площини, а також ризики, пов’язані з маскуванням, конфіденційністю, повторенням даних, зниженням пропускної спроможності, “людиною посередині”, сервісними інтерфейсами (SBI) та безпекою міжоператорських мереж, було впроваджено додаткові заходи безпеки. Ці заходи спрямовані на зміцнення захисту в мережі 5G та забезпечення надійного обміну даними між користувачами.

З переходом від неавтономного розгортання до повністю автономної системи 5G, модель довіри еволюціонувала. Вважається, що довіра в мережі зменшується, чим далі просувається від ядра. Це впливає на рішення, які приймаються при проектуванні безпеки 5G [9].

Модель довіри UE(User equipment) є відносно простою: існують два домени довіри — захищена від несанкціонованого доступу універсальна інтегрована плата (UICC), на якій розміщений універсальний модуль ідентифікації абонента (USIM) як основа довіри, та мобільне обладнання (ME). ME та USIM разом створюють UE. На рисунках 2.1. та 2.2. зображено модель довіри з роумінгом та без роумінгу в декількох рівнях.

Автентифікаційна функція (AUSF) зберігає ключ, який можна використати повторно, отриманий після процесу автентифікації, коли UE реєструється одночасно в різних технологіях мережевого доступу, наприклад, в мережах 3GPP та не-3GPP, таких як бездротова локальна мережа IEEE 802.11 (WLAN). Функція

обробки та репозиторій облікових даних автентифікації (ARPF) зберігає дані автентифікації. Це відповідає USIM на стороні клієнта, або UE.

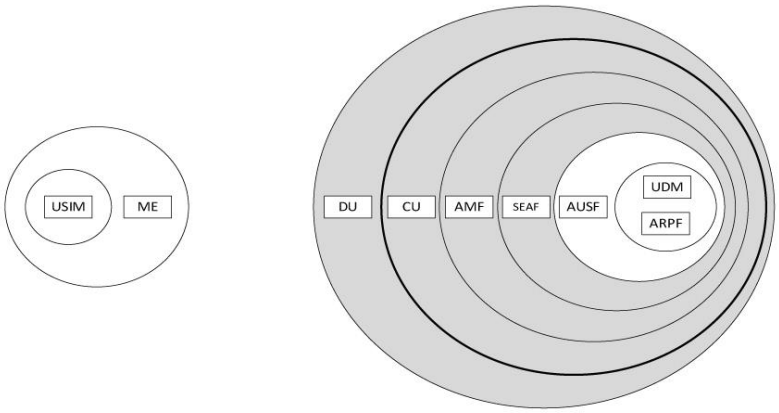

Рисунок 2.1 – Модель довіри без роумінгу [9]

Дані про абонента зберігаються в Єдиному сховищі даних (UDR). Уніфіковане керування даними (UDM) використовує дані підписки, які зберігаються в UDR, і виконує логіку програми для виконання різноманітних функцій, таких як створення облікових даних автентифікації, ідентифікація користувача, безперервність обслуговування та сеансу і тощо. Активні та пасивні атаки через повітряний інтерфейс розглядаються як на площині керування, так і на площині користувача. Конфіденційність стає все більш важливою, що призводить до того, що постійні ідентифікатори залишаються в таємниці через повітряний інтерфейс [9].

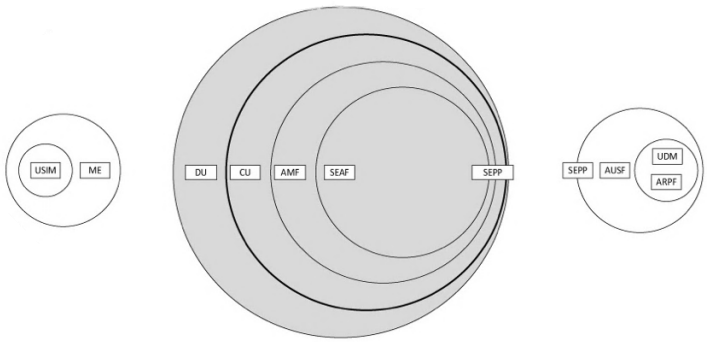

Рисунок 2.2 – Модель довіри з роумінгом [9]

У роумінговій архітектурі домашня та відвідувана мережі з’єднані через проксі захисту безпеки (SEPP) для управління міжмережевим з’єднанням. Це поліпшення було зроблене у 5G внаслідок збільшення кількості атак, таких як викрадення ключів та перенаправлення в мережах SS7, а також наслідування мережевих вузлів та фальсифікація адрес джерел у сигнальних повідомленнях DIAMETER, які використовували довірливість міжмережевого з’єднання.

5G Phase-1 внесла кілька поліпшень до безпеки 4G LTE. Основна автентифікація: Взаємна автентифікація мережі та пристрою в 5G базується на основній автентифікації. Це схоже на 4G, але є кілька відмінностей. Механізм автентифікації має вбудований контроль домашнього оператора, що дозволяє домашньому оператору знати, чи пристрій автентифіковано в даній мережі, та приймати остаточне рішення про автентифікацію. У Фазі 1 5G є два обов’язкові варіанти автентифікації: Автентифікація 5G та Угода про ключі (5G-AKA) та Розширюваний протокол автентифікації (EAP)-AKA’, тобто EAP-AKA’. За бажанням, інші механізми автентифікації на основі EAP також дозволені в 5G - для конкретних випадків, таких як приватні мережі. Також, основна автентифікація є незалежною від технології радіодоступу, тому вона може працювати через технології, що не є 3GPP, такі як IEEE 802.11 WLAN [9].

Одним із ключових аспектів є вторинна автентифікація, яка дозволяє здійснювати перевірку автентичності поза межами домену мобільного оператора за допомогою різноманітних методів на основі EAP. Ця інтеграція в архітектуру 5G сприяє більш гнучкому та безпечному підключенню до різних мереж. Функція управління сесіями (SMF) виконує роль EAP-автентифікатора і покладається на зовнішній сервер DN-AAA для аутентифікації та авторизації запиту UE на встановлення PDU-сесій.

UE реєструється в мережі, виконуючи первинну автентифікацію з AUSF/ARPF та встановлює контекст безпеки NAS з AMF. UE ініціює встановлення нової PDU-сесії, надсилаючи повідомлення SM NAS, що містить запит на встановлення PDU-сесії до AMF. UE включає інформацію про зріз (ідентифіковану S-NSSAI) та PDN, до якої воно хоче підключитися

(ідентифіковану DNN). AMF надсилає запит до SMF для встановлення PDU-сесії (повідомлення Nsmf PDUSession CreateSMContext Request) з повідомленням SM NAS, SUPI, отриманим S-NSSAI та DNN. SMF надсилає повідомлення Nsmf PDUSession CreateSMContext Response до AMF. Потім SMF отримує дані про підписку з UDM для даного SUPI та перевіряє, чи відповідає запит UE підписці користувача та місцевим політикам. SMF також може перевірити, чи було UE автентифіковано та/або авторизовано тією ж DN, як вказано DNN, або тим же AAA-сервером при попередньому встановленні PDU-сесії. SMF може пропустити решту процедури, якщо перевірка успішна [9].

Якщо SMF виявляє, що UE не було автентифіковано з зовнішнім сервером DN-AAA, то SMF ініціює EAP-аутентифікацію для отримання авторизації від зовнішнього сервера DN-AAA та надсилає повідомлення EAP Request/Identity до UE. Потім UE надсилає повідомлення EAP Response/Identity зі своєю DN-специфічною ідентичністю, що відповідає формату Network Access Identifier (NAI). Сервер DN AAA та UE можуть обмінюватися повідомленнями EAP, як це вимагається методом EAP. Повідомлення EAP надсилаються у повідомленні SM NAS між UE та SMF; SMF спілкується з зовнішнім сервером DN-AAA через UPF, використовуючи інтерфейси N4 та N6. Після завершення процедури аутентифікації сервер DN AAA надсилає повідомлення EAP Success до SMF. SMF може зберегти ідентифікатор UE та DNN (або ідентифікатор сервера AAA DN, якщо він доступний) у списку для успішної аутентифікації/авторизації між UE та SMF. Альтернативно, SMF може оновити список в UDM [9].

У випадку роумінгу залучені два SMF, такі як відвідувач SMF (V-SMF) та домашній SMF (H-SMF), де H-SMF виступає в ролі автентифікатора. Після повідомлення про запит на встановлення PDU-сесії від UE через AMF, як обговорювалося вище, V-SMF надсилає запит Nsmf PDUSession Create до H-SMF. Для встановлення запитуваної PDU-сесії після успішної EAP-базованої вторинної аутентифікації, H-SMF надсилає відповідь Nsmf PDUSession Create до V-SMF з EAP Success, і це повідомлення, в свою чергу, надсилається до UE V-SMF.

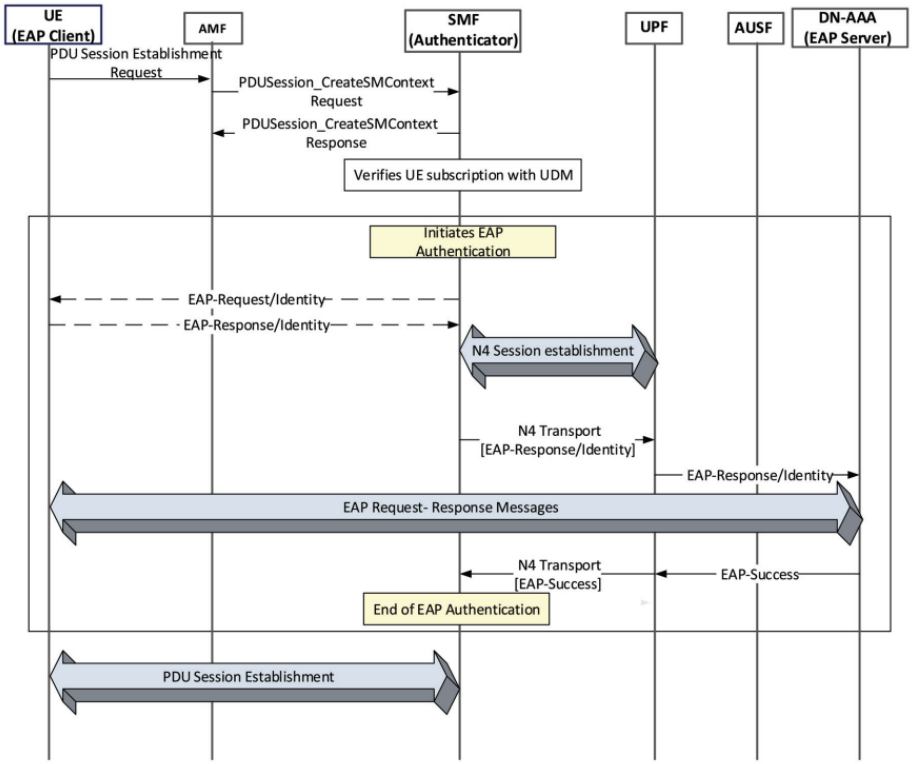

Рисунок 2.3 – Вторинна автентифікація [9]

З метою забезпечення безпеки на міжоператорському рівні, 5G Phase-1 впроваджує заходи, які протидіють вразливостям, виявленим у системах SS7 та Diameter. Ці заходи впроваджуються з самого початку, щоб запобігти потенційним загрозам. Інтерфейс N32 забезпечує міжоператорське мережеве з'єднання, яке може проходити через Internetwork Packet Exchange (IPX). Для забезпечення безпеки з'єднання вводиться SEPP як сутність, що розташована на периметрі PLMN. SEPP реалізує безпеку на рівні додатків для всієї інформації сервісного шару, що обмінюється між двома функціями мережі (NF) через дві різні PLMN. При отриманні повідомлень сервісного шару від даної NF, SEPP захищає повідомлення перед їх відправленням через інтерфейс N32. Аналогічно, при отриманні повідомлення через інтерфейс N32, SEPP пересилає повідомлення до відповідної NF після перевірки безпеки. SEPP забезпечує захист цілісності, конфіденційності частин повідомлення та захист від повторного відтворення. Взаємна автентифікація, авторизація, договір про шифрувальні набори та

управління ключами також є частинами функцій безпеки SEPP. Він також виконує приховування топології та захист від підробки [9].

Конфіденційність абонента, яка була проблемою у попередніх поколіннях мобільних систем, у 5G отримує вдосконалене рішення. Використання публічного ключа домашньої мережі дозволяє захистити постійний ідентифікатор підписки користувача від активних атак, забезпечуючи конфіденційність ідентичності абонента.

Основна мережа 5G побудована на архітектурі на основі послуг, що є нововведенням у порівнянні з 4G та попередніми поколіннями. Ця архітектура забезпечує адекватний рівень безпеки для послуг, які вона надає.

