ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Метод зовнішнього безпроводового керування автомобілем»

на здобуття освітнього ступеня магістра

зі спеціальності 172 Електронні комунікації та радіотехніка

освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

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

(підпис) Андрій ЗЕМЛЯНІКІН (Ім'я, ПРІЗВИЩЕ)

Виконав: здобувач вищої освіти
групи АРДМ-61
Андрій ЗЕМЛЯНІКІН

Керівник: Лариса ДАКОВА

Рецензент: Костянтин ЛАВРІНЕЦЬ

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра	Мобільних та відеоінформаційних технологій
Ступінь вищої освіти	Магістр
Спеціальність	172 Електронні комунікації та радіотехніка
Освітньо-професійна програма	Апаратура радіозв'язку, радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
« » _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Землянікіну Андрію Ігоровичу

1. Тема кваліфікаційної роботи: «Метод зовнішнього безпроводового керування автомобілем»,
керівник кваліфікаційної роботи Лариса ДАКОВА, к.т.н., доцент,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 15.10.2024 р. №320.

2. Строк подання кваліфікаційної роботи 25.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Wi-Fi модулі.
   2. Мікроконтролери.
   3. Засоби керування автомобілем.
   4. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Безпроводовий інтернет WiFi.
   2. Провадження протоколу WiFi у центральній системі керування автомобілем.
   3. Голосове керування через WiFi і nodemcu

4. Засоби безпеки та додаткові автомобільні пристрої

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання 27.10.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	27.10.24	Викон.
2.	Безпроводовий інтернет WiFi	31.10.24	Викон.
3.	Провадження протоколу WiFi у центральній системі керування автомобілем	15.11.24	Викон.
4.	Голосове керування через WiFi і nodemcu	29.11.24	Викон.
5.	Засоби безпеки та додаткові автомобільні пристрої	02.12.24	Викон.
6.	Висновки, вступ, реферат	11.12.24	Викон.
7.	Розробка презентації	18.12.24	Викон.

Здобувач вищої освіти Андрій ЗЕМЛЯНІКІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи Лариса ДАКОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 73 стор., 35 рис., 1 табл., 18 дж.

Мета роботи – є доведення ефективності використання технології Wi-Fi для реалізації керування автомобілем.

Об'єкт дослідження – процеси, системи та пристрої використовуючі технології Wi-Fi.

Предмет дослідження – принципи, моделі та методи використання технології Wi-Fi.

Короткий зміст роботи: у магістерській роботі досягнуто наступних результатів: у першому розділі проаналізовано архітектуру компонентів і стандартів мережі Wi-Fi, типів організації мереж та видів з'єднань, схема обміну даними між пристроями. У другому розділі досліджено принципи протокола WiFi в системі центрального керування автомобілем, а також роль Bright Box як постачальник рішень для підключених автомобілів. Протокол Wi-Fi у центральній системі керування автомобілем матиме вищу швидкість передачі даних, ширші сценарії застосування, сильнішу безпеку та глибоку інтеграцію з автономним керуванням. У третьому розділі розглянуто процес WiFi-робота із голосовим керуванням і NodeMCU. У четвертому розділі описано ключові етапи безпеки та додаткових автомобільних пристроїв, та створення концепції керування.

КЛЮЧОВІ СЛОВА: WI-FI МОДУЛІ, МІКРОКОНТРОЛЕР, ЗАСОБ КЕРУВАННЯ, ПРОТОКОЛ, РОБОТ З ГОЛОСОВИМ КЕРУВАННЯМ, РОЗУМНІ РИШЕННЯ

ABSTRACT

Text part of the master's qualification work: 73 pages, 35 pictures, 1 table, 18 sources.

The purpose of the work – is proof of the effectiveness of using Wi-Fi technology to implement car control.

Object of research – processes, systems and devices using Wi-Fi technologies.

Subject of research – principles, models and methods of using Wi-Fi technology.

Summary of the work: the following results were achieved in the master's thesis: in the first chapter, the architecture of Wi-Fi network components and standards, types of network organization and types of connections, data exchange scheme between devices was analyzed. The second chapter explores the principles of the WiFi protocol in the central control system of the car, as well as the role of Bright Box as a solution provider for connected cars. The Wi-Fi protocol in the car's central control system will have higher data rates, wider application scenarios, stronger security, and deeper integration with autonomous driving. In the third section, the WiFi robot process with voice control and NodeMCU is considered. The fourth chapter describes the key stages of safety and additional automotive devices, and the creation of the control concept.

KEYWORDS: WI-FI MODULES, MICROCONTROLLER, CONTROL TOOL, PROTOCOL, ROBOT WITH VOICE CONTROL, SMART SOLUTIONS

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Землянікін А.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Електронні комунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему: Метод зовнішнього безпроводового керування автомобілем

Кваліфікаційна робота і рецензія додаються.

В.о. директора ННІТ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Землянікін Андрій Ігорович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з програмно-апаратними засобами мобільного зв'язку, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Землянікіна Андрія Ігоровича на оцінку «відмінно» та присвоїти йому кваліфікацію «Магістр з електронних комунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Лариса ДАКОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Землянікін А.І.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедри
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Землянікіна Андрія Ігоровича

на тему: «Метод зовнішнього безпроводового керування автомобілем»

Актуальність:

Централізовані системи керування автомобілями стали однією з важливих функцій сучасних автомобілів. Щоб забезпечити кращий досвід роботи з користувачем і збільшити функціональність, все більше і більше центральних систем керування автомобілями починають підтримувати з'єднання WiFi. У кваліфікаційній роботі розповімо про протокол WiFi у системі центрального керування транспортним засобом, включаючи його принципи, програми та майбутні розробки.

Підключення Wi-Fi в автомобілі починає ставати все більш популярним як спосіб підключення як вбудованих пристроїв, так і пристроїв, що належать пасажирам. Але в машині не тільки wifi. Стандарт Bluetooth використовується протягом багатьох років для підключення смартфона до автомобільної функції гучного зв'язку.

Позитивні сторони:

1. Проведено аналіз структури мережі безпроводового доступу Wi-Fi.
2. Розглянуто можливості впровадження протоколу Wi-Fi у центральній системі керування автомобілем.

Недоліки:

1. Не проведено аналізу стандарту Bluetooth, що використовується автомобільної функції гучного зв'язку.
2. Не розглянуто етапи зборки робота із голосовим керуванням WiFi-NodeMCU.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота заслуговує оцінку «відмінно», а здобувач ЗЕМЛЯНІКІН Андрій Ігорович заслуговує присвоєння кваліфікації: «Магістр з електронних комунікацій та радіотехніки».

Рецензент: КТН, доцент каф. ТСМ _____ Костянтин ЛАВРІНЕЦЬ
(науковий ступінь, вчене звання) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ЗМІСТ

ВСТУП 9
1 БЕЗПРОВОДОВИЙ ІНТЕРНЕТ WI-FI 11
1.1. Структура мережі безпроводового доступу Wi-Fi 11
1.1.1. Інфраструктурна топологія 12
1.1.2. Спеціальна топологія мережі 13
1.1.3. Топологія безпроводової сітки 14
1.1.4. P2P мережева топологія 15
1.2. Аналіз стандартів доступу до мережі Wi-Fi сімейства IEEE 802.11 16
1.2.1. Базовий стандарт IEEE 802.11 22
1.2.2. 802.11a (Wi-Fi 2) 23
1.2.3 802.11b (Wi-Fi 1) 23
1.2.4 802.11g (Wi-Fi 3) 24
1.2.5 802.11n (Wi-Fi 4) 24
1.2.6 IEEE 802.11ac (гігабітний WiFi або WiFi 5) 25
1.2.7 IEEE 802.11ad (WiGig) 25
1.3 Аналіз протоколів захисту мереж безпроводового доступу Wi-Fi 26
1.4 Новизна розвитку сімейства IEEE 802.11 26
1.4.1. Етапи розробки 27
1.4.2. Новизна протоколу 28
2 ВПРОВАДЖЕННЯ ПРОТОКОЛУ WIFI У ЦЕНТРАЛЬНІЙ СИСТЕМІ КЕРУВАННЯ АВТОМОБІЛЕМ 30
2.1 Принципи протоколу WiFi в системі центрального керування автомобіля 30
2.2 Модульний підхід до безпроводових технологій 33
2.3 Автомобільні точки доступу Wi-Fi 41
2.4 Роль Bright Box у галузі автомобільного Wi-Fi 47
3 ГОЛОСОВЕ КЕРУВАННЯ ЧЕРЕЗ WIFI І NODEMCU 49
3.1 WiFi-робот із голосовим керуванням і NodeMCU 49
3.2 H-Bridge L293D 50
3.3 Додаток для Android 55

4 ЗАСОБИ БЕЗПЕКИ ТА ДОДАТКОВІ АВТОМОБІЛЬНІ ПРИСТРОЇ 58
4.1 Viper DS4 58
4.2 Протиугінна сигналізація ESP32 59
4.3 Домашній помічник і ESPhome .....
4.4 Автомобільний резервний датчик 68
4.5 Створення концепції керування 69
ВИСНОВКИ 74
ПЕРЕЛІК ПОСИЛАНЬ 75
ДЕМОНСТРАТИВНІ МАТЕРІАЛИ 77

ВСТУП

Існуюча тенденція використання технології Wi-Fi, приводить до того, що користувачі мають безпосередній безпроводовий високошвидкісний доступ до Інтернету. Різкий зріст придбаних приладів для використання Wi-Fi удома, або у інших містах безпосереднього скупчення людей, дозволяє користувачам мати постійний та стабільний доступ до мережі інтернет не залежно від покриття та стабільності стільникового зв'язку.

Все більше з'являється приладів які використовують Wi-Fi з'єднання. Побутові прилади оснащуються процесорами, та програмним забезпечення з підтримкою Wi-Fi, що в свою чергу дозволяє користувачу керувати приладами, та об'єднувати їх у суцільну екосистему. Прилади побутового призначення, системи безпеки, системи доступу до мережі інтернет, кліматичні системи та інші – мають змогу керуватися за допомогою мобільних пристроїв через спеціальне програмне забезпечення, та потребують Wi-Fi з'єднання.

Оскільки стандарти з'єднання Wi-Fi постійно розвиваються, у зв'зку з цим можна вважати, що ця технологія має перспективне призначення у використанні у майбутньому і не може розглядатися як застаріла.

Централізовані системи керування автомобілями стали однією з важливих функцій сучасних автомобілів. Щоб забезпечити кращий досвід роботи з користувачем і збільшити функціональність, все більше і більше центральних систем керування автомобілями починають підтримувати з'єднання WiFi. У кваліфікаційній роботі розповімо про протокол WiFi у системі центрального керування транспортним засобом, включаючи його принципи, програми та майбутні розробки.

Підключення Wi-Fi в автомобілі починає ставати все більш популярним як спосіб підключення як вбудованих пристроїв, так і пристроїв, що належать пасажирам. Але в машині не тільки Wi-Fi. Стандарт Bluetooth використовується протягом багатьох років для підключення смартфона до автомобільної функції гучного зв'язку.

Планується, що Bluetooth і надалі стане ключовим засобом для низки автомобільних додатків, від передачі аудіо до стереосистеми автомобіля, до використання смартфона для розблокування дверей автомобіля. З цих причин при розробці безпроводового підключення для автомобільних додатків Wi-Fi і Bluetooth є ключовими.

Мета роботи – є доведення ефективності використання технології Wi-Fi для реалізації керування автомобілем.

Об'єкт дослідження – процеси, системи та пристрої використовуючі технології Wi-Fi.

Предмет дослідження – принципи, моделі та методи використання технології Wi-Fi.

1 БЕЗПРОВОДОВИЙ ІНТЕРНЕТ WI-FI

1.1. Структура мережі безпроводового доступу Wi-Fi

За останні кілька років поширення безпроводових мереж Wi-Fi було сильним, тому розробники розглядають можливість винайдення, виробництва та впровадження нових стандартів зв'язку, які, на відміну від своїх попередників, будуть більш продуктивними, ефективними та безпечними. На початку свого існування безпроводові пристрої могли підтримувати швидкість передачі даних вище 1-2 Мбіт/с, що є незначним порівняно з поточними. У сучасному світі швидкість передачі інформації в безпроводових мережах може досягати 1 Гбіт/с а то і більше, що неминуче призводить до конкуренції за дротові мережі. Існує багато типів безпроводових мереж, кожна з яких відрізняється від свого попередника різними параметрами – швидкістю передачі даних, діапазоном і типом кодування інформації.

Безпроводова локальна мережа(Wi-Fi), заснована на стандартах серії IEEE 802.11. На ранніх етапах свого існування термін «Wi-Fi» використовувався лише для позначення технології, яка забезпечувала зв'язок у діапазоні частот вище 2,4 ГГц, але зараз він використовується для бездротових мереж та інших технологій. Мережа Wi-Fi використовується для зв'язку та обміну даними між вузлами, але це гнучка система обміну інформацією, яка працює як альтернативна дротова мережа, розташована в приміщенні або на відкритій території. Мережа також використовується для організації публічних точок доступу, таких як аеропорти, площі та для інших місць скупчення людей, а також для організації тимчасових без безпроводових мереж для проведення фестивалів, футбольних матчів або музейних виставок.