Базова станція в 5G логічно розділена на центральний блок та розподілений блок, між якими існує інтерфейс. Це розділення дозволяє забезпечити безпеку для інтерфейсу CU-DU, а також підтримує різні варіанти розгортання. Розподілені блоки, розташовані на краю мережі, не мають доступу до даних користувача, коли активовано захист конфіденційності, що зберігає безпеку на рівні повітряного інтерфейсу [9].

Ієрархія ключів у 5G відображає зміни в загальній архітектурі та моделі довіри, використовуючи принцип розділення ключів для забезпечення безпеки. Це включає можливість захисту цілісності даних на користувацькій площині, що є нововведенням у порівнянні з 4G [9].

Мобільність у 5G, хоча й схожа на 4G, пропонує новий підхід, де якір мобільності в основній мережі може бути відокремлений від якоря безпеки, що забезпечує більшу гнучкість та безпеку в управлінні мережею.

NSA та 5G Phase-1 дійсно відкривають нове покоління мобільного широкосмугового зв’язку. Наступним кроком будуть рішення для IoT, які охоплюють кілька сценаріїв у формі масової машинної комунікації (mMTC) та ультра надійних комунікацій з низькою затримкою (URLLC). mMTC пов’язана з великою кількістю пристроїв, що передають відносно невеликий обсяг даних, нечутливих до затримок, тоді як URLLC стосується послуг з жорсткими вимогами до пропускної здатності, затримки та доступності.

Для mMTC з дуже низькими швидкостями передачі даних, які можуть знижуватися до кількох бітів на день, необхідно враховувати рівень безпеки (автентифікація, конфіденційність, цілісність і тощо), який можна забезпечити. Ця категорія включає різноманітні IoT або M2M послуги та пристрої, такі як датчики температури, що оновлюються кожну годину, або датчики на сільськогосподарських тваринах, що передають важливі дані декілька разів на день. Ці пристрої також будуть мати обмеження за ресурсами, такими як живлення, обчислювальні можливості та пам’ять. Це призведе до декількох вимог до безпеки, наприклад, автентифікація, не повинна запускатися для кожного спілкування, і навіть коли вона запускається, то повинна виконуватися з мінімальним обсягом даних та часом відповіді. Інша вимога - зменшення бітів, пов’язаних з безпекою, наприклад, цілісність, для кожного спілкування. Алгоритми безпеки та криптографії повинні бути енергоефективними та оптимізованими для роботи з пристроями, які мають обмежені ресурси.

В той же час, (URLLC) це пристрої з високою швидкістю передачі даних, які потенційно мають більші батареї та обчислювальні ресурси: автомобілі, промислові IoT пристрої, такі як машини на заводах, та пристрої віртуальної або доповненої реальності (VR або AR), що використовуються для ігор або послуг у реальному часі. Забезпечення вищих швидкостей передачі даних також означає, що слід враховувати складність функцій безпеки, щоб уникнути затримок обробки. Водночас вищі швидкості передачі даних забезпечуються за рахунок зменшення кількості бітів у радіоінтерфейсі, що, в свою чергу, має наслідки для бітів, які можуть бути виділені для безпеки [9].

2.1.2 Оптимізація споживання енергії

У першому розділі було зроблено детальний огляд стандартів 3GPP для IoT, з акцентом на енергоефективність, яка є критичною для підтримки сталого розвитку та довготривалої роботи IoT пристроїв. Цей огляд виявив, що, розвиток мобільних мереж призвів до зростання їх можливостей для задоволення потреб

різноманітних сценаріїв використання, які перевищують їх первинну мету забезпечення широкосмугового доступу. Однією з таких інновацій є застосування мобільних мереж для Інтернету речей (IoT), відоме як Стільниковий IoT (CIoT). Зростання популярності CIoT стало ключовим напрямком у прогресі мобільних мереж, що сприяє створенню більш розгалужених та інтегрованих екосистем. Постійний розвиток IoT-бізнесу впливає на різні галузі, включаючи медицину, розумні міста, безпеку та аграрний сектор. Однак, велика кількість пристроїв IoT з різноманітними характеристиками та сценаріями використання стикається з проблемами з'єднання через специфіку їх трафіку та високу щільність пристроїв IoT.

Кожне нове покоління мобільних мереж створювалось на базі існуючих послуг попереднього покоління та пропонуючи технологічні удосконалення. Проте, всі чотири попередники мали схильність до дизайну який був переважно зосереджений на послугах, орієнтованих на людей. З появою п'ятого покоління зробили більший акцент на проектуванні мереж для підтримки ширшого спектру випадків використання, включаючи машинно-машинне спілкування та Інтернет речей (IoT). Якщо зосередитись на проблематиці впровадження IoT через мобільні мережі, то більшість з них виникає у трьох різних випадках: встановленні з'єднання, використанні ресурсів мережі та ефективності.

NB-IoT застосовує всього два методи зниження енергоспоживання, щоб гарантувати, що батарея може працювати понад 10 років без перезарядки:

- Режим енергозбереження (PSM);
- Розширений переривчастий прийом (eDRX).

Ці два методи дають змогу пристроям перейти в стан енергозбереження, у якому не потрібно постійно слідкувати за сигналами пейджингу чи розкладом.

У NB-IoT, режим енергозбереження (PSM) надає пристроям можливість перейти у стан глибокого сну, від'єднуючись від більшості з'єднань, але залишаючись у контакті з мережею, як показано на рисунку 2.4. Цей режим дозволяє економити енергію, коли пристрій не використовується, дозволяючи йому активуватися для передачі даних за потреби. PSM, який був введений у

специфікації 3GPP ще до NB-IoT, допомагає IoT-пристроям зберігати заряд батареї, збільшуючи термін їх служби до 10 років і більше. У цьому режимі пристрій може перебувати у стані, схожому на вимкнення, зберігаючи базове з'єднання з мережею, що дозволяє йому відновлювати активність без повторної реєстрації та сигналізації [10].

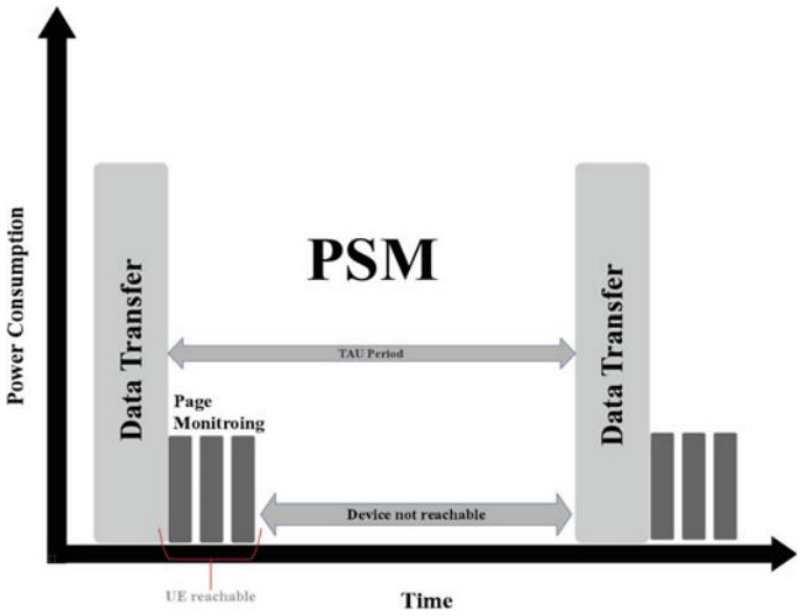

Рисунок 2.4 – Режим енергозбереження (PSM) [10]

Техніка розширеного переривчастого прийому (eDRX) у NB-IoT створює режим очікування для пристроїв, в якому вони не отримують радіосигнали протягом визначеного часу, що сприяє економії енергії. Пристрої періодично активізуються для перевірки пейджингових повідомлень, а потім знову переходять у сон. Часовий інтервал eDRX може становити від 20,48 до 10485,76 секунд, дозволяючи пристрою залишатися в неактивному стані довше. Включення eDRX у специфікацію 3GPP Release 13 надає додаткові можливості для зниження енергоспоживання IoT-пристроїв.

Завершуючи активний цикл, кінцеве обладнання (UE) переходить в режим PSM, вимикаючи радіопередачу та залишаючи включеним лише базовий генератор для відстеження часу. У цьому стані споживання енергії мінімальне,

подібно до вимкненого стану. Техніка eDRX дозволяє збільшити періоди сну I-DRX, встановлюючи активні фази, які регулюються таймером часового вікна пейджингу (PTW) для кожного циклу eDRX. У ці активні фази UE може приймати сигнали I-DRX, після чого настає фаза сну до кінця циклу eDRX, зображено на рисунку 2.5. Цей процес повторюється до того, як спливає таймер активності [10].

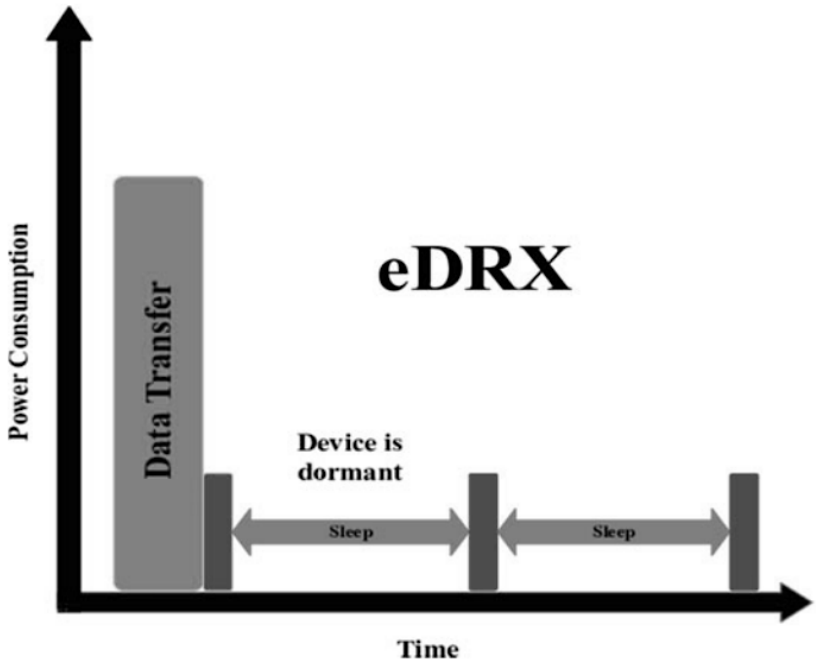

Рисунок 2.5 – Розширений переривчастий прийом (eDRX) [10]

Продовжуючи розглядати питання енергоефективності в стандартах 3GPP для IoT, особливу увагу слід звернути на техніки управління енергією, які дозволяють пристроям LPWA працювати ефективно, зберігаючи енергію та подовжуючи час роботи батареї. Використання режиму низького споживання та протоколів MAC з низькою потужністю є ключовими елементами в цьому процесі. Оптимізація топології мережі та використання більш складних базових станцій також відіграють важливу роль у зменшенні енергоспоживання, дозволяючи LPWA пристроям підтримувати надійне з’єднання без необхідності частого перезаряджання. Для економії енергії в технології LPWA, кінцеве обладнання (UE) не потребує постійної передачі даних. Воно активізується з режиму сну для відправки даних і користується енергоємними компонентами

лише на короткий час. Прості протоколи MAC знижують складність і енергоспоживання для UE LPWA. Варіанти топології мережі включають Mesh топологію, яка використовується у стандартних мобільних мережах та WLAN. UE повинні намагатися підключатися безпосередньо до базової станції, щоб уникнути зайвих перескоків, що допомагає покращити термін служби батареї. У стандартизованих технологіях 3GPP тільки користувач може активувати режим низького споживання. Відмова від зайвих операцій на базових станціях може подовжити термін служби батареї UE [10].

Технології LPWA, разом з мобільними мережами, використовують режим низького споживання енергії для оптимізації її використання та продовження роботи батареї. Цей режим передбачає насамперед, вимкнення важких компонентів, таких як процесор. Режим низького споживання може бути реалізований по-різному в залежності від застосування. Наприклад, пристрій, який передає дані тільки через висхідний канал, може бути запрограмований на відправлення інформації двічі на день або ініціювати передачу даних вручну. Якщо пристрій може отримувати сповіщення через низхідний канал, він повинен слухати мережу для цих повідомлень. Існує кілька способів для досягнення цієї мети, і найбільш підходящий підхід залежить від конкретного випадку використання та частоти активізації пристрою з режиму низького споживання. Якщо пристрій періодично передає повідомлення, він може одночасно слухати повідомлення на низхідному каналі.

У eMTC та NB-IoT, режим низького споживання реалізований по-різному, але обидва використовують енергоефективні техніки, такі як PSM та eDRX. Відмінність між цими техніками полягає в тому, що eDRX дозволяє модему приймати вхідні сигнали, тоді як PSM вимагає, щоб модем прокидався для відправлення даних перед отриманням будь-яких даних. Незважаючи на важливість енергоефективної комунікації для успішного впровадження MTC у існуючі мобільні мережі, потрібно більше досліджень, зосереджених на енергоефективному плануванні висхідного зв’язку MTC [10].

Для підвищення енергоефективності, UE у мобільних мережах можуть зберігати команду попереднього планування, передану через вузькосмуговий фізичний висхідний спільний канал (NPUSCH), і перевіряти її при настанні висхідного пакета. Якщо немає команди попереднього планування, UE дотримується стандартної процедури запиту на планування. Однак, якщо є команда попереднього планування, UE відкладає передачу висхідного пакета до запланованого часу, не ініціюючи процедуру запиту на планування.

У деяких випадках може відбутися радикальна зміна в прибутті трафіку, наприклад, коли деякі мікро-базові станції вимикаються для економії енергії під час періодів низького трафіку. Це вимагає від сусідніх базових станцій покрити зони покриття вимкнених станцій, що називається збільшенням комірки. Під час періодів низького трафіку густина активних базових станцій зменшується, а відстані комунікації збільшуються. Застарілі кінцеві пристрої, такі як смартфони, розраховані на щоденну зарядку і є більш ефективними в таких умовах [10].

2.1.3 Масштабування мережі IoT

Розповсюдження Інтернету речей (IoT) здійснило революцію у різних сферах нашого життя, розширюючи мережеве підключення до повсякденних об’єктів, що дозволяє їм спілкуватися між собою без втручання людини. Однак, ще одним викликом з яким довелося зіштовхнутися IoT – це масштабування мережі.

Проблематика масштабування мережі є комплексною та стосується різних аспектів, наприклад: складність управління та пропускна спроможність. Компанії, що впроваджують мережеві рішення, часто зіштовхуються з труднощами, пов’язаними зі збільшенням витрат на обслуговування та управління, коли мережа розширюється. Ефективне управління великою кількістю підключених пристроїв вимагає високої енергоефективності для легкого підключення та мінімізації потреби в заміні батареї та її зарядці [11]. Топологія «зірка», яка має довгий радіус дії, є значно простішою у встановленні та управлінні порівняно з

більш складною сітчастою топологією, яка включає вузли та гілки. Сітчасті мережі, засновані на технологіях з коротким радіусом дії, зазвичай потребують додаткових ретрансляторів для забезпечення належної щільності покриття, що ускладнює їх налаштування та управління.

Для архітектури IoT, орієнтованої на майбутнє, важливим є вибір комунікаційного рішення з високою пропускною здатністю, здатного обробляти велику кількість транзакцій без негативного впливу на доставку даних. Це дозволяє безперебійно інтегрувати нові пристрої в існуючу мережу.

Додатково, важливо розглянути використання інтелектуальних алгоритмів для оптимізації мережевого трафіку та управління енергією, що може допомогти зменшити витрати на обслуговування та продовжити термін служби пристроїв IoT. Також, розробка модульних мережевих компонентів, які можуть бути легко оновлені або замінені, може сприяти більшій гнучкості та масштабованості мережі.

2.2 Огляд сучасних напрямків та інновацій у вдосконаленні 3GPP для IoT

2.2.1 Способи забезпечення достовірного передавання інформації

Як вже раніше згадувалось, 3GPP співпрацює з організаціями стандартів телекомунікацій для розробки специфікацій мобільних комунікаційних технологій. Найвідомішою їх роботою є розробка та підтримка [12]:

- стандартів GSM, 2G та 2.5G, включаючи GPRS та EDGE,
- стандартів UMTS та 3G, включаючи HSPA та HSPA+,
- стандартів LTE та 4G, включаючи LTE Advanced та LTE Advanced Pro,
- стандартів 5G NR та пов’язаних з 5G, включаючи 5G-Advanced.

Очікується, що наступне видання стандарту 3GPP 5G Advanced принесе навколишній IoT у межах 6G для збільшення зв’язку від мільярдів пристроїв до трильйонів. «Якщо 5G відстежував автомобілі, побутову техніку та контейнери для перевезення, то 6G відстежуватиме все, що знаходиться в цих автомобілях,

побутовій техніці та контейнерах для перевезення», - Стів Статлер, CMO Wiliot [13].

Специфікації 3GPP забезпечують взаємодію між пристроями та мережами, дозволяючи безперебійне спілкування та роумінг між різними операторами мобільного зв’язку та географічними регіонами. Ця взаємодія гарантує, що пристрої можуть ефективно спілкуватися незалежно від мережі, до якої вони підключені, сприяючи глобальним розгортанням та масштабованості.

Роль 3GPP в Інтернеті речей (IoT) є значною. Вона розробляє стандарти та специфікації, які забезпечують зв’язок, взаємодію та масштабованість для пристроїв та додатків IoT. 3GPP також відіграє важливу роль у розробці стандартів для мобільних технологій, включаючи LTE-M (LTE для машин) та NB-IoT (Narrowband IoT, LPWAN), які оптимізовані для додатків IoT. Ці стандарти забезпечують надійне та ефективне рішення для зв’язку багатьох пристроїв IoT, від сенсорів до розумних лічильників та носимих пристроїв.

LTE-M [14] (також LTE-MTC та LTE Cat M) - це технологія мережі широкого охоплення з низьким споживанням енергії, яка дозволяє повторно використовувати встановлену базу LTE з розширеним охопленням. LTE-M, що означає LTE-Machine Type Communication (MTC), також було розроблено 3GPP для включення пристроїв та послуг, спеціально призначених для додатків IoT. LTE-M пропонує швидкість передачі даних 1 Мбіт/с для Release 13 3GPP, яка зростає до 4 Мбіт/с для Release 14, з більшою мобільністю та можливістю голосового зв’язку через мережу.

NB-IoT [14] (Narrowband IoT) - це радіотехнологія, розгорнута в мобільних мережах, яка особливо підходить для внутрішнього покриття, низької вартості, довгого терміну служби батареї та великої кількості пристроїв. NB-IoT обмежує смугу пропускання до однієї вузької смуги 200 кГц, пропонуючи пікові швидкості прийому даних 26 кбіт/с у Release 13 стандарту 3GPP. Release 14 збільшить це до 127 кбіт/с. Таблиця 2.1. відображає характеристики радіоканалу бездротового зв’язку та техніки для специфікацій радіоканалу LTE-M та NB-IoT для досягнення низького BER (bit error rate) та високої надійності передачі інформації.

Таблиця 2.1 – Методи досягнення надійної передачі інформації в системах бездротового зв'язку, побудованих на основі стандартів 3GPP для систем IoT

Характеристика радіоканалу	Description	LTE-M	NB-IoT
Тип кодування каналу, *C*	Кодування для виправлення помилок використовується для підвищення надійності передачі даних за рахунок деяких ресурсів каналу.	Турбо-коди, LDPC (коди з низькою щільністю перевірки на парність)	Турбо-коди, LDPC (коди з низькою щільністю перевірки на парність)
Multiposition Keying, *M*	Техніка модуляції використовується для кодування цифрових даних у несучий сигнал.	QPSK, 16/64-QAM	QPSK
Алгоритми керування потужністю, *P*	Алгоритми використовуються для динамічного регулювання рівнів потужності передачі для оптимізації якості сигналу та покриття.	Алгоритми керування потужністю для оптимізації покриття та мінімізації перешкод у різних умовах мережі.	Використовують алгоритми керування потужністю для економії енергії батареї та подовження терміну служби батареї пристрою в розгортаннях IoT.
Ширина частотного каналу, *F*	Ширина частотного каналу, виділеного для зв’язку.	1.4 МГц, 3 МГц, 5 МГц, 10 МГц або 20 МГц	Від 180 кГц до 3 МГц, оптимізовано для низької потужності, широкого охоплення.
Частотний діапазон	Діапазон частот у спектрі електромагнітних хвиль, що використовується для бездротового зв’язку.	700 МГц, 800 МГц або 1.8 ГГц	800 МГц, 900 МГц або 1.9 ГГц
Максимальна швидкість передачі даних, *V*	Максимально досяжна швидкість передачі даних, яку підтримує радіоканал.	До 1 Мбіт/с, залежно від ширини каналу та умов мережі.	До 250 кбіт/с, оптимізовано для додатків IoT з низькою потужністю та низькою складністю.
Робоча відстань, *L*	Максимальна відстань, на якій може	Кілька кілометрів, що робить його	Кілька кілометрів, оптимізований для дальнього

	підтримуватися надійний зв’язок.	придатним для додатків, що вимагають широкосмугового підключення.	зв'язку при малопотужному розгортанні IoT.

Надійна передача інформації відноситься до здатності системи зв’язку точно та послідовно доставляти дані від відправника до одержувача, навіть у присутності різних ускладнень та викликів, які можуть погіршити якість передачі. Вона має такі характеристики, як точність, послідовність, надійність та своєчасність. У надійній передачі інформація доходить до одержувача з мінімальними помилками (низький рівень помилок бітів, BER) або спотвореннями, забезпечуючи точне передавання та інтерпретацію призначеного повідомлення на стороні одержувача. Надійна передача інформації зазвичай є болючою точкою каналів бездротового зв’язку, а не дротових.

Математична функція для мінімізації BER та максимізації відстані L та швидкості передачі даних V залежить від та пропорційна до комбінації параметрів, таких як тип кодування C та його швидкість, Multiposition Keying M, частотний діапазон F та потужність передавача P:

$$\begin{Bmatrix} \min BER \\ \max L \\ \max V \end{Bmatrix} \propto \{C, M, F, P\}$$

Розрахунок бюджету зв’язку NB-IoT та LTE-M визначено у Дослідженні моделі каналу для частот від 0,5 до 100 ГГц (3GPP TR 38.901 версія 17.1.0 Release 17), ETSI TR 138 901 V17.1.0 [15].

2.2.2 Впровадження штучного інтелекту та машинного навчання

Вплив штучного інтелекту та машинного навчання (AI/ML) зростає в кожній галузі технологій. В контексті розвитку технологій 3GPP, ініціативи,

пов’язані зі штучним інтелектом (AI) та машинним навчанням (ML), відіграють ключову роль у формуванні майбутнього автоматизованих мереж. З появою Rel-18, ці ініціативи набувають нового виміру, розширюючи можливості мережевого аналізу та оптимізації.

Функція аналізу мережевих даних (NWDAF), яка була запроваджена ще у Rel-15, стала основою для розвитку аналітичних здібностей мережі, що згодом отримала подальше розширення у Rel-16 та Rel-17. Це дозволило збирати та аналізувати дані на рівні ядра 5G та кінцевих пристроїв користувачів [16].

Зусилля, спрямовані на самоорганізацію мережі (SON) та мінімізацію тестувань (MDT), визначили процедури збору даних для нових радіомережевих функцій (NR), що розпочалися з Rel-16. Використання цих даних залишалося відкритим для інтерпретації та реалізації.

У Rel-17, під егідою RAN3, було проведено дослідження, яке розглядало принципи високого рівня інтелекту RAN з підтримкою AI. Це дослідження вилилося у формування функціональної структури для інтелекту RAN та визначення переваг NG-RAN з підтримкою AI, аналізуючи різноманітність випадків використання. Це дослідження стало каталізатором для запуску нормативного проекту Rel-18, який фокусується на AI/ML для NG-RAN. Проект має на меті вдосконалення збору даних та сигналізації для підтримки енергоефективності мережі, балансування навантаження та оптимізації мобільності за допомогою AI/ML [16].

Особливу увагу в рамках Rel-18 RAN1 приділено дослідженню AI/ML для повітряного інтерфейсу NR, яке вивчає потенціал розширення радіоінтерфейсу з новими функціями, що підтримують алгоритми на основі AI/ML. Це має на меті підвищення продуктивності та зменшення складності та витрат.

Проект визначає три ключові області для пілотного дослідження: стан каналу (CSI), управління променем (BM) та позиціонування. Ці області допоможуть глибше зрозуміти можливості AI/ML та їх вплив на ефективність порівняно з традиційними методами.

Проект також визначить нотацію та термінологію AI/ML, необхідні для опису моделей AI/ML та їх життєвого циклу, а також взаємодії між мережею та обладнанням користувача. Важливим аспектом є оцінка продуктивності та порівняння з базовими показниками, що не використовують AI/ML, для визначення реального потенціалу цих методів.