Для побудови мереж безпроводового доступу інженери користуються мережевими топологіями, кожна з який адаптується під середовище. Мережі безпроводового доступу мають декілька мережевих топологій [14]:

- Інфраструктурна топологія мережі;
- Спеціальна топологія мережі;
- Топологія бездротової сітки;
- P2P мережева топологія.

В майбутньому зросте популярність інших топологій безпроводових домашніх мереж. З ростом обсягів трафіку розміщення додаткових роутерів або точок доступу допоможе обслуговувати більше клієнтів і передавати великі обсяги даних рис. 1.1. Ця нова Mesh-мережі (mesh network) розширює ефективність безпроводової мережі за рахунок використання деяких технологій, які вже застосовуються в офісах, лікарнях і університетських містечках.

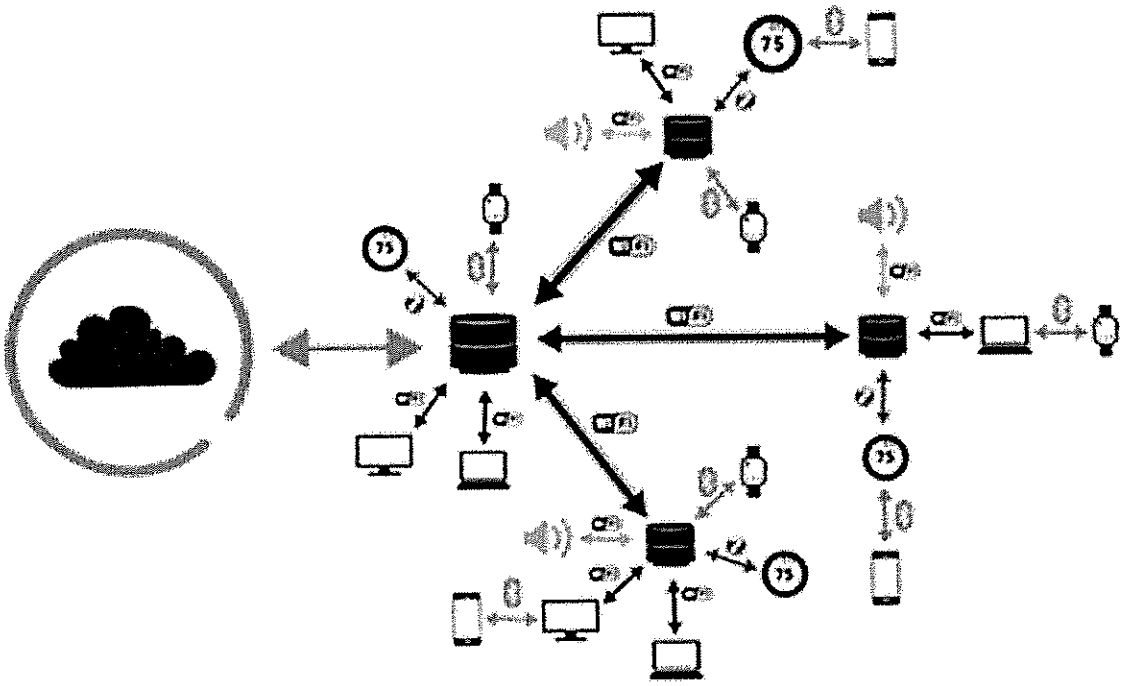


Рис. 1.1 Архітектура безпроводової мережі

1.1.1. Інфраструктурна топологія

На рис. 1.2 зображена інфраструктурна топологія:

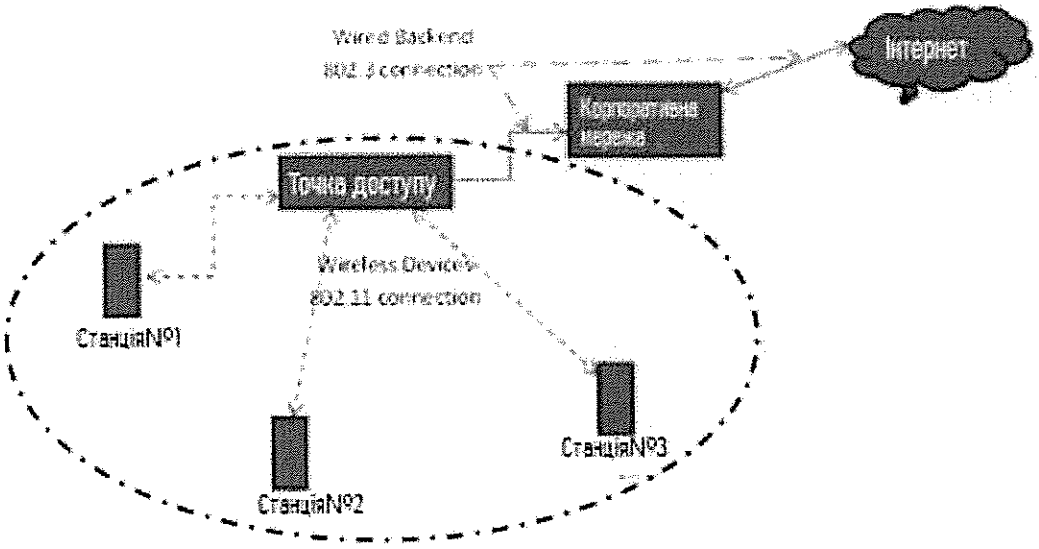


Рис. 1.2. Топологія інфраструктурної мережі

Область, яка позначена пунктирним лінією замкнуту в коло, називається базовим набором послуг (BSS). Всі станції, що підключені до точки доступу, утворюють базовий сервісний набір.

Також існує ще базова зона обслуговування (BSA). Основна зона обслуговування - це зона, яка охоплена точкою доступу. Сигнал точки доступу може виходити за межі діапазону підключених до нього пристроїв. Ця зона покриття – являється BSA.

1.1.2. Спеціальна топологія мережі

Спеціальна топологія зображена на рис.1.3 є самодостатньою мережею Peer-to-Peer. Тобто, це мережа без точки доступу, в якій пристрої не тільки являються кінцевими точками, а й маршрутизаторами. Це показано нижче:

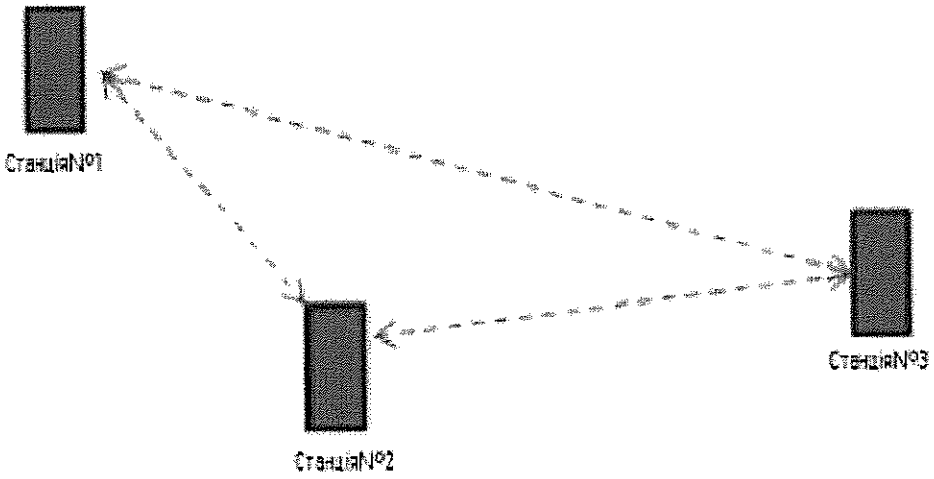


Рис. 1.3. Спеціальна топологія мережі

1.1.3. Топологія безпроводової сітки

Мережа Wireless Mesh - це взаємозв'язок підключених вузлів, які утворюють самостійну мережу. Якщо один вузол мережі «падає», то формується новий шлях для створення мережі, що працює. Сітчасті вузли використовують стандарти 802.11, щоб спілкуватись один з одним.

Резервний сітчастий вузол також може бути налаштований для підключення до загальнодоступного шлюзу, якщо первинний сітчастий вузол опуститься. До будь-якого мережевого вузла можуть бути підключені користувачі.

Навантаження на мережевий трафік потрібно збалансувати між різними вузлами та створити ефективні механізми маршрутизації, щоб забезпечити найшвидший шлях до загальнодоступної мережі. На рис. 1.4 зображена мережа безпроводової локальної мережі.

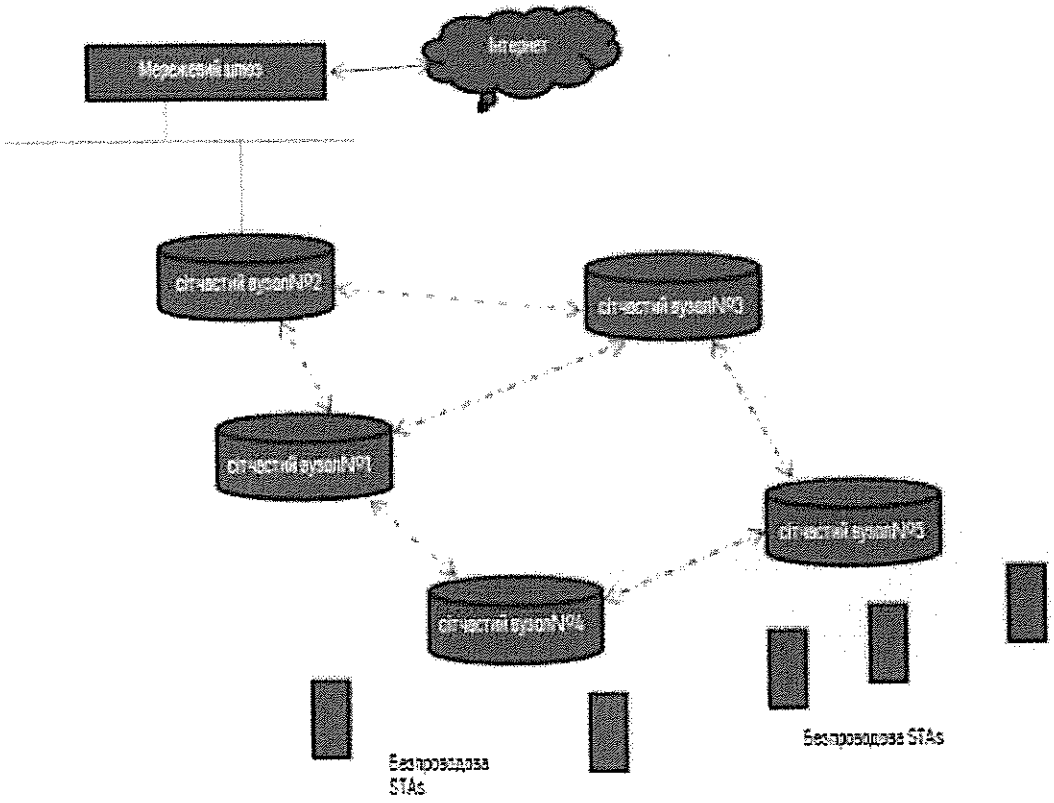


Рис. 1.4 Мережа безпроводової локальної мережі

1.1.4. P2P мережева топологія

Мережа P2P - це мережа Peer-to-Peer в якій одна бездротова станція виконує роботу бездротової головної станції. Головна станція розсилає маяки і відповідає за підтримку мережі Peer to Peer. Інші бездротові станції підключаються до власника групи.

Клієнтську станцію називають груповими клієнтами. Коли власник групи покидає мережу, клієнт групи прийме роль власника групи. Пристрій власника групи також може одночасно приєднатися як пристрій групового клієнта до іншої мережі P2P, якщо він підтримує кілька радіостанцій 802.11[8].

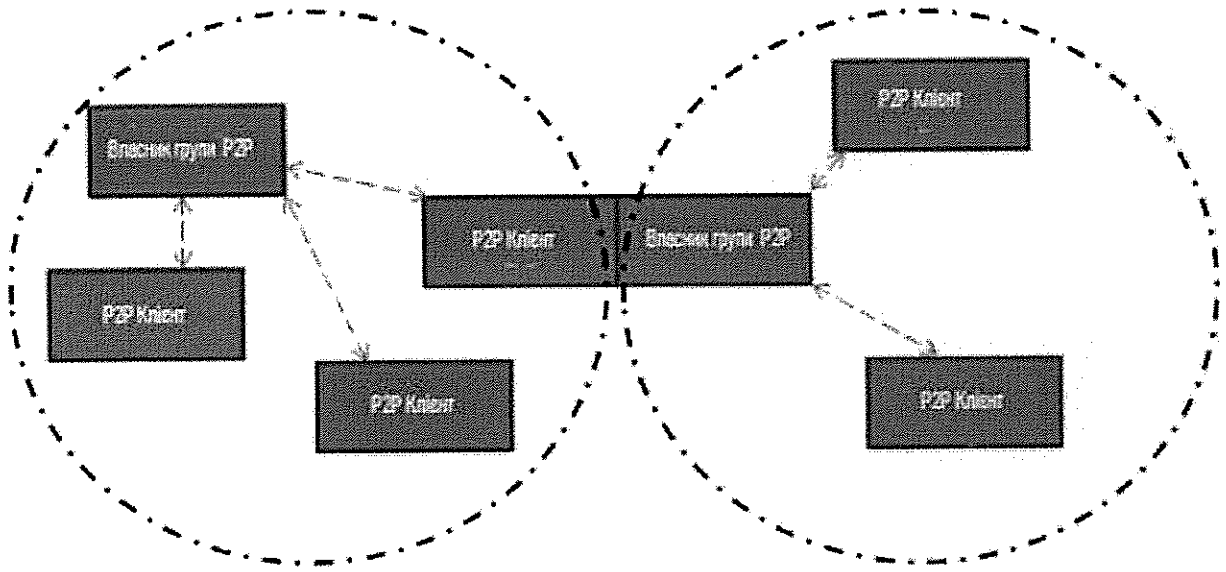


Рис. 1.5 Топологія мережі P2P

1.2. Аналіз стандартів доступу до мережі Wi-Fi сімейства IEEE 802.11

У 1990 році IEEE 802 створив групу для вивчення стандартів для бездротових мереж Wi-Fi. Їхнє головне завдання — створити загальний стандарт для мереж, що працюють у діапазоні частот 2,4 ГГц зі швидкістю з'єднання 1-2 Мбіт/с. У 1997 році була завершена розробка стандарту і була затверджена перша специфікація 802.11.

Цей стандарт вважається першим стандартом для обладнання WLAN. Однак початкова швидкість передачі інформації на той момент не відповідала побажанням користувачів. Саме тому, щоб задовольнити всіх користувачів і зробити технологію популярною, розробники створили новий стандарт. А восени 1999 року були затверджені удосконалення існуючих стандартів.

На сьогодення існує велика кількість стандартів групи IEEE 802.11. Розглянемо найбільш розповсюдженні і найбільш вживані:

1. Базовий 802.11;
2. IEEE 802.11a (Wi-Fi 2);
3. IEEE 802.11b (Wi-Fi 1);

4. IEEE 802.11g (Wi-Fi 3);

5. IEEE 802.11n (Wireless-N чи Wi-Fi 4);

6. IEEE 802.11ac (гігабітний WiFi або WiFi 5);

7. IEEE 802.11ax (WiFi 6 або високоефективна WLAN).

Всі стандарти IEEE 802.11 працюють на нижніх двох рівнях моделі ISO / OSI, фізичному та канальному, тому будь-який мережевий додаток, мережева операційна система, або протокол (наприклад, TCP / IP), будуть так само добре працювати в мережі 802.11, як і в мережі Ethernet [8].

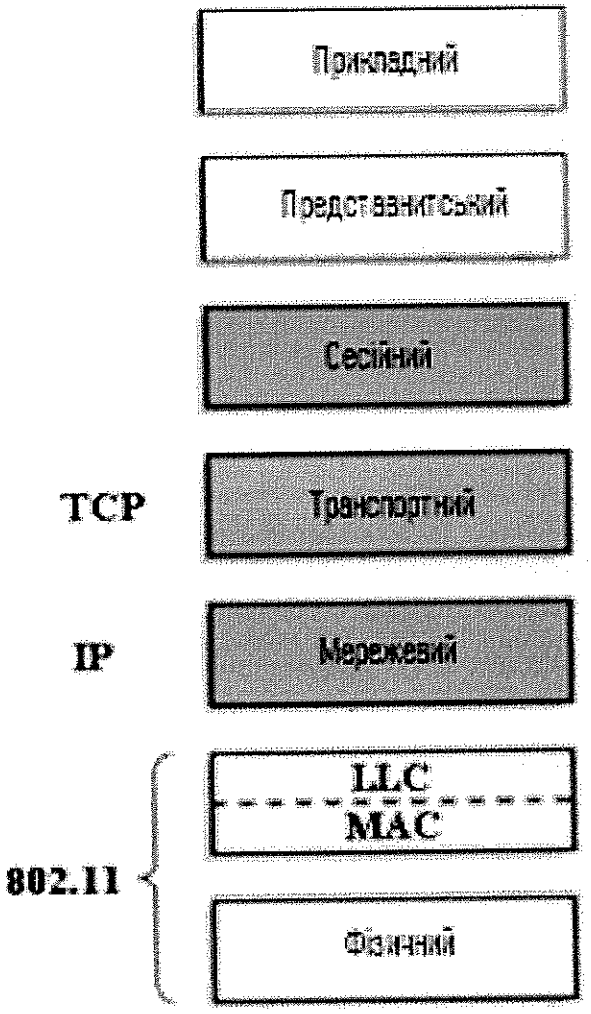


Рис. 1.6 Рівні моделі ISO / OSI і їх відповідність стандарту 802.11

Фізичний рівень IEEE 802.11.

Стандарт IEEE 802.11 передбачає передачу сигналу одним з двох методів - прямий послідовності (Direct Sequence Spread Spectrum, DSSS) і частотних стрибків (Frequency Hopping Spread Spectrum, FHSS) розрізняються способом модуляції, але використовують одну і ту ж технологію розширення спектру. Основний принцип технології розширення спектру (Spread Spectrum, SS) полягає в тому, щоб від вузькосмугового спектру сигналу, що виникає при звичайному потенційному кодуванні, перейти до широкосмугового спектру, що дозволяє значно підвищити стійкість переданих даних.

Метод FHSS передбачає зміну несучої частоти сигналу при передачі інформації. Для підвищення завадостійкості потрібно збільшити спектр переданого сигналу, для чого несуча частота змінюється по псевдовипадковому закону, і кожен пакет даних передається на своїй частоті. При використанні FHSS конструкція приймача виходить дуже простою, але цей метод можна застосовувати, тільки якщо пропускна здатність не перевищує 2 Мбіт/с, так що в доповненні IEEE 802.11b залишився один DSSS. З цього випливає, що спільно з пристроями IEEE 802.11b може застосовуватися тільки те обладнання стандарту IEEE 802.11, яке підтримує DSSS, при цьому швидкість передачі не перевищить максимальної швидкості в "вузькому місці" (2 Мбіт/с), яким є обладнання, що використовує старий стандарт без розширення.

В основі методу DSSS лежить принцип фазової маніпуляції (тобто передачі інформації стрибкоподібною зміною початкової фази сигналу). Для розширення спектру сигналу застосовується перетворення переданої інформації в так званий код Баркера, який є псевдовипадковою послідовністю. На кожен рухаючий біт доводиться 11 біт в послідовності Баркера. Розрізняють пряму і инверсну послідовності Баркера. Через велику надмірність при кодуванні ймовірність того, що дія перешкоди перетворить пряму послідовність Баркера в инверсну, близька до нуля. Поодинокі біти передаються прямим кодом Баркера, а нульові - інверсним.

Під бездротові комп'ютерні мережі в діапазоні 2,4 ГГц відведений досить вузький "коридор" шириною 83 МГц, розділений на 14 каналів. Для виключення

взаємних перешкод між каналами необхідно, щоб їх смуги відстояли один від одного на 25 МГц. Нескладний підрахунок показує, що в одній зоні одночасно можуть використовуватися тільки три канали. В таких умовах неможливо вирішити проблему відбудови від перешкод автоматичною зміною частоти, ось чому в бездротових локальних мережах використовується кодування з високою надмірністю. У ситуації, коли і цей захід не дозволяє забезпечити задану достовірність передачі, швидкість з максимального значення 11 Мбіт / с послідовно знижується до одного з наступних фіксованих значень: 5,5; 2; 1 Мбіт/с. Зниження швидкості відбувається не тільки при високому рівні перешкод, але і якщо відстань між елементами бездротової мережі досить велика.

Канальний рівень IEEE 802.11.

Подібно провідної мережі Ethernet, в бездротових комп'ютерних мережах Wi-Fi канальний рівень включає в себе підрівні управління логічним з'єднанням (Logical Link Control, LLC) і управління доступом до середовища передачі (Media Access Control, MAC). У Ethernet і IEEE 802.11 один і той же LLC, що значно спрощує об'єднання дротяних і бездротових мереж. MAC у обох стандартів має багато спільного, однак є деякі тонкі відмінності, принципові для порівняння дротяних і бездротових мереж.

У Ethernet для забезпечення можливості множинного доступу до загального середовища передачі (в даному випадку кабелю) використовується протокол CSMA/CD, що забезпечує виявлення і обробку колізій (в термінології комп'ютерних мереж так називаються ситуації, коли кілька пристроїв намагаються почати передачу одночасно).

У мережах IEEE 802.11 використовується напівдуплексний режим передачі, тобто в кожен момент часу станція може або приймати, або передавати інформацію, тому виявити колізію в процесі передачі неможливо. Для IEEE 802.11 був розроблений модифікований варіант протоколу CSMA / CD, який отримав назву CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance). Працює він у такий спосіб. Станція, яка збирається передавати інформацію, спочатку "слухає ефір". Якщо не виявлено активності на робочій частоті, станція спочатку

чекає протягом деякого випадкового проміжку часу, потім знову "слухає ефір" і, якщо середовище передачі даних все ще вільне, здійснює передачу. Наявність випадкової затримки необхідно для того, щоб мережа не зависла, якщо кілька станцій одночасно захочуть отримати доступ до частоти. Якщо інформаційний пакет приходить без спотворень, приймаюча станція посилає назад підтвердження. Цілісність пакету перевіряється методом контрольної суми. Отримавши підтвердження, передавальна станція вважає процес передачі даного інформаційного пакету завершеним. Якщо підтвердження не отримане, станція вважає, що сталася колізія, і пакет передається знову через випадковий проміжок часу.

Ще одна специфічна для бездротових мереж проблема - дві клієнтські станції мають поганий зв'язок одна з одним, але при цьому якість зв'язку кожної з них з точкою доступу гарна. В такому випадку клієнтська станція може надіслати на точку доступу запит на очищення ефіру. Тоді по команді з точки доступу інші клієнтські станції припиняють передачу на час "спілкування" двох точок з поганим зв'язком. Режим примусового очищення ефіру (протокол Request to Send / Clear to Send - RTS / CTS) реалізований далеко не у всіх моделях обладнання IEEE 802.11 і, якщо він є, то включається лише в крайніх випадках.

У Ethernet при передачі потокових даних використовується управління доступом до каналу зв'язку, розподілене між усіма станціями. Навпаки, в IEEE 802.11 в таких випадках застосовується централізоване управління з точки доступу. Клієнтські станції послідовно опитуються на предмет передачі потокових даних. Якщо яка-небудь із станцій повідомляє, що вона буде передавати потокові дані, точка доступу виділяє їй проміжок часу, в який з усіх станцій мережі передаватиме тільки вона.

Слід зазначити, що примусове очищення ефіру знижує ефективність роботи бездротової мережі, оскільки пов'язана з передачею додаткової службової інформації і короткочасними перервами зв'язку. Крім цього, в провідних мережах Ethernet при необхідності можна реалізувати не тільки напівдуплексний, але і двобічний варіант передачі, коли колізія виявляється в процесі передачі (це

підвищує реальну пропускну здатність мережі). Тому, на жаль, при інших рівних умовах реальна пропускна здатність бездротової мережі IEEE 802.11b буде нижче, ніж у проводового Ethernet. Таким чином, якщо мережа Ethernet 10 Мбіт/с і IEEE 802.11b (максимальна швидкість передачі інформації 11 Мбіт/с) з однаковим числом користувачів даватиме однакове навантаження, поступово збільшуючи її, то, починаючи з деякого порога, мережа IEEE 802.11b почне "гальмувати ", а Ethernet все ще буде функціонувати нормально.

Оскільки клієнтські станції можуть бути мобільними пристроями з автономним живленням, в стандарті IEEE 802.11 велика увага приділена питанням управління живленням. Зокрема, передбачено режим, коли клієнтська станція через певні проміжки часу "прокидається", щоб прийняти сигнал включення, який, можливо, передає точка доступу. Якщо цей сигнал прийнятий, клієнтський пристрій включається, в іншому випадку воно знову "засипає" до наступного циклу прийому інформації.

З усіх існуючих стандартів бездротової передачі даних IEEE 802.11, на практиці найбільш часто використовуються всього три, це: 802.11g , 802.11 n і 802.11ac, зображено на таблиці 1.1.