Завершальною метою є визначення впливу специфікацій на розгортання та взаємодію методів на основі AI/ML. Хоча конкретні моделі AI/ML не будуть визначені на рівні 3GPP, інтеграція AI/ML у радіоінтерфейс вимагатиме впливу на специфікації на різних рівнях.

Це дослідження, яке охоплює весь період Rel-18, має на меті забезпечити чітке розуміння ролі 3GPP у підтримці AI/ML для радіоінтерфейсу, що може призвести до нормативних проектів у майбутніх версіях 5G Advanced. Поточна робота, безумовно, є важливою віхою у визначенні наступного етапу 5G, а саме 5G Advanced. Це також закладає основу для майбутньої стандартизації мобільних мереж і, безсумнівно, стимулюватиме додаткову роботу з розширення рішень на основі AI/ML у різних напрямках.

У майбутньому випуску Rel-19, підтримка AI/ML стане ключовою для підвищення енергоефективності та оптимізації мобільності в мережах. Зокрема, AI/ML зможе допомогти прогнозувати енергоспоживання та впливати на рішення, пов’язані з енергозбереженням. Однією з нових можливостей є динамічне формування комірок, яке дозволяє коміркам змінювати форму для оптимізації радіозв’язку, розподілу навантаження та енергоефективності. Це може включати зміни в конфігурації мережі та взаємодії між комірками, що впливає на мобільність користувачів та покриття мережі [16].

AI/ML також може сприяти оптимізації продуктивності не тільки на рівні RAN, але й для кінцевих пристроїв користувачів (UE). Наприклад, використання AI/ML може допомогти у вдосконаленні сценаріїв енергозбереження, оптимізуючи споживання енергії UE та продовжуючи термін служби їх батареї, зберігаючи при цьому ефективність мережі. Це відкриває широкі перспективи для

подальшої роботи над AI/ML у рамках 3GPP RAN3, спрямованої на покращення бездротових мереж.

2.3 Висновки до розділу 2

В цьому розділі було розглянуто та проаналізовано ключові аспекти проблематики, розвитку та вдосконалення технологій 3GPP для IoT. Було виявлено, що 5G, як новий крок у розвитку мобільних комунікацій, пропонує покращену безпеку у порівнянні з 4G. Модель довіри 5G еволюціонувала з переходом до повністю автономної системи, що впливає на проектування безпеки.

Також, було з’ясовано, що стандарти 3GPP для IoT зосереджуються на енергоефективності, що є важливим для сталого розвитку та довготривалої роботи IoT пристроїв. Технологія NB-IoT використовує два методи зниження енергоспоживання: режим енергозбереження (PSM) та розширений переривчастий прийом (eDRX).

Важливо підкреслити, що масштабування мережі IoT виявилося викликом, але використання інтелектуальних алгоритмів для оптимізації мережевого трафіку та управління енергією може допомогти зменшити витрати на обслуговування та продовжити термін служби пристроїв IoT.

3GPP, як важливий розробник стандартів мобільних комунікацій, відіграє значну роль у розвитку Інтернету речей. Штучний інтелект та машинне навчання відіграють все більш важливу роль у розвитку технологій 3GPP, особливо в контексті автоматизованих мереж.

Враховуючи загальну картину, отриману в результаті аналізу першого та другого розділів, ми можемо перейти до третього розділу, в якому буде розроблено лабораторну роботу на основі пристроїв зв'язку 3GPP для рішень IoT.

Це дозволить нам використати отримані знання та інформацію для практичного застосування та демонстрації роботи технологій IoT на практиці.

3 РОЗРОБКА І РЕАЛІЗАЦІЯ ЛАБОРАТОРНОЇ РОБОТИ НА ОСНОВІ ПРИСТРОЇВ ЗВ'ЯЗКУ 3GPP ДЛЯ РІШЕНЬ IOT

3.1 Огляд провайдерів і мереж IoT в Україні з використанням стандартів та технологій 3GPP

У сучасному світі, де технології розвиваються стрімкими темпами, важливість зв'язку стає все більшою. Інтернет речей відкриває нові горизонти можливостей для бізнесу та повсякденного життя, перетворюючи звичайні предмети на розумні пристрої, які здатні збирати дані та взаємодіяти з оточенням.

Перш за все, необхідно розглянути готові рішення, які надають мобільні оператори в Україні та на основі яких технологій. Київстар, як один з провідних операторів, пропонує систему Розумного обліку, яка автоматизує процеси моніторингу та управління споживанням природних ресурсів. Ця система не лише сприяє ефективності, але й забезпечує безпеку, виявляючи аварії та незаконні втручання. Їхня послуга Мобільної мережі як сервісу дозволяє клієнтам налаштувати стільникове радіопокриття згідно з власними потребами, що є ідеальним для створення приватних мереж або забезпечення покриття у віддалених місцях. Київстар розгорнув технологію NB-IoT у 2019 році, після успішного тестування на промислових та муніципальних підприємствах. Завдяки цьому, компанія змогла підключити "розумні" лічильники, які моніторять якість електро та тепломереж та подачі води або газу. Це дозволило досягти економії близько 17% операційних витрат підприємств [17].

Vodafone пропонує Smart ESL, систему електронних цінників, яка революціонізує роздрібну торгівлю, дозволяючи автоматизувати процеси ціноутворення та обліку товарів. Їхній сервіс Smart Metering автоматизує збір та облік даних про споживані ресурси, що є важливим для комунальних підприємств та постачальників ресурсів. Smart Parking це інтелектуальна система паркування, яка надає інформацію про наявність паркувального місця в режимі реального часу. Smart Waste — це рішення, які спрямовані на покращення міських сервісів, зменшення викидів вихлопних газів та оптимізацію управління відходами [18].

Vodafone Україна запустила комерційну мережу NB-IoT, яка надає надійний та стабільний зв’язок для інтернету речей, відкриваючи можливості для підключення мільйонів пристроїв та сенсорів. Ця мережа дозволяє клієнтам оптимізувати свої бізнес-процеси та скоротити операційні витрати за рахунок віддаленого моніторингу та аналізу даних.

Lifecell відзначається своїми рішеннями для Розумного міста, включаючи моніторинг довкілля, інтелектуальне освітлення та паркування, а також управління громадським транспортом. Ці рішення спрямовані на підвищення якості життя міських жителів та оптимізацію міських сервісів. У сфері Розумної логістики та Розумного сільського господарства, Lifecell пропонує інноваційні рішення для моніторингу активів та вантажів, а також для контролю вологості ґрунту та температури, що сприяє ефективному управлінню ресурсами. Lifecell, розвиває дві технології: NB-IoT та LoRaWAN [19]. NB-IoT використовується для підключення широкого спектру автономних пристроїв, таких як медичні датчики та лічильники споживання ресурсів. LoRaWAN, який є протоколом низької потужності для широкої зони покриття, оптимізований для низького енергоспоживання на довгих відстанях, ідеально підходить для самопрацюючих бездротових пристроїв.

Наступним пунктом варто розглядати тарифні плани кожного оператора, щоб зрозуміти, які з них найкраще відповідають потребам конкретного застосування. Від правильності цього вибору залежить не лише стабільність роботи пристроїв, але й загальна економічна ефективність впровадження IoT-рішень. Розглянемо детальніше тарифні плани трьох провідних мобільних операторів України — Vodafone, Lifecell та Київстар — та оцінимо їх переваги та недоліки в контексті різних бізнес-задач.

Київстар пропонує чотири основні тарифи для IoT, як зображено на таблиці 3.1., вони включають пакети з обмеженою кількістю SMS та даних, що є достатнім для базових потреб зв’язку між пристроями. Наприклад, тариф “IoT Старт” включає 25 SMS та 25 одиниць трафіку для передачі даних. Ці плани

можуть бути вигідними для невеликих проектів або для пристроїв, які не потребують великого обсягу даних.

Таблиця 3.1 – Тарифні плани Київстар

Послуга	IoT Platform 30	IoT Platform 35	IoT Platform 60	IoT Platform POOL 40
Мобільний інтернет	30 МБ	300 МБ	1000 МБ	400 МБ
Пакетні хвилини	10 хв	20 хв	100 хв	40 хв
SMS по Україні	10 SMS	20 SMS	100 SMS	40 SMS
Ціна	30 грн/міс	40 грн/міс	60 грн/міс	40 грн/міс

Vodafone пропонує ширший спектр тарифів IoT (таблиця 3.2.), які варіюються від невеликих пакетів до планів з великим обсягом даних, таких як “IoT Max” з 5000 МБ інтернету. Ці плани можуть бути більш вигідними для компаній, які потребують інтенсивного обміну даними між пристроями. Також Vodafone пропонує 50% знижку для юридичних осіб та ФОП, що робить саме їх тарифні плани більш привабливими, саме у фінансовому плані відносно інших мобільних операторів.

Таблиця 3.2 – Тарифні плани Vodafone

Послуга	IoT Start	IoT L	IoT Pro	IoT Max	IoT Streaming	IoT Unlim
Мобільний інтернет	24 МБ	400 МБ	1500 МБ	5000 МБ	250000 МБ	Безліміт
Пакетні хвилини	24 хв	50 хв	1000 хв	2500 хв	-	-
SMS по Україні	24 SMS	50 SMS	100 SMS	100 SMS	100 SMS	100 SMS
Ціна	24 грн/міс	35 грн/міс	50 грн/міс	100 грн/міс	250 грн/міс	500 грн/міс

Lifecell відзначається гнучкістю своїх IoT тарифів (таблиця 3.3.), які варіюються від базових пакетів для невеликих IoT пристроїв до розширених планів для великих IoT систем. Наприклад, тариф 4G IoT 25 пропонує 30 MB інтернету та 30 SMS, що є оптимальним для пристроїв, які не потребують інтенсивного обміну даними. Для більш вимогливих IoT рішень, таких як віддалене моніторингове обладнання або системи розумного міста, тариф 4G IoT 120 з 10000 MB інтернету та 1000 SMS надає достатній обсяг ресурсів для стабільної та ефективної роботи.

Таблиця 3.3 – Тарифні плани Lifecell

Послуга	4G IoT 25	4G IoT 30	4G IoT 40	4G IoT 60	4G IoT 90	4G IoT 120
Мобільний інтернет	30 МБ	350 МБ	1000 МБ	3000 МБ	6000 МБ	10000 МБ
Пакетні хвилини	30 хв	50 хв	100 хв	300 хв	600 хв	1000 хв
SMS по Україні	30 SMS	50 SMS	100 SMS	300 SMS	600 SMS	700 SMS
Ціна	25 грн/міс	30 грн/міс	40 грн/міс	60 грн/міс	90 грн/міс	120 грн/міс

Порівнюючи ці рішення, можна побачити, що у контексті IoT-рішень на українському ринку, Київстар, Vodafone та Lifecell пропонують різноманітні технології та тарифні плани, які відповідають різним потребам бізнесу. Київстар зосереджений на автоматизації моніторингу та управління споживанням ресурсів, а також налаштуванні стільникового радіопокриття, що є корисним для створення приватних мереж. Їх технологія NB-IoT, запущена у 2019 році, дозволяє підключення “розумних” лічильників, що сприяє економії операційних витрат.

Vodafone відкриває можливості для роздрібної торгівлі за допомогою системи Smart ESL, а також надає рішення для комунальних підприємств, паркування та управління відходами через Smart Metering, Smart Parking та Smart Waste. Їх комерційна мережа NB-IoT забезпечує стабільний зв’язок для мільйонів пристроїв, що дозволяє оптимізувати бізнес-процеси.

Lifecell вирізняється своїми рішеннями для Розумного міста, включаючи моніторинг довкілля, інтелектуальне освітлення та паркування, а також управління громадським транспортом. Їх технології NB-IoT та LoRaWAN підходять для широкого спектру пристроїв, від медичних датчиків до систем контролю ресурсів.

У плані тарифів, Київстар пропонує базові пакети, які підходять для проектів з обмеженим обміном даними, тоді як Vodafone має ширший спектр тарифів, включаючи знижки для юридичних осіб, що робить їх пропозицію привабливою для компаній з інтенсивним обміном даними. Lifecell надає гнучкі тарифні плани, які можуть бути оптимальними як для невеликих, так і для великих IoT систем.

Загалом, вибір між цими операторами залежить від специфіки проекту, вимог до обміну даними та фінансових можливостей. Ретельний аналіз технологічних можливостей та тарифних планів допоможе компаніям визначити найбільш підходящого мобільного оператора для реалізації своїх IoT-ініціатив.

На сьогодні, вже існує багато розроблених технічних рішень згідно стандартів 3GPP. У моїй роботі, я вибрала SIM7000E до Raspberry Pi, як такий, що доступний для широкого кола користувачів та має гнучкі можливості для налаштування та дослідження.

3.2 Технічний аналіз модуля зв'язку NB-IoT/Cat-M/EDGE/GPRS/GNSS на SIM7000E до Raspberry Pi

3.2.1 Технічний огляд мікроконтролера Raspberry Pi

Raspberry Pi представляє собою інноваційний одноплатний комп’ютер, розроблений організацією Raspberry Pi Foundation з метою підвищення рівня комп’ютерної грамотності серед шкільної молоді. Завдяки своїй економічності, модульності, відкритості конструкції та сумісності з універсальними інтерфейсами HDMI та USB, цей пристрій здобув значну популярність не лише в освітніх кругах, а й у сферах, що вимагають високотехнологічних рішень, таких

як робототехніка, автоматизація житла та виробництва, а також серед шанувальників комп’ютерної техніки та електроніки [20].

Наразі в лінійці Raspberry Pi представлено три основні серії, кожна з яких має декілька поколінь. Основні одноплатні комп’ютери Raspberry Pi оснащені інтегрованою системою на чіпі (SoC) від Broadcom, яка включає ARM-сумісний процесор (CPU) та графічний процесор (GPU). У свою чергу, Raspberry Pi Pico використовує чіп RP2040, що також містить ARM-сумісний центральний процесор. З часом випуску першого покоління Raspberry Pi у 2012 році, цей одноплатний комп’ютер пройшов через значні удосконалення та ітерації. Початкові моделі, такі як Model B та більш проста Model A, були оснащені процесорами ARM11 і мали розмір приблизно з кредитну картку, що встановило стандарт для базових форм-факторів у цій категорії пристроїв. Згодом, у 2014 році, було представлено Model B+, який приніс покращення у дизайн, а також було випущено Обчислювальний модуль для вбудованих застосувань.

У 2015 році з’явився Raspberry Pi 2 Model B з 32-розрядним чотирьохядерним процесором ARM Cortex-A7, який згодом був оновлений до 64-розрядного ARM Cortex-A53. Наступне покоління, Raspberry Pi 3, випущене у 2016 році, продовжило цю тенденцію з підвищенням тактової частоти до 1,2 ГГц та інтеграцією Wi-Fi та Bluetooth. Model B+ цього покоління, представлений у 2018 році, приніс ще більшу швидкість процесора, покращений Ethernet та подвійний діапазон Wi-Fi.

Raspberry Pi 4, випущений у 2019 році, став значним стрибком у продуктивності з його 1,5 ГГц чотирьохядерним процесором ARM Cortex-A72, підтримкою до 8 ГБ оперативної пам’яті та можливістю підключення двох моніторів з роздільною здатністю до 4K. Ця модель також вирішила проблему живлення, яка виникла з USB-C, та впровадила поліпшення у вигляді нового чіпа Broadcom BCM2711 C0.

Raspberry Pi 400, представлений у 2020 році, відзначився інтеграцією одноплатного комп’ютера з клавіатурою, створюючи компактний клавіатурний комп’ютер з підвищеною тактовою частотою. Новітнє покоління, Raspberry Pi 5,

анонсоване у 2023 році, принесло подвійне збільшення потужності порівняно з попередником, нові функції управління живленням та відсутність аудіо/відеороз'єму 3,5 мм, замість якого користувачі можуть використовувати альтернативні звукові інтерфейси.

Окремо від основної лінійки, Raspberry Pi Zero, випущений у 2015 році, запропонував більш компактний та доступний варіант з обмеженими можливостями вводу/виводу. Його наступні версії, такі як Zero W та Zero 2 W, розширили можливості з Wi-Fi та Bluetooth, а також підтримкою 64-бітної архітектури.

Raspberry Pi Pico, запущений у 2021 році, відкрив новий напрямок для Raspberry Pi як мікроконтролер, призначений для фізичних обчислень та програмування на різних мовах, включаючи MicroPython та C++. Його версія Pico W додала підтримку Wi-Fi, розширюючи можливості для IoT-проектів.

Кожне нове покоління Raspberry Pi пропонувало значні удосконалення у продуктивності, інтеграції та функціональності, роблячи ці пристрої все більш привабливими для широкого спектру застосувань від освіти до промисловості.

Для написання дипломної роботи, було використано мікроконтролер Raspberry Pi 3 Model B+, як зображено на рисунку 3.1.

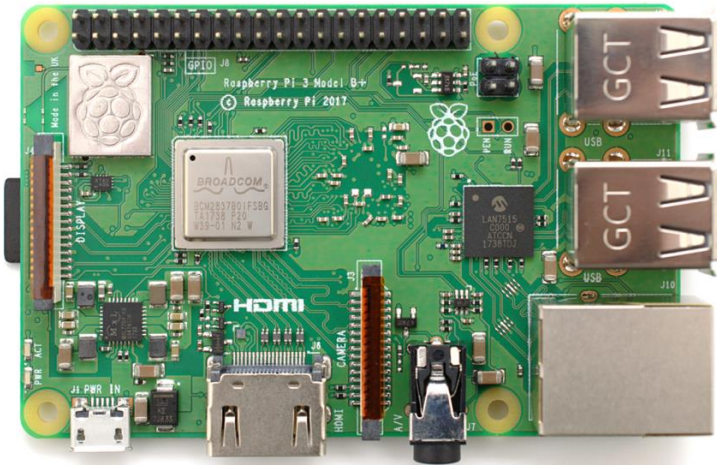

Рисунок 3.1 – Raspberry Pi 3 Model B+ [20]

Raspberry Pi 3 Model B+ відрізняється використанням більш потужного процесора з частотою 1,4 ГГц (4-ядерний ARM Cortex-A53), двоканального Wi-Fi модуля з підтримкою 802.11ac, Bluetooth 4.2, удосконаленого Ethernet модуля з можливістю живлення через Ethernet (PoE), покращеними опціями завантаження з PXE/USB та вдосконаленими температурними характеристиками. Ethernet модуль було модернізовано до Gigabit Ethernet, але через підключення через USB 2.0, максимальна швидкість передачі даних становить 300 Мб/с. Незважаючи на це, тести показали значне збільшення швидкості передачі даних через Ethernet та Wi-Fi порівняно з попередньою моделлю Raspberry Pi 3.

Оперативна пам’ять складається з 1 ГБ LPDDR2 SDRAM. Для зберігання даних використовується лише SD-карта у слоті Micro SD.

Пристрій має два відеовиходи: стандартний HDMI порт для підключення зовнішнього монітора чи проектора та MIPI (DSI) для використання з 7-дюймовим сенсорним екраном Raspberry Pi. Для аудіо є 3,5 мм стерео джек та HDMI аудіовихід. Плата оснащена 40-контактним GPIO з’єднувачем, який включає цифрові сигнали, I2C, SPI, UART інтерфейси, а також апаратне та програмне PWM сигнал генерації. Також присутні контакти для 5V та 3.3V живлення. Плата може отримувати живлення через microUSB роз’єм або GPIO піни з номінальною напругою 5В. USB 2.0 порти збережені, а USB 3.0 порти, як і раніше, відсутні. На рисунку 3.2. зображена схема розташування роз'ємів і основних мікросхем на Raspberry Pi 3.

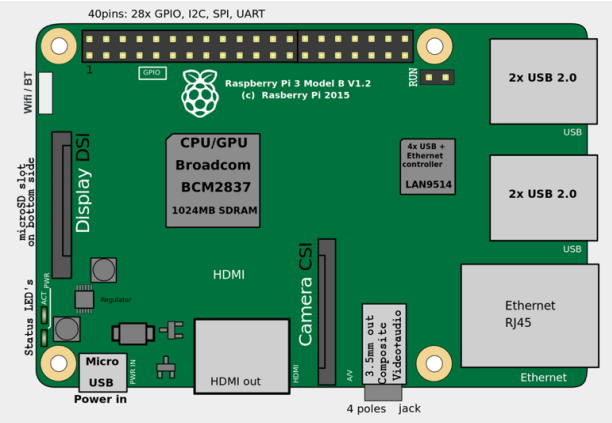

Рисунок 3.2 – Розташування роз'ємів і основних мікросхем на Raspberry Pi 3

Для підключення зовнішніх датчиків, модулів, контролерів чи дисплеїв до мікрокомп’ютера Raspberry PI використовуються GPIO порти на платі. GPIO, або General Purpose Input/Output, це універсальні піни вводу/виводу, які можна використовувати для різноманітних завдань. На Raspberry Pi A+, B+ та 2, GPIO піни розташовані на 40-контактному роз'ємі. Кожен пін має свій номер та може мати кілька функцій (рисунок 3.3.), включаючи I2C, SPI, UART, а також можливість бути використаним як звичайний цифровий вхід або вихід

I2C - це двопровідний інтерфейс, який використовується для зв'язку між мікросхемами на короткі відстані. Він дозволяє підключати багато пристроїв (кожен з яких має свій унікальний адрес) до двох ліній: SDA (дані) та SCL (годинник).

UART - це послідовний інтерфейс, який передає дані біт за бітом. Він використовується для зв'язку між комп'ютерами або пристроями, де не потрібна висока швидкість передачі, але важлива простота підключення.

SPI- це інтерфейс, який використовує чотири лінії для зв'язку: MISO, MOSI, SCLK та SS. Він дозволяє швидку передачу даних між мікросхемами.

Крім того, на платах Raspberry Pi є піни, які призначені для заземлення (Ground), а також піни з живленням 3.3V та 5V, які можуть бути використані для живлення зовнішніх пристроїв. Для активації та використання цих інтерфейсів необхідно налаштувати Raspberry Pi через файл конфігурації або використовуючи команди в терміналі.

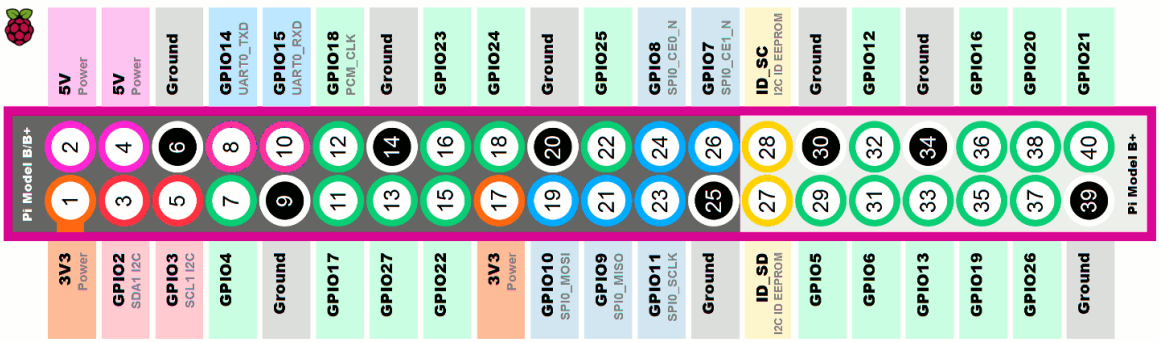

Рисунок 3.3 – Розташування портів мікроконтролера [21]

Raspberry Pi працює на базі операційної системи Raspberry Pi OS, яка раніше була відома як Raspbian. Ця система є офіційно підтримуваною та рекомендованою операційною системою для Raspberry Pi. Raspberry Pi OS заснована на Debian Linux і спеціально розроблена для використання з Raspberry Pi, включаючи широкий спектр попередньо встановлених програм та інструментів, які готові до використання. Операційна система доступна у декількох варіантах, включаючи версії з робочим столом та рекомендованим програмним забезпеченням, а також легку версію без графічного інтерфейсу.

3.2.2 Технічний огляд модуля зв’язку SIM7000E NB-IoT HAT

Модуль зв'язку NB-IoT/Cat-M/EDGE/GPRS/GNSS на модулі SIM7000E (SIM7000E NB-IoT HAT) який є універсальним модулем для Raspberry Pi HAT, надає широкий спектр комунікаційних можливостей, включаючи NB-IoT, eMTC, EDGE, GPRS і GNSS і NB -IoT (рисунок 3.4.). Цей модуль було створено консорціумом 3GPP в процесі розробки стандартів нового покоління мобільних мереж. Початкова версія специфікації була випущена у червні 2016 року. Ці технології IoT, які є розвитком стандарту LTE (4G), мають такі переваги, як низьке споживання енергії, низька вартість та широке покриття. Вони ідеально підходять для застосувань, таких як розумні пристрої, дистанційне керування, відстеження активності, віддалений моніторинг, електронне здоров’я, мобільні POS-термінали, спільне використання велосипедів і багато іншого. Тим часом GSM/GPRS і EDGE є класичними технологіями 2G/2.5G, які можуть надсилати SMS або забезпечувати інші види бездротового зв’язку [22].