Таблиця 1.1

Порівняння типових стандартів бездротової передачі

Стандарт	802.11b	802.11g	802.11a
Кількість використовуваних радіоканалів	3 що не перекриваються	3 що не перекриваються	8 що не перекриваються
Частотний діапазон	2.4 ГГц	2.4 ГГц	5 ГГц
Макс. швидкість передачі даних	11 Мб/с	54 Мб/с	54 Мб/с
Приблизна відстань дії	30 м при 11 Мб/с 100 м при 1 Мб/с	15 м при 54 Мб/с 50 м при 11 Мб/с	12 м при 54 Мб/с 100 м при 6 Мб/с

1.2.1. Базовий стандарт IEEE 802.11

В середині літа 1997 року був оприлюднений стандарт IEEE 802.11 який мав назву «Специфікація фізичного рівня і рівня контролю доступу до каналу передачі бездротових локальних мереж». Цей протокол ідентифікував архітектуру мережі, формати пакетів, способи захисту даних та автентифікацію, а також різні принципи доступу пристроїв до каналів зв'язку.

В початковому етапі свого існування стандарт 802.11 працював з обладнанням на частоті 2.4ГГц і максимальною швидкістю до 2 Мбіт/сек [14]. Базовий протокол 802.11 на своєму фізичному рівні реалізує 2 методи передачі даних:

- Метод частотних стрибків FHSS (Frequency Hopping Spread Spectrum);
- Метод прямої послідовності DSSS (Direct Sequence Spread Spectrum);

Стандарт 802.11 став «фундаментом» для наступних стандартів.

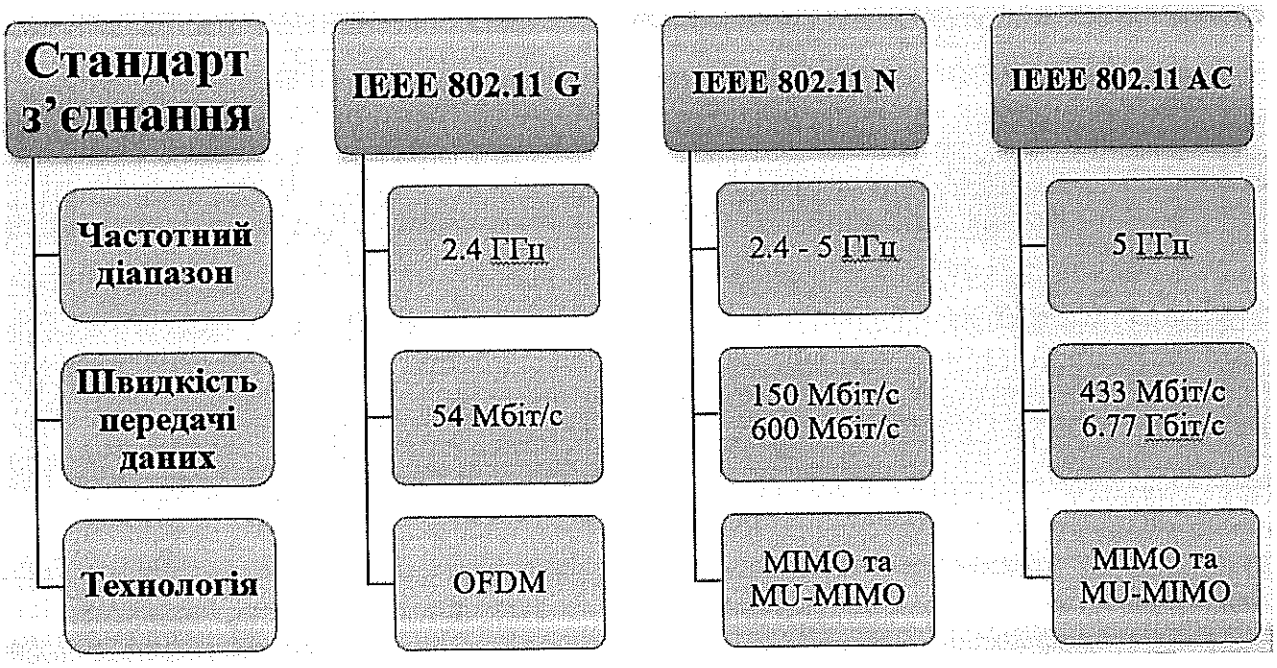


Рис. 1.7 Найпоширеніший набір стандартів зв'язку - IEEE 802.11

1.2.2. 802.11a (Wi-Fi 2)

Стандарт IEEE 802.11a був впроваджений в 1999 році. Замість діапазону 2,4 ГГц він передбачає використання частоти 5 ГГц. Як правило, більш високі частоти поєднуються з більш високими швидкостями, але з меншим діапазоном. Для досягнення більш високої швидкості він першим реалізував технологію OFDM (мультиплексирування з ортогональним частотним розділенням) - метод цифрової модуляції, що використовується для кодування даних на кількох частотах - у своїй схемі кодування, що дозволило йому мати теоретично максимальну швидкість 54 Мбіт / с, що було радіаційним покращення в порівнянні з вихідним стандартом WiFi.

Недоліками цього стандарту є висока споживча потужність і менший радіус дії обладнання. 802.11a працював у діапазоні 5 ГГц, це зробило продукти більш дорогими [13]. Тому в основному він використовувався у бізнес-мережах.

1.2.3 802.11b (Wi-Fi 1)

802.11b використовує DSSS (Direct -Sequence Spread Spectrum) - метод модуляції, використовуваний для зменшення приміщень сигналів - у діапазоні 2,4 ГГц, що дозволяє досягти швидкості до 11 Мбіт / с. Діапазон 2.4 відмінно справляється з подоланням перешкод, забезпечуючи більше покриття WiFi. На жаль, дані передаються набагато повільніше, особливо коли це пов'язано із мережевими завадами, винятковими пристроями, працюючими на тих же частотах, таких як радіоняні, мікрохвилевої печі, бездротові телефони, швидкісна техніка та пристрої Bluetooth. Завади можуть бути зменшені, якщо утримувати пристрої 802.11b подалі від таких пристроїв.

У зв'язку з тим, що Wi-Fi 1 використовував тільки діапазон 2,4, продукти були набагато дешевші, ніж 802.11a, що зробило його більш популярним для домашніх мереж [13].

1.2.4 802.11g (Wi-Fi 3)

Стандарт IEEE 802.11g є удосконаленням стандарту IEEE 802.11b. Завдяки застосування ефективніших технологій модуляції сигналу було підвищено швидкість передачі інформації до 54Мбіт/с.

У той час зворотна сумісність була обов'язковою, тому що у багатьох людей все ще були точки доступу та комп'ютери, які використовували попередні стандарти. 802.11g сумісний з продуктами 802.11b. Однак продукти Wi-Fi можуть підключатися тільки до того стандарту, відповідно до якого вони працюють. Комп'ютер 802.11b, підключений до точки доступу 802.11g, може працювати тільки з тією швидкістю, яку дозволяє стандарт b. З іншого боку, agякий пристрій, підключений до ab AP, буде працювати тільки з тією швидкістю, яку пропонує AP [13].

1.2.5 802.11n (Wi-Fi 4)

Wireless-N був розроблений в 2009 році для підвищення швидкості, надійності і розширення діапазону бездротової передачі.

Це був перший стандарт, в якому використовувалася технологія MIMO (Multiple-Input Multiple-Output). Продукти MIMO використовують серію антен для прийому більшої кількості даних від одного пристрою за раз, що призводить до більш швидкої передачі даних. Крім того, він першим дозволив використовувати дві радіочастоти - 2,4 ГГц і 5 ГГц. Використання обох частот робить стандарт 802.11n сумісним з пристроями 802.11a / b / g. Основними покращеннями були:

1. Створення багатоканального входу/виходу(MIMO);
2. Збільшення ширини смуги пропускання від 20МГц до 40МГц.

З усіма поліпшеними функціями Wi-Fi 4 підтримує швидкість передачі даних до 600 Мбіт / с і теоретичну дальність дії в 70 метрів в приміщенні, що є значним оновленням у порівнянні з попередніми стандартами [13].

1.2.6 IEEE 802.11ac (гігабітний WiFi або WiFi 5)

5-е покоління Wi-Fi було створено в 2013 році. Щоб зменшити перешкоди в діапазоні 2,4 ГГц, він був розроблений для роботи в діапазоні 5 ГГц. Технологія Wi-Fi 802.11ac використовує дві смуги частот для бездротового зв'язку. Щоб зробити це можливим, деякі постачальники включили технологію Wireless-N, щоб продукти змінного струму були сумісні з діапазоном 2,4 ГГц. Швидкості передачі даних розрізняються залежно від того, яка частота використовується, швидкість смуги пропускання до 1300 Мбіт / с може бути досягнута в діапазоні 5 ГГц, а в діапазоні 2,4 ГГц максимальна швидкість складає 450 Мбіт / с.

WiFi 802.11ac перший стандарт, який використав багато користувачів MIMO спадного каналу. Технологія Wireless-N MIMO зробила ще один крок вперед, щоб ще більше поліпшити передачу даних. DL MU-MIMO дозволяє бездротовим маршрутизаторам передавати інформацію на кілька пристроїв одночасно, підвищуючи швидкість смуги пропускання і зменшуючи затримку. Завдяки технології Wireless-N 802.11ac сумісний з 802.11a / b / g / n [9]. Також протягом декількох років розроблялись доповнення на основі цього типу стандарту - IEEE 802.11ad та IEEE 802.11ah.

1.2.7 IEEE 802.11ad (WiGig)

Розроблений для забезпечення багатогігабітної бездротової системи (MGWS) з високою пропускною здатністю даних, 802.11ad став частиною серії 802.11 в 2012 році. Він досяг неймовірно високій швидкості - до 6,7 Гбіт / с. На відміну від попередніх стандартів, він не використовував діапазони 2,4 або 5 ГГц, він працював в діапазоні 60 ГГц. Пам'ятайте, що чим вище частота, тим менше діапазон. В ідеальних умовах пристрою 802.11ad повинні знаходитися на відстані близько 9 метрів від точки доступу.

1.3 Аналіз протоколів захисту мереж безпроводового доступу Wi-Fi

Існує багато технологій безпеки, кожна з яких забезпечує рішення для найважливіших компонентів стратегії захисту даних: перевірка ідентичності, цілісність даних та активна перевірка. Ми визначаємо перевірку ідентичності як автентифікацію користувача або термінального пристрою та його місцезнаходження, а потім авторизацію користувача та кінцевого пристрою.

Цілісність даних включає такі сфери, як безпека мережевої інфраструктури, безпека периметра та конфіденційність даних. Проактивний огляд допомагає забезпечити дотримання встановлених політик безпеки на практиці та відстежувати всі відхилення та спроби несанкціонованого доступу.

1.4 Новизна розвитку сімейства IEEE 802.11

У травні 2019 року підгрупа BE (TGbe) Комітету 802.11 з питань стандартів локальних та міжміських мереж розпочала роботу над новим стандартом Wi-Fi, що дозволить збільшити номінальну пропускну здатність до більш ніж 40 Гбіт / с на одному частотному каналі "типовий" для діапазону Wi-Fi <= 7 ГГц. Хоча багато документів посилаються на "максимальну пропускну здатність щонайменше 30 Гбіт / с", новий протокол фізичного рівня забезпечить номінальну швидкість понад 40 Гбіт / с.

Ще одна важлива сфера розвитку Wi-Fi 7-це підтримка додатків у реальному часі (ігри, віртуальна та доповнена реальність, управління роботами). Хоча Wi-Fi обслуговує аудіо- та відеотрафік особливим чином, довгий час вважалося, що гарантування низької затримки (одиниці мілісекунд) на рівні стандарту, також відоме як Time-Sensitive Networking, принципово неможливо у мережах Wi-Fi. Літом 2018 року була створена спеціальна підгрупа для подальшого вивчення цього питання. Оскільки підтримка додатків у реальному часі вимагає як високої номінальної швидкості передачі даних, так і розширеної функціональності шару

зв'язку, робоча група 802.11 вирішила розробити методи підтримки додатків у режимі реального часу через Wi-Fi 7.

Важливим питанням, пов'язаним з Wi-Fi 7, є його співіснування із стільниковими технологіями (4G / 5G), які розробляються компанією 3GPP і працюють у тих самих неліцензійних діапазонах частот. Це LTE-LAA / NR-U. Для дослідження проблем, пов'язаних із співіснуванням Wi-Fi та стільникових мереж, IEEE 802.11 запустив Coexisting Standing Committee (Coex SC). Незважаючи на численні зустрічі та навіть спільний семінар учасників 3GPP та IEEE 802.11 у Вені літом 2019 року, технічні рішення ще не затверджені. Можливим поясненням цієї безрезультатної діяльності є те, що як IEEE 802, так і 3GPP неохоче змінюють власні технології, щоб привести їх у відповідність з іншою.

1.4.1. Етапи розробки

Хоч процес розробки Wi-Fi 7 знаходиться на самій початковій версії, на даний час було майже близько 450 запропонованих нових функцій для майбутнього Wi-Fi 7, а також відомого, як IEEE 802.11be.