Завдяки вбудованому USB-інтерфейсу, модуль дозволяє легко тестувати AT-команди та отримувати дані GPS-позиціонування. Роз’єм управління UART забезпечує зручне підключення до хост-плат, таких як Arduino або STM32. Вбудований перетворювач напруги з можливістю перемикання між 3,3 В та 5 В, слот для SIM-карти, сумісний зі звичайними та NB-IoT картами, а також два

світлодіодні індикатори для контролю робочого стану роблять цей модуль надзвичайно зручним у використанні.

Рисунок 3.4 – Модуль зв’язку SIM7000E NB-IoT HAT

Швидкість передачі даних через UART інтерфейс може варіюватися від 300 біт/с до 3686400 біт/с, що забезпечує високу гнучкість для різних потреб комунікації. Модуль також підтримує управління за допомогою AT-команд, відповідно до стандартів 3GPP TS 27.007, 27.005 та розширених AT-команд SIMCOM, а також інструментарій додатку SIM, включаючи SAT Class 3, GSM 11.14 Release 98, USAT.

На таблиці 3.4 зображені параметри зв’язку SIM7000C NB-IoT HAT.

Таблиця 3.4 – Параметри зв’язку [22]

SIM7000C NB-IoT HAT	NB-IoT	EMTC	EDGE	GSM / GPRS
Група	SIM7000E: FDD-LTE B3 / B8 / B20 / B28		GPRS / EDGE 900/1800 МГц	
	SIM7000C: FDD-LTE B1 / B3 / B5 / B8			
Енергозбереження	Струм в сплячому режимі: 1,2 мА (@ DRX = 2,56 с). Струм в режимі PSM: 9 мкА.			

Продовження таблиці 3.4

Випромінююча потужність	Клас 3 (0.25W@LTE)		Клас E2 (0.5W@EGSM900) Клас E1 (0.4W@DCS1800)	Клас 4 (2 Вт @ GSM900) Клас 1 (1 Вт @ DCS1800)
Швидкість передачі даних	Uplink≤66kbps Downlink≤34kbps	Uplink≤375kbps Downlink≤300kbps	Uplink≤236.8kbps Downlink≤236.8kbps	Uplink≤85.6kbps Downlink≤85.6kbps
Сім-картка	NB Специфічно (не включено)	Звичайна SIM-картка (не входить в комплект)		

3.2.3 Процес налаштування модуля зв'язку SIM7000E NB-IoT HAT до Raspberry Pi

На основі технічного огляду модуля зв’язку SIM7000E NB-IoT HAT та Raspberry Pi, який було проведено в попередньому підпункті, ми можемо перейти до детального опису процесу налаштування цих пристроїв. Цей процес включатиме в себе ряд послідовних кроків, які дозволяють нам перетворити ці пристрої на повноцінну систему, здатну передавати дані в Інтернет.

Першим кроком є завантаження образу операційної системи Raspbian OS з офіційного сайту і запис його на SD-карту за допомогою спеціального програмного забезпечення, наприклад, Balena Etcher. Після завершення запису, SD-карту можна вставити в слот для карт пам’яті Raspberry Pi. Після цього нам необхідно підключити всі необхідні периферійні пристрої: монітор (через HDMI), клавіатуру і мишу (через USB). З вбудованим Wi-Fi модулем в Raspberry Pi 3, ми можемо підключитися до мережі. Для цього нам потрібно відкрити налаштування Wi-Fi в графічному інтерфейсі Raspbian OS і вибрати потрібну мережу. Після цього ввести пароль мережі для підключення. Також, можна змінити стандартний пароль користувача Raspberry Pi для забезпечення безпеки вашого пристрою.

Наступним кроком буде підключення модуля SIM7000E NB-IoT HAT до Raspberry Pi. Для цього спочатку вставляється SIM-карта в слот SIM7000E NB-IoT HAT. Це дозволить модулю з’єднатися з мережею за допомогою мобільного зв’язку. Потім підключається GSM-антена до модуля, яка забезпечує прийом та передачу сигналів мобільного зв’язку.

Після цього модуль SIM7000E NB-IoT HAT підключається до GPIO портів Raspberry Pi. А також, підключається USB інтерфейс модуля до Raspberry Pi за допомогою мікро USB кабелю. Це дозволяє Raspberry Pi та модуль SIM7000E NB-IoT HAT обмінюватися даними.

Після підключення модуля зв’язку SIM7000E NB-IoT HAT до Raspberry Pi, потрібно оновити систему. Це важливий етап, оскільки оновлення системи забезпечує наявність найновіших пакетів та безпеки. Для цього відкриваємо вікно терміналу та вводимо наступні команди: sudo apt-get update, яка синхронізує вашу систему з серверами пакетів, щоб вона знала про всі доступні оновлення та sudo apt-get upgrade, яка потім встановлює ці оновлення [23].

Після оновлення системи потрібно виконати конфігурацію інтерфейсів, нам потрібно увімкнути зв'язок через послідовний порт, це те мікроконтролер та модуль зв’язку будуть спілкуватися між собою. Знову відкриваємо вікно терміналу та вводимо команду sudo raspi-config та натискаємо Enter, після цього ми побачимо меню, в якому нам потрібно вибрати Interfacing Options та натиснути Enter, ми потрапляємо в більш детальне меню в якому обираємо Serial Port, після цього натискаємо No далі Yes [23]. Після цього Raspberry Pi потрібно перезавантажити для застосування змін.

Після перезавантаження, ми повертаємося на робочий стіл. Тепер нам потрібно встановити minicom для нашої системи [23]. Minicom – це програма послідовного зв’язку. Ми знову відкриваємо вікно терміналу та вводимо наступну команду: sudo apt-get install minicom, тиснемо Enter. Далі ми побачимо запитання, чи хочемо ми продовжити – тиснемо Y та Enter, щоб продовжити процес.

Тепер нам потрібно завантажити демо – коди. Для того, аби завантажити zip-файл з прикладами кодів та драйверів для роботи модуля зв’язку нам

необхідно відкрити нове вікно терміналу та ввести наступну команду: wget https://files.waveshare.com/upload/2/24/SIM7000X-Demo.7z. Після завершення, в цьому ж вікні ми послідовно вводимо наступні команди:

- sudo apt-get install p7zip-full
- 7z x SIM7000X -Demo.7z -r -o/home/pi
- sudo chmod 777 -R /home/pi/SIM7600X-4G-HAT-Demo
- sudo nano /etc/rc.local

Після введення останнього рядку, у нас відкриється нова сторінка (файл | rc.local |). Нам потрібно буде додати команду в | rc.local | файл. Наступну команду ми повинні ввести на рядку між: fi та exit. Текст команди буде наступним: sh /home/pi/SIM7000X-Demo/Raspberry/c/sim7000_init. Після цього натискаємо Ctrl+X , далі Y , а потім клавішу Enter , щоб зберегти зміни. Виконання цієї команди означає, що драйвери запускатимуться під час завантаження Raspberry Pi.

Тепер нам знову потрібно відкрити нове вікно терміналу, та ввести кожну з поданих нижче команд по черзі. Перша команда направить фокус на папку bcm2835, де знаходиться драйвер: cd /home/pi/SIM7000X-Demo/Raspberry/c/bcm2835. Наступна команда надасть доступ та активує драйвер: chmod +x configure && ./configure && sudo make && sudo make install. На цьому етапі, ми повністю налаштували модуль зв’язку для роботи з мікроконтролером.

Враховуючи вищезазначені кроки, ми можемо стверджувати, що процес налаштування модуля зв’язку SIM7000E NB-IoT HAT до Raspberry Pi є досить прямолінійним і систематичним. Він включає в себе ряд важливих етапів, які, будучи виконаними в правильному порядку, дозволяють створити робочу систему, здатну передавати дані в Інтернет. З урахуванням цієї інформації, ми можемо перейти до наступного розділу, де буде розглянуто розробку та реалізацію лабораторної роботи.

3.3 Розробка опису до Лабораторної роботи для налаштування рішення IoT на основі модуля зв'язку 3GPP SIM7000E та мікроконтролера Raspberry Pi

Спираючись на детальний процес налаштування модуля зв’язку SIM7000E NB-IoT HAT до Raspberry Pi у попередньому пункті, можна зробити опис лабораторної роботи. Весь текст лабораторної роботи вказаний у додатку А.

У додатку А міститься вступна частина, із загальною інформацією про лабораторну роботу, включаючи її мету та зміст, яка дає розуміння, що буде виконано у лабораторні роботі. Далі відображений алгоритм виконання роботи, який містить покроковий опис виконання лабораторної роботи, який допоможе зрозуміти, які дії повинні бути виконані та в якому порядку. Також, наданий приклад виконання роботи, який містить детальний опис кожного кроку, включаючи конкретні команди, які потрібно виконати, та місця, де їх потрібно вставити. Для наглядного розуміння процесу було додано скріншоти. В останньому пункті, було розміщено, контрольні питання, які допомагають перевірити засвоєння матеріалу студентами.

В цій лабораторній роботі студенти зможуть налаштувати модуль зв’язку SIM7000E NB-IoT HAT для Raspberry Pi і провести тестування для перевірки його роботи. Це надасть їм практичний досвід роботи з цими технологіями та допоможе зрозуміти, як вони можуть бути використані для розробки рішень IoT.

Ця лабораторна робота надасть студентам можливість глибше вивчити процес конфігурації та використання модуля зв’язку SIM7000E та мікроконтролера Raspberry Pi. Ці компоненти є важливими елементами при створенні рішень для Інтернету речей (IoT). Крім того, ця робота допомагає студентам набути практичних навичок у проведенні тестування та перевірки роботи цих компонентів, що є важливим етапом при розробці надійних та ефективних систем IoT.

Виконуючи цю лабораторну роботу, студенти отримають цінний досвід роботи з передовими технологіями IoT, такими як модуль зв’язку SIM7000E та мікроконтролер Raspberry Pi. Більше того, вони зможуть глибше зануритися в світ

IoT, вивчаючи, як ці технології можуть бути застосовані для створення інноваційних рішень.

Ця лабораторна робота є важливим кроком на шляху до розуміння та використання технологій IoT. Вона надає студентам необхідні навички та знання, які вони зможуть використовувати в майбутніх проектах та дослідженнях.

3.4 Висновки до розділу 3

У третьому розділі було зосереджено увагу на розробці та реалізації лабораторної роботи, що базується на пристроях зв’язку 3GPP для рішень Інтернету речей.

Було зроблено порівняльний аналіз провайдерів та мереж IoT в Україні, які використовують стандарти та технології 3GPP. Було проведено огляд провайдерів, таких як Київстар, Vodafone та Lifecell, щодо їх технологій, тарифних планів та специфічних рішень для різних секторів бізнесу.

Виконано технічний аналіз модуля зв’язку NB-IoT/Cat-M/EDGE/GPRS/GNSS на SIM7000E до Raspberry Pi. Було розглянуто мікроконтролер Raspberry Pi та модуль зв’язку SIM7000E NB-IoT HAT, а також було описано процес налаштування цього модуля до Raspberry Pi. У завершальній частині розділу, було приділено увагу створенню опису лабораторної роботи для налаштування рішення IoT на основі модуля зв’язку 3GPP SIM7000E та мікроконтролера Raspberry Pi.

ВИСНОВКИ

У результаті виконаної роботи було проведено детальний аналіз стандартів 3GPP для рішень Інтернету речей. В першому розділі було зроблено акцент на аналізі основних технологій 3GPP, що використовуються для IoT. Було виявлено, що специфікації, розроблені 3GPP, формують основу для стандартів IoT, відкриваючи широкі можливості для розробки різноманітних IoT-рішень.

В другому розділі було зосереджено увагу на ключових аспектах проблематики, розвитку та вдосконалення технологій 3GPP для IoT. Було встановлено, що 5G, як наступний етап розвитку мобільних комунікацій, пропонує покращення в області безпеки порівняно з 4G. Також, було з'ясовано, що стандарти 3GPP для IoT фокусуються на енергоефективності, що є досить важливим для сталого розвитку та довготривалої роботи IoT пристроїв.

У третьому розділі основна увага була приділена розробці та реалізації лабораторної роботи, що базується на пристроях зв'язку 3GPP для рішень Інтернету речей. Було зроблено порівняльний аналіз провайдерів та мереж IoT в Україні, які використовують стандарти та технології 3GPP.