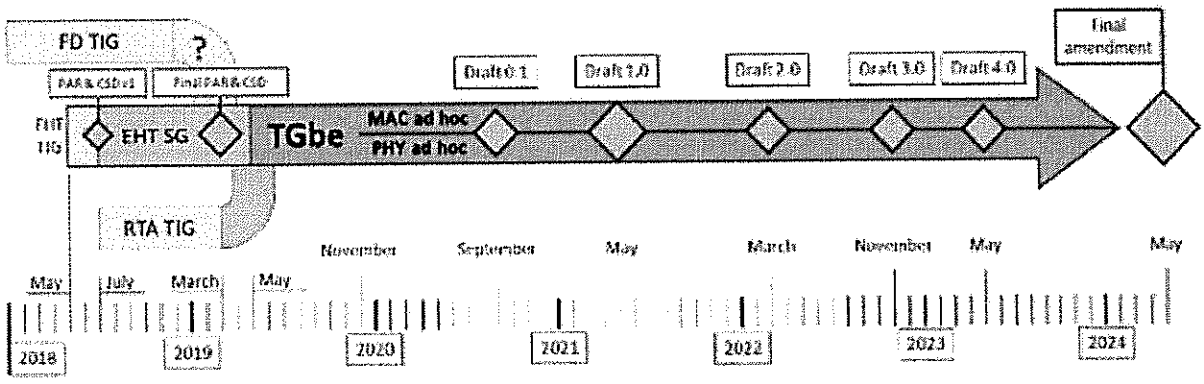


Рис. 1.8 Етапи розробки стандарту IEEE 802.11be

Значно планувалося, що розробка основних нових механізмів завершиться до березня 2021 року. У січні 2020 року в підгрупі 11 буде виражена сповіщення

темпу, буде розроблено відповідати графіці на нинішньому темпі роботи. Щоб прискорити процес розробки стандартів, підгрупа узгодила вибір невеликого набору високопріоритетних функцій, які можуть бути випущені до 2021 року (Випуск 1), а інші залишити у Релізі 2. Високопріоритетні функції повинні забезпечувати основну природну продукцію та включати в себе підтримку 320 МГц, 4K- QAM, очевидне покращення OFDMA від Wi-Fi 6, MU-MIMO с 16 потоками [11].

Через коронавірус група зараз очно не збирається, але регулярно проводить телеконференції, тому розробка затримується.

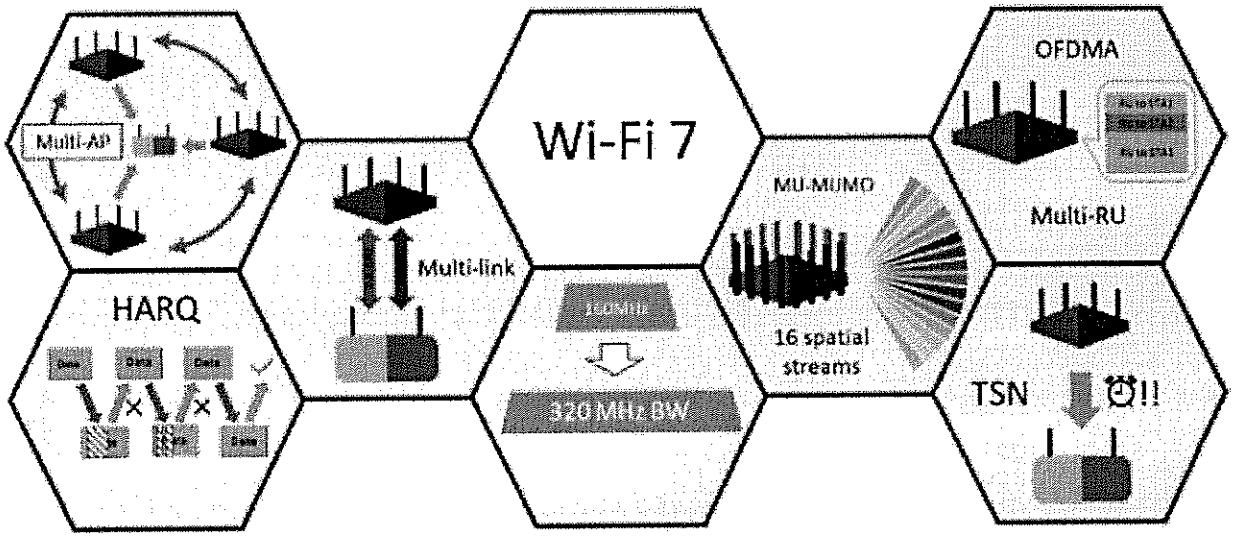


Рис. 1.9 Ілюстрація новизни протоколу

1.4.2. Новизна протоколу

Новий протокол фізичного рівня є розвитком протоколу Wi-Fi 6 с двократним збільшенням ширини смуги до 320 МГц, двократним збільшенням числа просторових потоків MU-MIMO, що збільшує номінальну пропускну здатність в 2x2 = 4 рази. Wi-Fi 7 також починає використовувати модуляцію 4K-QAM, що додає ще 20% до номінальної пропускної здатності. Таким чином, Wi-Fi 7 забезпечуватиме номінальну швидкість передачі даних в 2x2x1,2 = 4,8 раз вище в

порівнянні з Wi-Fi 6: максимальна номінальна пропускна здатність Wi-Fi 7 становить 9,6 Гбіт / с х 4,8 = 46 Гбіт / с.

Введений в Wi-Fi 6 (802.11ax) OFDMA - метод доступу до каналу з поділом за часом і частоті (аналогічний тому, що використовується в мережах 4G і 5G) - надає нові можливості для оптимального розподілу ресурсів. Однак в 11ax OFDMA недостатньо гнучкий. По-перше, він дозволяє точці доступу виділяти для клієнтського пристрою тільки один ресурсний блок заздалегідь визначеного розміру. По-друге, він не підтримує пряму передачу між клієнтськими станціями. Обидва нестачі знижують спектральну ефективність. Крім того, відсутність гнучкості успадкованого від Wi-Fi 6 OFDMA погіршує продуктивність в щільних мережах і збільшує затримку, що критично для додатків реального часу. 11be вирішить ці проблеми OFDMA.

Одним із затверджених революційних змін Wi-Fi 7 є вбудована підтримка одночасного використання декількох паралельних з'єднань на різних частотах, яка дуже корисна як для великих швидкостей передачі даних, так і для надзвичайно низькою затримки.

Використанням дуже широких каналів і великого числа просторових потоків призводить до проблеми високих накладних витрат, пов'язаних з процедурою оцінювання стану каналу, необхідної для MIMO і OFDMA.

Нарешті, ще одним важливим нововведенням, але з неясною долею, є скоординована робота точок доступу.

2 ВПРОВАДЖЕННЯ ПРОТОКОЛУ WIFI У ЦЕНТРАЛЬНІЙ СИСТЕМІ КЕРУВАННЯ АВТОМОБІЛЕМ

2.1 Принципи протоколу WiFi в системі центрального керування автомобіля

Протокол WiFi у центральній системі керування транспортним засобом відноситься до протоколу, який з'єднує центральну систему керування та інші пристрої через безпроводову мережу. Його принципи в основному включають такі аспекти:

Протокол WiFi у центральній системі керування транспортним засобом використовує технології безпроводової мережі, головним чином Wi-Fi та Bluetooth Технологія Wi-Fi може забезпечити більш високі швидкості передачі та стабільніші з'єднання, тоді як технологія Bluetooth більше підходить для з'єднань пристроїв із низьким енергоспоживанням. Завдяки цим технологіям безпроводової мережі центральна система керування транспортним засобом може обмінюватися безпроводовим зв'язком з іншими пристроями.

Протокол WiFi у центральній системі керування транспортним засобом використовує стек протоколів TCP/IP. Стек протоколів TCP/IP є основним протоколом Інтернету, який забезпечує надійну передачу даних і керування мережевими з'єднаннями. Завдяки стеку протоколів TCP/IP центральна система керування транспортним засобом може встановлювати стабільні мережеві з'єднання з іншими пристроями та передавати дані.

Протокол WiFi в центральній системі керування автомобілем забезпечує безпеку під час передачі даних. Шифрування даних є одним із важливих методів забезпечення безпеки. Протокол Wi-Fi у центральній системі керування транспортним засобом використовує алгоритм шифрування WPA2 для шифрування даних, запобігаючи несанкціонованому доступу та підробці даних.

Протокол WiFi у центральній системі керування транспортним засобом має різні застосування в практичних сценаріях.

Користувачі можуть підключати систему центральної системи керування до Інтернету через протокол WiFi у центральній системі керування автомобілем, забезпечуючи такі функції, як онлайн-оновлення карт і пошук інформації про дорожній рух у реальному часі. Це дозволяє користувачам бути в курсі дорожніх умов і вибирати оптимальний маршрут руху.

Протокол WiFi у центральній системі керування автомобілем також можна використовувати для передачі мультимедіа. Користувачі можуть бездротовим способом підключити центральну систему керування до таких пристроїв, як смартфони, планшети тощо, щоб передавати музику, відео та інші мультимедійні файли для відтворення на центральній системі керування транспортним засобом. Це дозволяє користувачам насолоджуватися більшою кількістю розважального контенту під час подорожей.

Протокол WiFi в центральній системі керування автомобілем можна використовувати для діагностики автомобіля. Завдяки бездротовому підключенню центральної системи керування транспортним засобом до діагностичного інтерфейсу автомобіля користувачі можуть контролювати різні параметри автомобіля в режимі реального часу, такі як температура двигуна, витрата палива тощо. Це дозволяє користувачам швидко виявляти та вирішувати проблеми автомобіля, покращуючи водіння безпеки.

За допомогою протоколу WiFi в центральній системі керування транспортним засобом користувачі можуть дистанційно керувати транспортним засобом. Як приклад на рис. 2.1, користувачі можуть використовувати мобільний додаток для дистанційного запуску кондиціонера автомобіля, блокування/розблокування автомобіля тощо, попередньо підготувавши автомобіль. Це дозволяє користувачам насолоджуватися більш комфортним досвідом водіння після досягнення місця розташування автомобіля.

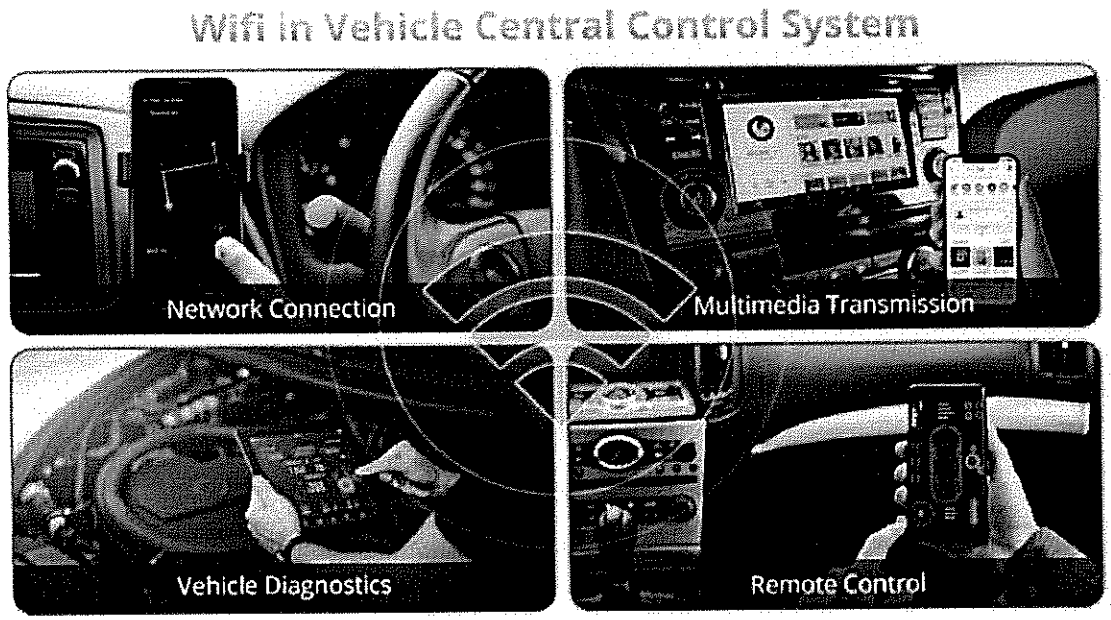


Рис. 2.1 Застосування протоколу WiFi в центральній системі керування транспортним засобом

З удосконаленням технології бездротової мережі протокол WiFi у центральній системі керування транспортним засобом досягне вищих швидкостей передачі. Це дозволить користувачам швидше завантажувати картографічні дані, передавати мультимедійні файли тощо, покращуючи роботу користувача.

У майбутньому протокол WiFi у центральній системі керування автомобілем відіграватиме роль у ширших сценаріях застосування. Наприклад, його можна використовувати для зв'язку між транспортними засобами для спільного водіння. Він також може підключатися до систем розумного дому, щоб полегшити взаємозв'язок між транспортними засобами та домашніми пристроями.

Зі збільшенням оцифруванням транспортних засобів протокол WiFi у центральній системі керування транспортним засобом потребуватиме більш надійного захисту. У майбутньому протокол використовуватиме більш просунуті алгоритми шифрування для посилення захисту даних, запобігання хакерським атакам і витоку інформації.

З розвитком технології автономного водіння протокол WiFi у центральній системі керування автомобілем буде глибоко інтегрований із системами

автономного водіння. Через безпроводової мережеві підключення центральна система керування транспортним засобом може передавати дані в реальному часі та надсилати команди керування системам автономного водіння, підвищуючи точність і безпеку автономного водіння.

2.2 Модульний підхід до безпроводових технологій

Ми всі сприймаємо доступ до Wi-Fi як належне. У нашому офісі, вдома чи в нашій улюбленій кав'ярні Wi-Fi пропонує нам обчислювальну та комунікаційну мобільність. Як споживачі Wi-Fi, ми також почали очікувати його під час руху.

Підключення Wi-Fi в автомобілі починає ставати все більш популярним як спосіб підключення як вбудованих пристроїв, так і пристроїв, що належать пасажирам. Але в машині не тільки wifi. Стандарт Bluetooth використовується протягом багатьох років для підключення смартфона до автомобільної функції гучного зв'язку.

Планується, що Bluetooth і надалі стане ключовим засобом для низки автомобільних додатків, від передачі аудіо до стереосистеми автомобіля, до використання смартфона для розблокування дверей автомобіля. З цих причин при розробці бездротового підключення для автомобільних додатків Wi-Fi і Bluetooth є ключовими.

Окрім суто телефонних додатків, де історично перевагу надавали Bluetooth, головною сферою зростання стало надання медіа-контенту для пасажирів із інформаційно-розважальної системи. Для цього добре використано Wi-Fi. Рис.2.2 ілюструє деякі приклади застосування.

Wi-Fi тепер можна використовувати для потокової передачі відеоконтенту, надання навігаційних карт на автомобільний дисплей і навіть для підключення камери заднього виду. Оскільки ці функції, на додаток до додатків для екрану Wi-Fi, заснованих на Apple CarPlay, Android Auto та MirrorLink, стають все більш поширеними, високошвидкісний Wi-Fi стане фундаментальною частиною автомобільної електроніки, а не буде вважатися просто розкішшю.

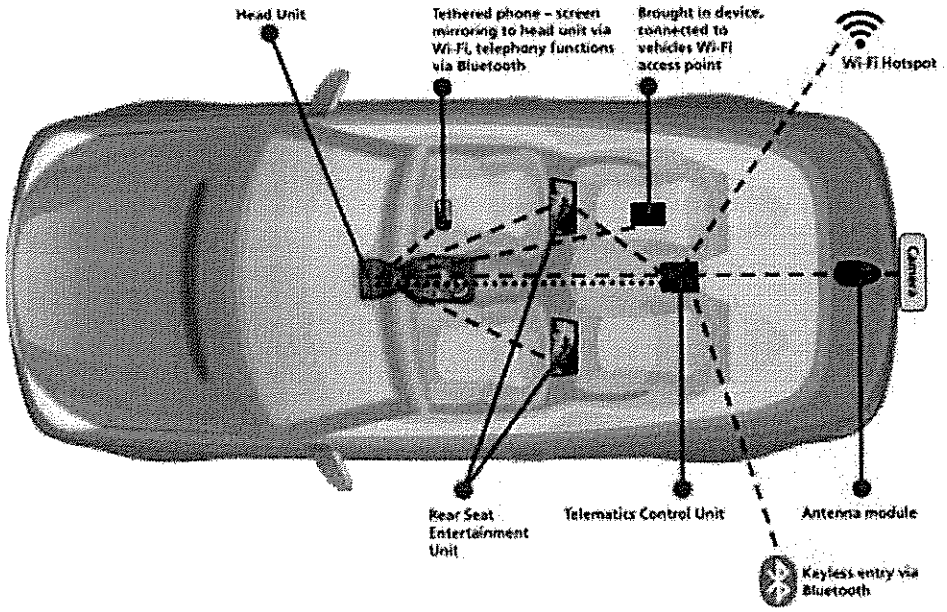


Рис. 2.2 Приклади застосування Wi-Fi у автомобілі

Опублікований наприкінці 2009 року стандарт 802.11n став де-факто Wi-Fi-з'єднанням, додавши значно покращену пропускну здатність мережі порівняно з попередніми стандартами 802.11a та 802.11g. Збільшивши теоретичну максимальну пропускну здатність з 54 до 600 Мбіт/с, це також був перший стандарт, який додав підтримку потоків із множинним входом і множинним виходом (mimo), агрегацію кадрів і кілька покращень безпеки. Його можна використовувати як на діапазонах 2,4, так і на 5 ГГц.

Технічно 802.11n siso може забезпечувати швидкість передачі даних до 150 Мбіт/с, чого недостатньо для сучасних зростаючих потреб. Отримавши схвалення на початку 2014 року, стандарт 802.11ac розроблений виключно для роботи на частоті 5 ГГц і має заявлену максимальну пропускну здатність кількох станцій трохи більше 1 Гбіт/с і практичну швидкість одного каналу наближається до 450 Мбіт/с.

Зіткнувшись із впровадженням як Wi-Fi, так і Bluetooth і швидким виведенням продуктів на ринок, гнучка команда розробників, швидше за все, вибере для свого дизайну мультирадіомодуль. Створення дизайну дискретного трансивера завжди можливе, але модулі пропонують попередньо сертифікований

підхід, який, швидше за все, означатиме, що інженер може мати проект, який працює на стадії прототипу, перш ніж закінчити дискретну специфікацію.

Вибираючи модуль для автомобільних додатків Wi-Fi і Bluetooth, інженери повинні враховувати низку ключових критеріїв. Висока швидкість передачі даних Wi-Fi і можливість працювати одночасно як точка доступу Wi-Fi (AP), станція (STA) або в прямому режимі (P2P) є ключовими критеріями.

Зайве говорити, що одночасна робота Wi-Fi і Bluetooth також буде ключовою вимогою. Для оптимальної продуктивності та співіснування двох стандартів модуль повинен мати окремі інтерфейси для Wi-Fi і Bluetooth, а також дозволяти конструкції з окремими антенами Wi-Fi і Bluetooth.

Для Bluetooth модуль має запропонувати подвійний режим Bluetooth v4.2, оскільки це дозволяє підключатися як до пристроїв Bluetooth Classic, так і до пристроїв Bluetooth LE, а також забезпечує реалізацію майбутніх варіантів використання LE, таких як вхід без ключа.

З нормативної точки зору, розробник повинен знати про ринки, на які може потрапити його система. Тип модуля, схвалений на всіх ринках, які приймають модульні схвалення, забезпечить довіру, якщо маркетингова специфікація раптово зміниться, включивши інші області, які раніше не вважалися необхідно.

Для автомобільних застосувань використання компонентів, які відповідають або перевищують специфікації якості компонентів AEC-Q100 Ради автомобільної електроніки (AEC), є ключовим. Крім того, життєво важливою є кваліфікація продукту відповідно до стандарту ISO 16750-4, який визначає екологічні та кліматичні умови, з якими зазвичай стикається електричне та електронне обладнання, встановлене в автомобілях. З ширшої точки зору виробництва та ланцюга постачання, модуль має виготовлятися в середовищі, яке відповідає вимогам системи управління якістю ISO/TS 16949.

Плати оцінювання також доступні для прискорення проектування кінцевої системи. Такі плати діють як платформа прототипування для підключення до головної програми, надаючи повний доступ до всіх інтерфейсів модулів. Роз'єми

SMA дозволяють встановлювати антени як на трансиверах Wi-Fi, так і на Bluetooth, а вбудовану антену NFC можна встановити на плату.

Cypress покращує користувальницький досвід автомобільної інформаційно-розважальної системи преміум-класу за допомогою рішення для підключення Wi-Fi 6.

Нові комбінації Wi-Fi ® і Bluetooth ® забезпечують одночасну потокову передачу для кількох пристроїв у більш широкому діапазоні категорій автомобілів.

На рис. 2.3 зображено комбіноване рішення Cypress CYW89650 Wi-Fi 6 і Bluetooth 5.0 для автомобільних інформаційно-розважальних систем. Рішення забезпечує пропускну здатність понад 1 Гбіт/с, а архітектура Real Simultaneous Dual Band (RSDB) Cypress забезпечує одночасну роботу у високопродуктивних системах без погіршення якості аудіо чи відео. (Графіка: Business Wire)

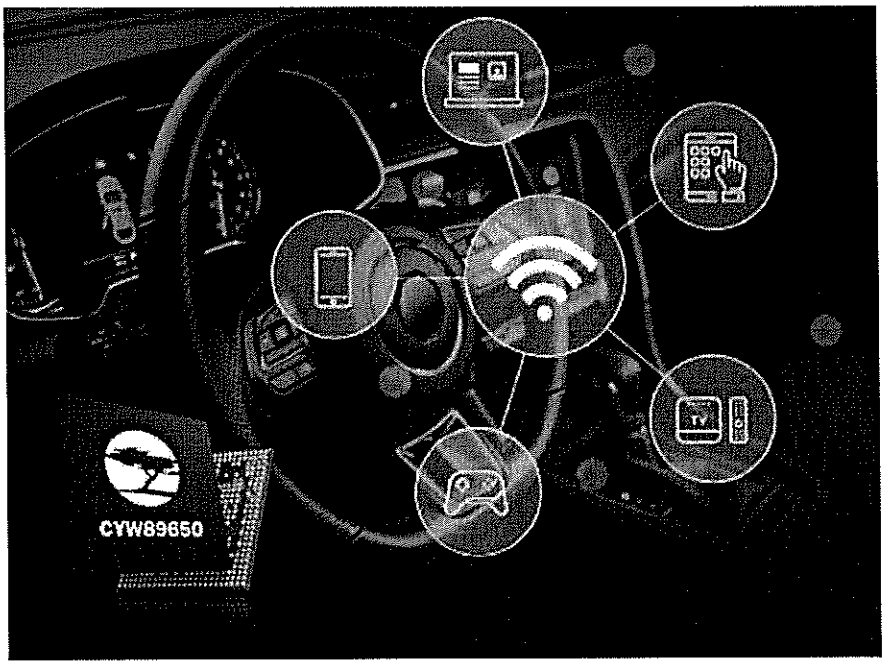


Рис. 2.3 Комбіноване рішення Cypress CYW89650 Wi-Fi 6 і Bluetooth 5.0

Комбіновані чіпсети Wi-Fi ® і Bluetooth ® і допоміжне програмне забезпечення служать платформами для розробки додатків, які дозволяють декільком користувачам підключатися та безперешкодно передавати унікальний

контент на 10 мобільних пристроїв одночасно. Нові інформаційно-розважальні платформи включають комбіноване рішення WiFi 6 (802.11ax) і Bluetooth, яке використовує архітектуру Cypress Real Simultaneous Dual (RSDB). RSDB став стандартом де-факто для підключених інформаційно-розважальних систем преміум-класу, дозволяючи двом унікальним потокам даних працювати з повною пропускною здатністю одночасно завдяки інтеграції двох підсистем Wi-Fi в один чіп. Wi-Fi 6 забезпечує пропускну здатність на рівні гігабіт і підвищує надійність потокової передачі вмісту на кілька пристроїв одночасно.

Cypress також додав до свого портфоліо два комбінованих рішення WiFi 5 (802.11ac) і Bluetooth, надавши виробникам автомобілів і постачальникам автомобільних систем рішення масштабованої платформи для широкого спектру транспортних засобів з єдиною архітектурою програмного забезпечення, яка мінімізує розробку та системну інтеграцію витрати.

«Виробники автомобілів прагнуть забезпечити багатокористувацький доступ і потокове передавання медіа у своїх автомобілях, що можна порівняти з першокласним особистим мультимедійним досвідом вдома; Cypress пропонує єдину в галузі лінійку продуктів, розроблену спеціально для автомобільних інформаційно-розважальних систем, із підходом до платформи для постачальників і виробників комплектного обладнання, щоб використовувати наші рішення низького, середнього та високого класу для покриття діапазону від економічних до розкішних автомобілів», – сказав Брайан Бедросян, віце-президент. маркетингу бізнес-підрозділу IoT Compute and Wireless у Cypress. «Розробка програмного забезпечення для випадків використання автомобільного бездротового підключення стає дедалі складнішою. Наша масштабована платформа дозволяє розподіляти витрати на розробку програмного забезпечення між інформаційно-розважальними системами для різних моделей. Ці нові рішення демонструють наше прагнення інтегрувати передові технології в рамках нашої зосередженості на забезпеченні підключення до Інтернету речей світового рівня для наших клієнтів на різних ринках».