Підсумовуючи, можна сказати, що ця робота робить значний внесок у розуміння та використання стандартів 3GPP для рішень Інтернету речей. Вона демонструє, як ці стандарти можуть бути використані для розробки та впровадження ефективних IoT-рішень, які відповідають потребам сучасного суспільства. Завдяки цій роботі, ми можемо краще розуміти та оцінювати потенціал та можливості, які надає 3GPP для розвитку Інтернету речей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Singh G. 3GPP IoT. *Telecom Trainer*. URL: https://www.telecomtrainer.com/3gpp-iot/

2. Contributors to Wikimedia projects. LTE-M - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/LTE-M

3. Contributors to Wikimedia projects. Narrowband IoT - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Narrowband_IoT

4. Extended Coverage - GSM – Internet of Things (EC-GSM-IoT). *Internet of Things*. URL: https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/extended-coverage-gsm-internet-of-things-ec-gsm-iot/

5. 3*GPP – The Mobile Broadband Standard*. URL: https://www.3gpp.org/images/presentations/3GPP_Standards_for_IoT.pdf

6. Cellular IoT in the 5G era / A. Zaidi et al. *Ericsson - Helping to shape a world of communication*. URL: https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-in-the-5g-era

7. 3GPP EDGEAPP: Roaming, Federation and Edge Node Sharing. *3GPP – The Mobile Broadband Standard*. URL: https://www.3gpp.org/technologies/edge-app

8. Predictions for 2024 – 3GPP and Ambient IoT. *Electronics Weekly*. URL: https://www.electronicsweekly.com/news/design/communications/predictions-for-2024-3gpp-and-ambient-iot-2023-12/

9. IEEE Xplore Full-Text PDF:. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10258086

10. Rajab H., Cinkler T. Enhanced Energy Efficiency and Scalability in Cellular Networks for Massive IoT. *SpringerLink*. URL: https://link.springer.com/chapter/10.1007/978-981-99-3668-7_13

11. Thieme W. Council Post: Top Five IoT Networking Challenges And How To Conquer Them. *Forbes*.

URL: https://www.forbes.com/sites/forbestechcouncil/2020/07/16/top-five-iot-networking-challenges-and-how-to-conquer-them/?sh=7d1c85bf3a33

12. 3GPP – The Mobile Broadband Standard. *3GPP*. URL: http://www.3gpp.org

13. Internet of Things (IoT) Platform | Wiliot. *Wiliot*. URL: https://www.wiliot.com/

14. LTE-M vs NB-IoT – A Guide Exploring the Differences between LTE-M and NB-IoT. *Telenor IoT*. URL: https://iot.telenor.com/iot-insights/lte-m-vs-nb-iot-guide-differences

15. Welcome to the World of Standards!. *ETSI*. URL: https://www.etsi.org

16. AI/ML for NR Air Interface. *3GPP – The Mobile Broadband Standard*. URL: https://www.3gpp.org/technologies/ai-ml-nr

17. IoT (інтернет речей) для бізнесу від Київстар . *Мобільний зв'язок від Київстар | Національний оператор мобільного зв'язку*. URL: https://kyivstar.ua/business/products/iot-for-business

18. NB-IoT (Narrowband Internet of Things) | Vodafone. *Vodafone для бізнесу*. URL: https://business.vodafone.ua/produkty/iot/nb-iot

19. IoT lifecell. *IoT lifecell*. URL: https://iot.lifecell.ua/

20. Учасники проектів Вікімедіа. Raspberry Pi – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Raspberry_Pi

21. Знакомство с GPIO в Raspberry Pi, подключение светодиода и кнопки, программа на Python. *Ph0en1x.net - информационная безопасность, программирование, радиоэлектроника, лайфхак и полезные фишки*. URL: https://ph0en1x.net/86-raspberry-pi-znakomstvo-s-gpio-perekluchatel-i-svetodiod.html

22. Модуль зв'язку NB-IoT/Cat-M/EDGE/GPRS/GNSS на SIM7000E до Raspberry Pi купити в Києві та Україні. *Arduino в Україні*. URL: https://arduino.ua/prod3019-modyl-svyazi-nb-iotemtcedgegprsgnss-na-sim7000e-dlya-raspberry-pi

23. SIM7000E-NB-IoT-HAT Manual. *Waveshare*. URL: https://files.waveshare.com/upload/7/76/SIM7000E-NB-IoT-HAT-Manual-EN.pdf

ДОДАТКИ

ДОДАТОК А

ЛАБОРАТОРНА РОБОТА
НАЛАШТУВАННЯ РІШЕННЯ IOT НА ОСНОВІ МОДУЛЯ ЗВ'ЯЗКУ 3GPP SIM7000E ТА МІКРОКОНТРОЛЕРА RASPBERRY PI

1. ВСТУПНА ЧАСТИНА

1. Мета роботи:

1) Ознайомитися з основами роботи модуля зв’язку SIM7000E та мікроконтролером Raspberry Pi для розробки рішень IoT.
2) Навчитися налаштовувати модуль зв’язку SIM7000E та мікроконтролер Raspberry Pi.
3) Ознайомитися з методами перевірки функціональності та ефективності модуля зв’язку, що дозволить гарантувати його надійність та стабільність роботи в реальних умовах.

2. Зміст роботи:

Розглядається процес налаштування модуля зв’язку SIM7000E, та тестування функцій.

Загальні відомості

Raspberry Pi - це лінійка компактних одноплатних комп’ютерів (SBC), створених Raspberry Pi Foundation у Великобританії у співпраці з Broadcom. Raspberry Pi містить усі елементи, що є в типовому ПК (процесор, пам’ять, USB-порти і тощо), може працювати з різними операційними системами і може бути використаний в широкому спектрі проектів, включаючи настільні комп’ютери, електроніку, робототехніку, ретро-ігри та багато іншого. Модуль зв’язку це одне з важливих доповнень Raspberry Pi. SIM7000E NB-IoT HAT - це модуль зв’язку, який підтримує технологій NB-IoT, Cat-M, EDGE та GPRS, а також має функцію GNSS позиціювання. Його компактність, низька затримка та широкий радіус дії

роблять його чудовим вибором для IoT-застосунків, включаючи розумні пристрої, відстеження активів, дистанційний моніторинг, е-здоров’я та інше.

Процес налаштування цих пристроїв, відбувається через інтерфейс командного рядка, де користувач вводить специфічні команди для контролю та налаштування пристроїв. Одним з ключових інструментів для цього є AT-команди, які використовуються для взаємодії з модулем зв’язку. AT-команди - це стандартний набір команд, які використовуються для контролю модемів. налаштування цих пристроїв. На таблиці 1 представлений список загальних AT-команд для налагодження NB-IoT.

Таблиця 1 – Список загальних AT-команд для налагодження NB-IoT

Команди	Опис	Повернення
AT+CGATT?	Перевірка стану GPRS приєднання	+CGATT:1
AT+CPSI?	Запит інформації про URS	+CPSI:
AT+CGDCONT?	Перевірка доступного APN	+CGDCONT:
AT+CSTT	Встановлення APN на CMNET	OK
AT+CIICR	Встановлення бездротового з’єднання з GPRS	OK
AT+CIFSR	Отримати локальну IP адресу	OK
AT+CIPSTART	Режим: “IP”, Тип: “”, Адреса: Remote server IP address; Порт: Remote server port	CONNECT
AT+CIPSEND	Надсилання даних	OK

2. АЛГОРИТМ ВИКОНАННЯ РОБОТИ

1. Завантажте образ операційної системи Raspbian OS з офіційного сайту і запишіть його на SD-карту за допомогою спеціального програмного забезпечення.
2. Вставте SD-карту в слот для карт пам’яті Raspberry Pi.
3. Підключіть всі необхідні периферійні пристрої.
4. Підключіться до мережі за допомогою вбудованого Wi-Fi модуля в Raspberry Pi.
5. Підключіть модуль SIM7000E NB-IoT HAT до Raspberry Pi. Вставте SIM-карту в слот SIM7000E NB-IoT HAT. Потім підключіть GSM-антену до модуля. Підключіть модуль SIM7000E NB-IoT HAT до GPIO портів Raspberry Pi. Також підключіть USB інтерфейс модуля до Raspberry Pi за допомогою мікро USB кабелю.
6. Оновіть систему. Відкрийте вікно терміналу та введіть наступні команди: sudo apt-get update та sudo apt-get upgrade.
7. Виконайте конфігурацію інтерфейсів. Увімкніть зв’язок через послідовний порт.
8. Встановіть minicom для вашої системи. Відкрийте вікно терміналу та введіть команду: sudo apt-get install minicom.
9. Завантажте демо-коди. Вони надають приклади того, як програмувати та взаємодіяти з модулем за допомогою Raspberry Pi.
10. Додайте команду в файл rc.local. Введіть команду sh /home/pi/SIM7000X-Demo/Raspberry/c/sim7000_init на рядку між: fi та exit. Збережіть зміни.
11. Виконайте тестування.

3. ПРИКЛАД ВИКОНАННЯ РОБОТИ

Першим кроком є завантаження образу операційної системи Raspbian OS з офіційного сайту і запис його на SD-карту за допомогою спеціального

програмного забезпечення, наприклад, Balena Etcher. Після завершення запису, SD-карту можна вставити в слот для карт пам’яті Raspberry Pi. Після цього нам необхідно підключити всі необхідні периферійні пристрої: монітор (через HDMI), клавіатуру і мишу (через USB). З вбудованим Wi-Fi модулем в Raspberry Pi 3, ми можемо підключитися до мережі. Для цього нам потрібно відкрити налаштування Wi-Fi в графічному інтерфейсі Raspbian OS і вибрати потрібну мережу. Після цього ввести пароль мережі для підключення. Також, можна змінити стандартний пароль користувача Raspberry Pi для забезпечення безпеки вашого пристрою.

Наступним кроком буде підключення модуля SIM7000E NB-IoT HAT до Raspberry Pi. Для цього спочатку вставляється SIM-карта в слот SIM7000E NB-IoT HAT. Це дозволить модулю з’єднатися з мережею за допомогою мобільного зв’язку. Потім підключається GSM-антена до модуля, яка забезпечує прийом та передачу сигналів мобільного зв’язку.

Після цього модуль SIM7000E NB-IoT HAT підключається до GPIO портів Raspberry Pi. А також, підключається USB інтерфейс модуля до Raspberry Pi за допомогою мікро USB кабелю. Це дозволяє Raspberry Pi та модуль SIM7000E NB-IoT HAT обмінюватися даними.

Після підключення модуля зв’язку SIM7000E NB-IoT HAT до Raspberry Pi, потрібно оновити систему. Це важливий етап, оскільки оновлення системи забезпечує наявність найновіших пакетів та безпеки. Для цього відкриваємо вікно терміналу та вводимо наступні команди: sudo apt-get update, яка синхронізує вашу систему з серверами пакетів, щоб вона знала про всі доступні оновлення та sudo apt-get upgrade, яка потім встановлює ці оновлення.

Після оновлення системи потрібно виконати конфігурацію інтерфейсів, нам потрібно увімкнути зв'язок через послідовний порт, це те мікроконтролер та модуль зв’язку будуть спілкуватися між собою. Знову відкриваємо вікно терміналу та вводимо команду sudo raspi-config, як зображено на рисунку 1 та натискаємо Enter, після цього ми побачимо меню, в якому нам потрібно вибрати Interfacing Options та натиснути Enter, ми потрапляємо в більш детальне меню в

якому обираємо Serial Port, після цього натискаємо No далі Yes. Після цього Raspberry Pi потрібно перезавантажити для застосування змін.