Інформаційно-розважальним системам преміум-класу потрібна багатофункціональна одночасна робота з високою пропускною здатністю для впровадження бездротового віддзеркалення для таких програм, як Apple® CarPlay, Android Auto та Mirrorlink. Комбіновані рішення Cypress Wi-Fi і Bluetooth відповідають цим потребам, а також пропонують одночасну точку доступу Wi-Fi і доступ до вмісту, а також співіснування багатодіапазонного/багатодіапазонного радіо для відео та аудіо Bluetooth. Комбіноване рішення Cypress CYW89650 2x2 плюс 2x2 Wi-Fi 6 і Bluetooth 5.0 забезпечує пропускну здатність понад 1 Гбіт/с, а архітектура RSDB забезпечує одночасну роботу для цих випадків використання у високопродуктивних інформаційно-розважальних системах без погіршення якості звуку чи відео. Новий CYW89459 2x2 Wi-Fi 5 і Bluetooth 5.0 комбо з RSDB спирається на успіх існуючих автомобільних рішень Cypress Wi-Fi 5, дозволяючи підключати більше пристроїв до головного пристрою та включаючи такі нові функції, як безпека WPA3, Wi-Fi Location ™ і Wi-Fi Aware™. Разом із новим економічно ефективним комбо CYW89373 1x1 Wi-Fi 5 і Bluetooth 5.0 портфоліо забезпечує масовий ринок автомобілям класу «люкс» із передовою продуктивністю бездротового зв'язку та середнім керуванням співіснуванням для безперервних розваг.

Автомобільні бездротові рішення Cypress повністю відповідають вимогам стандарту AEC-Q100 класу 3. Існуючі рішення Cypress були розроблені багатьма провідними OEM-виробниками автомобілів і автомобільними постачальниками, і сьогодні вони знаходяться у серійному виробництві, підтримуючи інформаційно-розважальні та телематичні програми, такі як дзеркальне відображення екрану смартфона, потокова передача вмісту та голосовий зв'язок Bluetooth у автомобільних комплектах.

Cypress демонструє свої автомобільні бездротові рішення разом із повним портфоліо вбудованих системних рішень для автомобільних систем та Інтернету речей тут, на виставці CES 2019, у Південному залі 2 конференц-центру Лас-Вегаса в конференц-залі MP25776.

Cypress співпрацює з провідними світовими автомобільними компаніями над розробкою передових автомобільних систем, включаючи Advanced Driver Assistance Systems (ADAS), 3-D графічні дисплеї, бездротове підключення, повнофункціональні сенсорні екрани та чудову електроніку для кузова. Автомобільний портфель Cypress включає мікроконтролери Traveo™ і PSoC® (MCU), ємнісні датчики CapSense®, сенсорні екрани TrueTouch®, рішення для підключення Wi-Fi®, Bluetooth® і USB, мікросхеми керування живленням (PMIC) і флеш-пам'ять NOR., F-RAM™ і SRAM. Портфоліо підтримується зобов'язанням Cypress прагнути до нульового виявлення дефектів, надавати відмінне обслуговування та дотримуватися найсуворіших стандартів автомобільної промисловості.

Cypress є лідером у сфері передових вбудованих рішень для найінноваційніших у світі автомобільних, промислових, розумних побутових приладів, споживчої електроніки та медичних виробів. Мікроконтролери Cypress, рішення для бездротового підключення та підключення на основі USB, аналогові мікросхеми та надійна, високопродуктивна пам'ять допомагають інженерам розробляти диференційовані продукти та виводити їх на ринок першими. Cypress прагне надавати клієнтам найкращі ресурси підтримки та розвитку на планеті, що дозволить їм підірвати ринки шляхом створення нових категорій продуктів у рекордно короткі терміни.

Cypress, логотип Cypress, PSoC і CapSense є зареєстрованими товарними знаками, а Traveo і F-RAM є товарними знаками Cypress Semiconductor Corp. Усі інші товарні знаки є власністю їх власників.

Автомобілями з уразливістю WiFi все ще безпечно керувати.

Ford попереджає про вразливість переповнення буфера в своїй інформаційно-розважальній системі SYNC3, яка використовується в багатьох автомобілях Ford і Lincoln, що може дозволити дистанційне виконання коду, але каже, що це не впливає на безпеку водіння автомобіля.

SYNC3 — це сучасна інформаційно-розважальна система, яка підтримує автомобільні точки доступу Wi-Fi, підключення до телефону, голосові команди, програми сторонніх розробників тощо.

Нападники поруч.

Уразливість відстежується як CVE-2023-29468 і міститься в драйвері WL18xx MCP для підсистеми WiFi, вбудованої в інформаційно-розважальну систему автомобіля, що дозволяє зловмиснику в зоні дії WiFi ініціювати переповнення буфера за допомогою спеціально створеного кадру «Зловмисник у зоні дії бездротового зв'язку потенційно вразливого пристрою може отримати можливість перезаписати пам'ять головного процесора, який виконує драйвер MCP», — йдеться в бюлетені безпеки постачальника системи.

Ford був проінформований постачальником про виявлення недоліку Wi-Fi і негайно вжив заходів, щоб перевірити його, оцінити вплив і розробити заходи для пом'якшення.

У заяві, опублікованій на медіа-порталі Ford, автовиробник обіцяє незабаром зробити доступним програмний патч, який клієнти зможуть завантажити на USB-накопичувач і встановити на своїх автомобілях.

«Незабаром Ford випустить патч програмного забезпечення онлайн для завантаження та встановлення через USB», — йдеться в повідомленні Ford.

«Тимчасом клієнти, які стурбовані уразливістю, можуть просто вимкнути функцію WiFi через меню налаштувань інформаційнорозважальної системи SYNC 3». Щоб ще більше заспокоїти будь-які занепокоєння, американський автовиробник також заявив, що недолік непросто використати, і навіть у цьому малоймовірному сценарії він не поставить під загрозу безпеку цільових транспортних засобів.

«На сьогоднішній день ми не бачили жодних доказів того, що ця вразливість була використана, що, ймовірно, потребуватиме значного досвіду, а також включало б фізичне перебування поблизу окремого транспортного засобу з увімкненим запалюванням і Wi-Fi», — пояснює Форд.

«Наше розслідування також виявило, що використання цієї вразливості, хоч і малоймовірне, це не вплине на безпеку пасажирів транспортного засобу, оскільки інформаційно-розважальна система захищена від елементів керування, таких як рульове керування, дроселювання та гальмування».

2.3 Автомобільні точки доступу Wi-Fi

Інтернет всюди, ми завжди на зв'язку з нашими гаджетами, щоб могли спілкуватися, телефонувати, ділитися, читати, працювати, грати та робити все інше. Але машини не можна підключити дротом.

Wi-Fi є у всіх вдома та в офісі, і ми отримуємо Wi-Fi у кафе та спортзалах. Чому використовуємо Wi-Fi замість підключення LTE або 3G на наших смартфонах? Це дешевше. Вчора теж було швидше, а сьогодні зі швидкостями LTE тільки дешевше. Звичайний Wi-Fi має дротове підключення до Інтернету — це дешево і безлімітно.

Але машини не можна підключити дротом. Отже, якщо говорити про автомобільний Wi-Fi — він використовує мобільну мережу 3G або LTE і має таку саму ціну за передачу даних, як і наш смартфон.

Спочатку розділимо точки інтересу для автомобільного Wi-Fi на два типи «користувачів» автомобілів таких як пасажири автомобіля і водії автомобілів, використовується Wi-Fi, коли керується автомобіль.

Якщо є діти будь-якого віку, то знаємо, навіщо вашій машині потрібен Wi-Fi. YouTube, месенджери, Facebook, онлайн-ігри і так далі. Діти щасливі, коли їм є чим зайнятися — батьки можуть безпечно керувати своїми автомобілями, оскільки їхні діти почуваються як вдома з хорошим Wi-Fi з'єднанням для всіх своїх гаджетів (планшетів, PSP, смартфонів тощо).

Перш за все, Wi-Fi в автомобілі забезпечить набагато краще підключення до Інтернету. А люди використовують час за кермом, щоб відповідати на електронні листи або перевіряти оновлення у Facebook. Але вони мають власне підключення на своїх смартфонах. Тоді чому Wi-Fi має сенс для них?

Перш за все, Wi-Fi в автомобілі забезпечить набагато краще підключення до Інтернету. Автомобілі їздять швидко, а підключення до мобільної мережі змінюється щосекунди. Автомобільні точки доступу Wi-Fi використовують спеціальні стратегічно розташовані антени. Тому автомобільні точки доступу Wi-Fi можуть забезпечити набагато швидший і стабільніший Інтернет для всіх пасажирів. Особливо на автомагістралях, де покриття оператора мобільного зв'язку нестабільне, а звичайні смартфони з вбудованими маленькими антенами втрачають сигнал або їхній сигнал занадто слабкий, щоб комфортно користуватися Інтернетом.

Що щодо пристроїв, які підтримують лише Wi-Fi? Ноутбуки, планшети, переносні пристрої — з автомобільним Wi-Fi усіма цими гаджетами можуть легко користуватися пасажири під час руху як на рис. 2.4.



Рис. 2.4 Гаджетами можуть легко користуватися пасажири під час руху

Крім того, Wi-Fi може економити заряд акумулятора. Завдяки підключенню Wi-Fi смартфон або інший гаджет на рис.2.5 економить енергію для підключення та працює довше.

Аспеціальне слово для бізнес-пасажирів, які користуються особистими водіями. Wi-Fi має бути обов'язковою опцією. Для бізнес-пасажирів їхня машина – це завжди офіс на колесах.



Рис. 2.5 Робота з гаджетом

Як згадувалося раніше, він пропонує краще підключення до Інтернету. З автомобільним Wi-Fi водії не матимуть перерв у з'єднанні з Інтернетом під час телефонної розмови. Це також важливо під час використання онлайн навігації, як-от Google Maps або Waze, під час водіння як на рис. 2.6.



Рис. 2.6 Google Maps або Waze, під час водіння

Використання тільки Wi-Fi електроніки також важливо для водія. Сьогодні багато водіїв використовують планшети для навігації, і сьогодні існує багато видів підключеної автомобільної електроніки, представлено на рис. 2.7:

- підключені дзеркала Wi-Fi;
- підключені Wi-Fi гарнітури;
- Wi-Fi відеореєстратори.

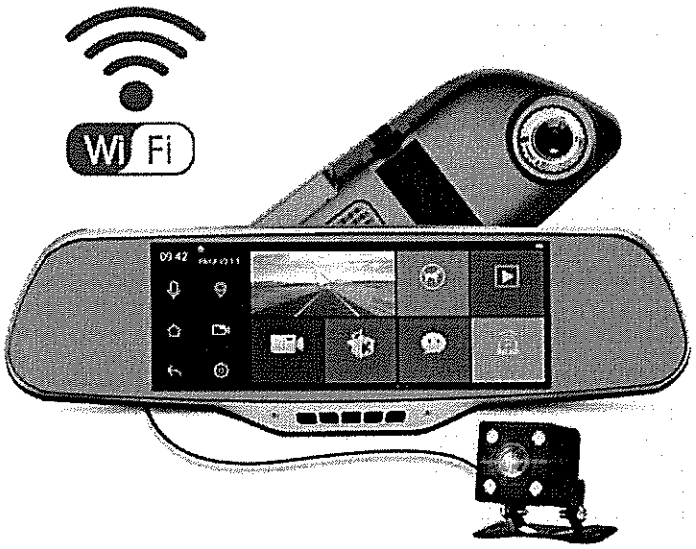


Рис. 2.7 Декілька видів підключеної автомобільної електроніки

Для автомобільний Wi-Fi для туристичного бізнесу таксі та оренда автомобілів дуже важливі точки доступу Wi-Fi. Особлива тема — Wi-Fi в автомобілі для туристів. Якщо говорити про туристичний ринок, то Wi-Fi сьогодні є найважливішою послугою для туристів. Вони не хочуть платити нестандартні рахунки за послуги мобільного Інтернету в роумінгу та завжди шукають доступний Wi-Fi.

Найкращий сценарій – коли виробники автомобілів попередньо встановлюють гарячі точки у свої автомобілі на виробничій лінії. Це означає, що пристрій матиме хороші зовнішні антени для гарного підключення, а його керування живленням буде інтегровано в автомобіль.

Вбудованими точками доступу Wi-Fi зазвичай керують із спеціальних мобільних додатків або за допомогою мультимедійного сенсорного екрана автомобіля.

Сьогодні кілька виробників автомобілів використовують попередньо встановлені SIM-карти, які ви не можете замінити. Це проблема, коли ви хочете змінити постачальника мережевих послуг вашої точки доступу. Іноді навіть вбудовані SIM-карти мають фіксовані тарифні плани, які ви не можете змінити.

Наприклад — Audi Connect для ринку США, із SIM-картками T-Mobile і тарифними планами, які ви не можете змінити, за 30 доларів на місяць. Звучить жахливо!

Інші дозволяють розмістити власну SIM-карту у вбудованій точці доступу Wi-Fi. Принаймні добре мати можливість змінити тарифний план, якщо SIM-карту неможливо замінити. Новітні технології також пропонують використовувати смартфон водія замість SIM-карти для спільного доступу до Інтернету через точку доступу Wi-Fi автомобіля.

Простий і доступний у мобільних операторів різних країн, що пропонує автомобільні точки доступу Wi-Fi для вторинного ринку це Huawei CarFi.