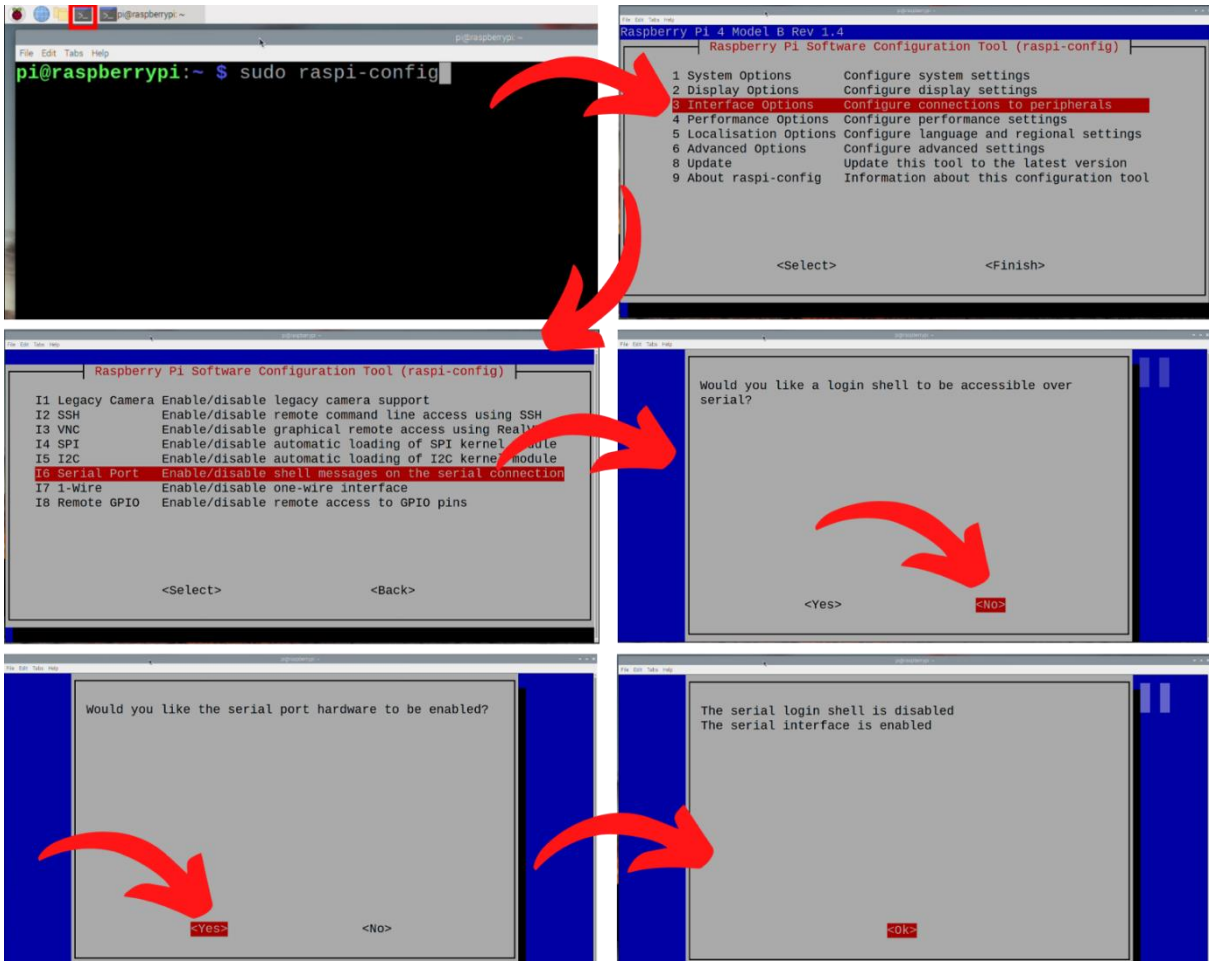

Рисунок 1 – Конфігурацію інтерфейсів

Після перезавантаження, ми повертаємося на робочий стіл. Тепер нам потрібно встановити minicom для нашої системи. Minicom – це програма послідовного зв’язку. Ми знову відкриваємо вікно терміналу та вводимо наступну команду (рисунок 2): sudo apt-get install minicom, тиснемо Enter. Далі ми побачимо запитання, чи хочемо ми продовжити – тиснемо Y та Enter, щоб продовжити процес.

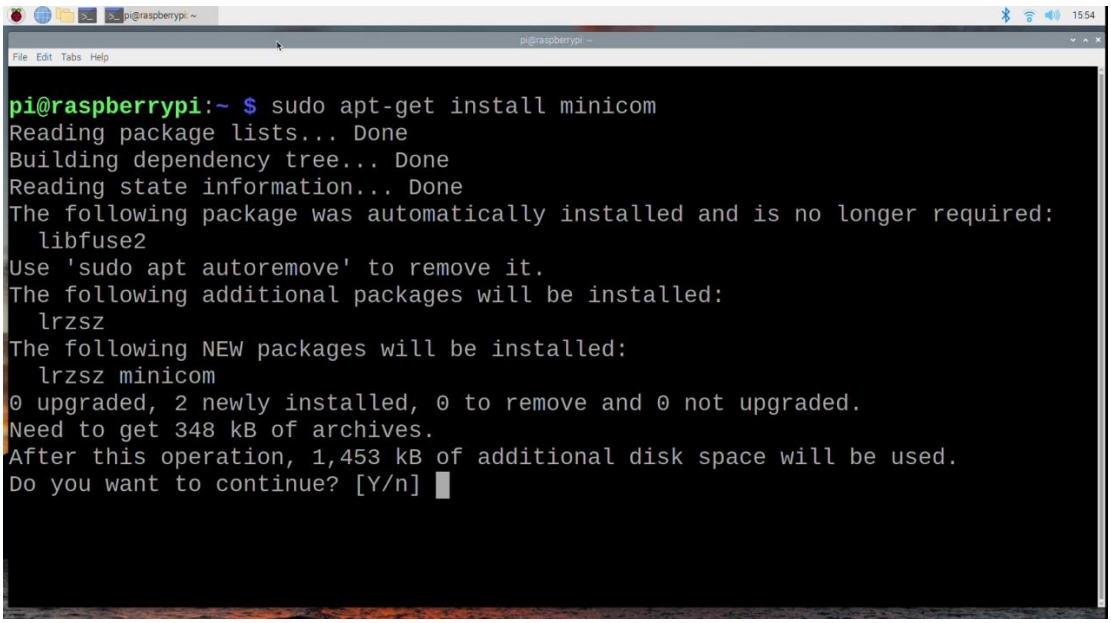

Рисунок 2 – Встановлення minicom

Тепер нам потрібно завантажити демо – коди. Для того, аби завантажити zip-файл з прикладами кодів та драйверів для роботи модуля зв'язку нам необхідно відкрити нове вікно терміналу та ввести наступну команду: wget https://files.waveshare.com/upload/2/24/SIM7000X-Demo.7z. Після завершення, в цьому ж вікні ми послідовно вводимо наступні команди:

- sudo apt-get install p7zip-full
- 7z x SIM7000X -Demo.7z -r -o/home/pi
- sudo chmod 777 -R /home/pi/SIM7600X-4G-HAT-Demo
- sudo nano /etc/rc.local

Після введення останнього рядку, у нас відкриється нова сторінка (файл | rc.local |). Нам потрібно буде додати команду в | rc.local | файл. Наступну команду ми повинні ввести на рядку між: fi та exit. Текст команди буде наступним: sh /home/pi/SIM7000X-Demo/Raspberry/c/sim7000_init. Після цього натискаємо Ctrl+X , далі Y , а потім клавішу Enter , щоб зберегти зміни. Виконання цієї команди означає, що драйвери запускатимуться під час завантаження Raspberry Pi. На рисунку 3, ці дії зображені послідовно.

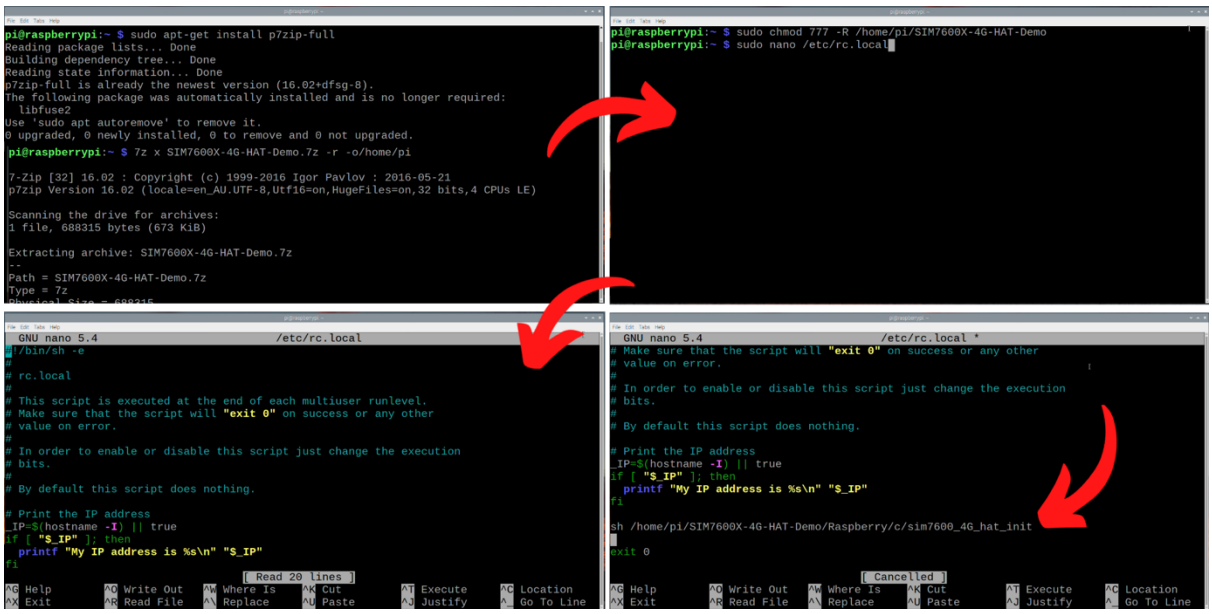

Рисунок 3 – Завантаження демо-кодів

Тепер нам знову потрібно відкрити нове вікно терміналу, та ввести кожну з поданих нижче команд по черзі. Перша команда направить фокус на папку bcm2835, де знаходиться драйвер: cd /home/pi/SIM7000X-Demo/Raspberry/c/bcm2835. Наступна команда надасть доступ та активує драйвер: chmod +x configure && ./configure && sudo make && sudo make install. На цьому етапі, ми повністю налаштували модуль зв’язку для роботи з мікроконтролером.

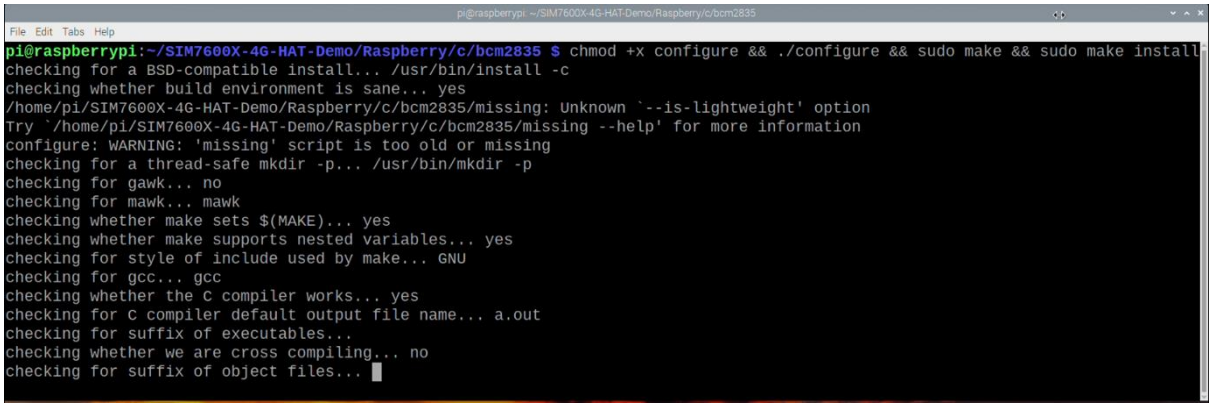

Рисунок 4 – BCM2835 бібліотека

Після закінчення повноцінного процесу налаштування, нам потрібно перевірити справність роботи наших пристроїв. Найпростішим варіантом буде використати AT-команди для перевірки зв'язку з модулем. AT-команди

дозволяють взаємодіяти з модулем зв'язку, надсилаючи текстові команди через серійний інтерфейс.

Для цієї задачі виконаємо сценарій | AT.py |, відкривши його за таким маршрутом: /home/pi/SIM7000X-Demo/Python/AT. Клацнувши на файл потрібно вибрати пункт відкрити за допомогою Thonny IDE. Після відкриття файлу AT.py в Thonny IDE, вам потрібно буде виконати цей сценарій. Це можна зробити, натиснувши кнопку “Виконати” або використавши комбінацію клавіш F5.

Після виконання сценарію, ви повинні побачити відповідь модуля на AT-команди в консолі Thonny IDE. Якщо модуль відповідає на AT-команди, це означає, що він працює правильно.

Також ви можете використати AT-команду для перевірки рівня сигналу (AT+CSQ), для перевірки стану реєстрації в мережі (AT+CREG?), або будь-яку з команд наданих в теоретичних відомостях до цієї лабораторної роботи. Це допоможе вам переконатися, що модуль зв’язку SIM7000E правильно підключений до мережі.

4. КОНТРОЛЬНІ ПИТАННЯ

1. Які методи тестування можна використовувати для перевірки функціональності та ефективності модуля зв’язку SIM7000E?
2. Які основні характеристики мікроконтролера Raspberry Pi?
3. Які можливості надає модуль зв’язку SIM7000E для розробки рішень IoT?
4. Які основні застосування модуля зв’язку SIM7000E в реальних умовах?
5. Чому Raspberry Pi часто використовується в якості мікроконтролера для розробки рішень IoT?