Це простий LTE-роутерна рис. 2.8, який підключається до прикурювача автомобіля. Крім того, він заряджатиме ваші гаджети через USB-порт.

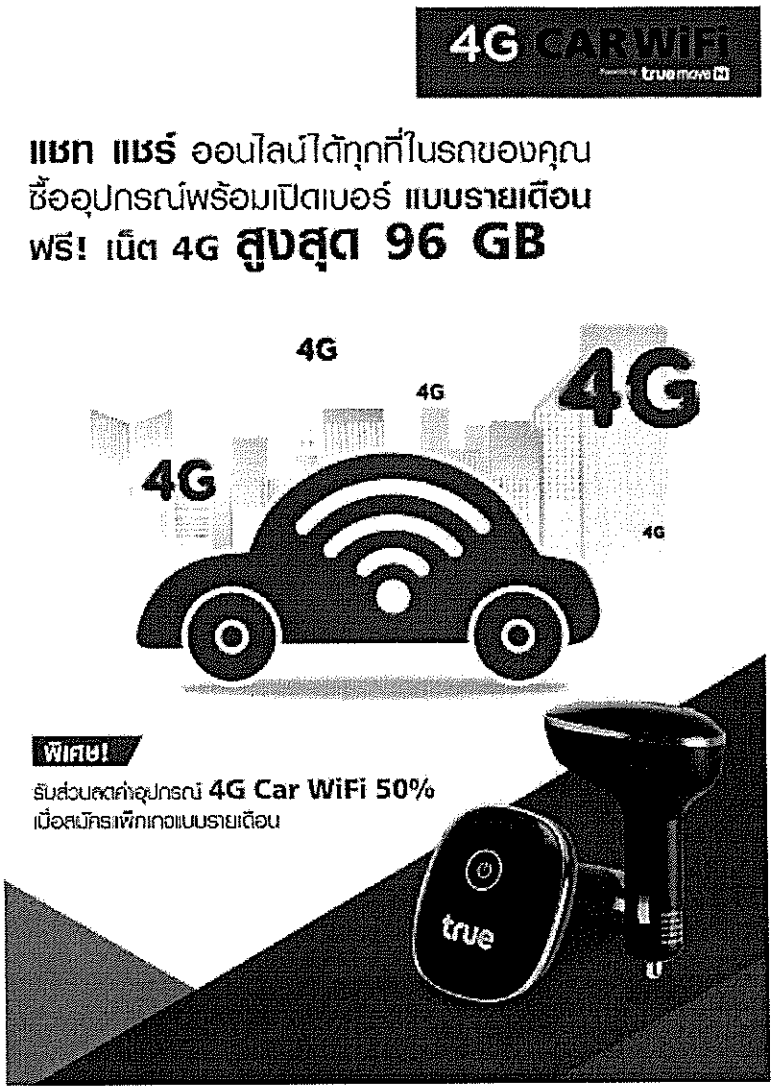


Рис. 2.8 Huawei CarFi

Основна проблема Huawei CarFi полягає в тому, що цей пристрій не знає, коли запускається або зупиняється автомобіль. Таким чином, точка доступу автоматично не керує своїм живленням (вмикається, коли запускається автомобіль, і вимикається, коли автомобіль вимикається). З Huawei CarFi доведеться вручну вмикати його кожного разу, коли сідаєте в автомобіль. Це може стати проблемою, якщо їздите на машині багато разів на день.

Набагато краще рішення — пристрій OBD Wi-Fi hotspot. Порт OBD доступний на кожному автомобілі з 1996 року. Зазвичай цей порт розташований під кермом.

Порт OBD забезпечує живлення пристроїв точки доступу та може інформувати пристрій про стан автомобіля. Тож пристрій OBD Wi-Fi може керувати своїм режимом живлення залежно від стану автомобіля. Це означає, що точка доступу OBD Wi-Fi буде дуже добре інтегрована з автомобілем, а функція Wi-Fi безперешкодно використовуватиметься в автомобілі.

Сьогодні більшість OBD Wi-Fi точок доступу на ринку також мають вбудовані GPS і G-сенсори та інші функції. Це дозволить створювати різні базові функції точки доступу пристрою. Хороший приклад і історія успіху від T-Mobile у Німеччині — ключі ZTE OBD у поєднанні з підключеними послугами від Mojio на рис.2.9.

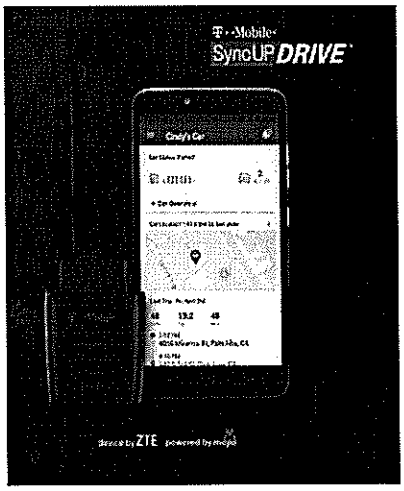


Рис. 2.9 ZTE OBD

Подібно до продукту SyncUp Drive, але від Telia Soneira та послуг, цей продукт був розроблений внутрішньою командою Telia.

2.4 Роль Bright Box у галузі автомобільного Wi-Fi

Компанія Bright Box як постачальник рішень для підключених автомобілів надає вбудовані автомобільні точки Wi-Fi для одного зі своїх клієнтів — Genesis. Система «Genesis Connect» стане ще однією перевагою для власників Genesis G90, зроблячи обслуговування автомобіля легким і зручним.

Продукт був розроблений спеціально для нового бренду і дозволяє користувачам відкривати/закривати центральний замок, запускати/зупиняти двигун, перевіряти стан дверей, відкривати багажник, стежити за швидкістю автомобіля, отримувати показники внутрішньої та зовнішньої температури, активувати horn — все це з додатка, встановленого на їхніх смартфонах.

Крім того, незабаром власники Genesis G90 отримають можливість дистанційної діагностики автомобіля. Крім того, власники нової моделі зможуть насолодитися інтегрованим рішенням Remoto Wi-Fi для бездротового доступу до Інтернету. Налаштування Wi-Fi керується з мобільного додатку Genesis G90 для iOS та Android як на рис.2.10.

Bright Box також має післяпродажний продукт для вторинного ринку у формі OBD — разом із мобільними додатками, які надають корисні послуги водіям, включаючи хмарні музичні сервіси, дистанційну діагностику, сповіщення про удар та інші.

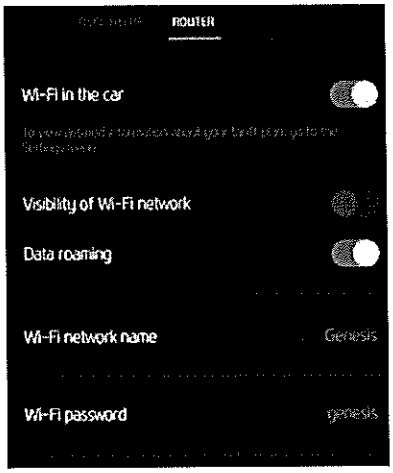


Рис. 2.10 Мобільний додаток Genesis G90 для iOS та Android

Це рішення зазвичай затребуване мобільними операторами — 99% автомобілів на дорогах ще не мають Wi-Fi на борту. Таким чином, це величезна ринкова можливість для мобільних операторів у всьому світі.

3 ГОЛОСОВЕ КЕРУВАННЯ ЧЕРЕЗ WIFI І NODEMCU

3.1 WiFi-робот із голосовим керуванням і NodeMCU

Як щодо того, щоб почати замість домашніх пристроїв керувати двигунами? І ще краще, як щодо того, щоб ці двигуни керували диференціальним роботом? Це саме те, що розробимо далі, WiFi Voice Controlled Robot на рис.3.1, використовуючи як контролер старий NodeMCU!

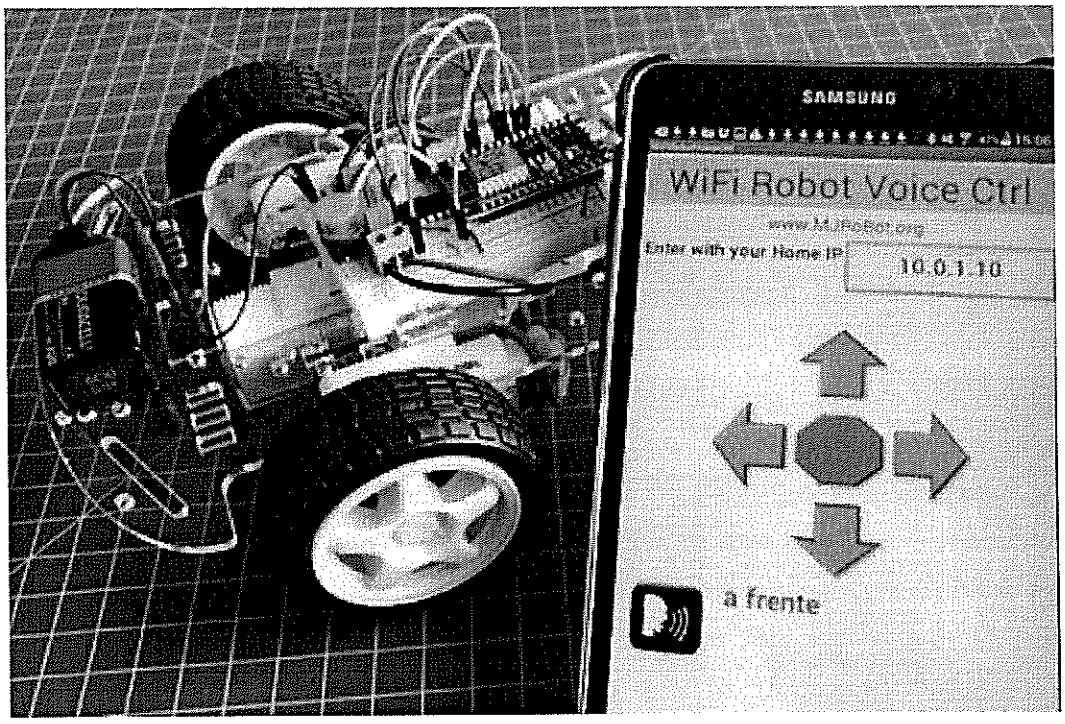


Рис. 3.1 WiFi Voice Controlled Robot

Наведена на рис.3.2 блок-схема показує, що буде зроблено в цілому, але потрібно враховувати, що один із двигунів мав дуже малий крутний момент. Незважаючи на те, що результат здається трохи рідкісним, робот працює належним чином.

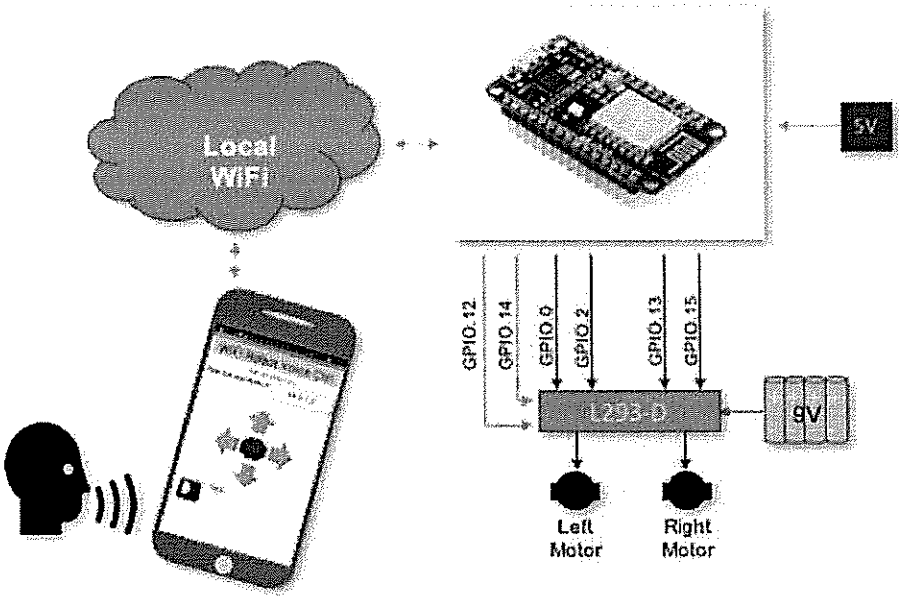


Рис. 3.2 Блок-схема WiFi Voice Controlled Robot

Для роботи над проєктом необхідні наступні матеріали:

- NodeMCU ESP8266-12E;
- 400-точкова експериментальна макетна дошка;
- H-Bridge L293D;
- набір автомобільного шасі Motor Robot;
- кабелі Dupont «чоловік-жінка»;
- портативний зарядний пристрій 5VDC 3000mAh Power Bank;
- зовнішня батарея 9VDC;
- будь-який смартфон або планшет Android.

3.2 H-Bridge L293D

Щоб керувати двигунами, будемо використовувати L293D на рис.3.3 з чотириразовим Н-мостом драйверів Half-H.

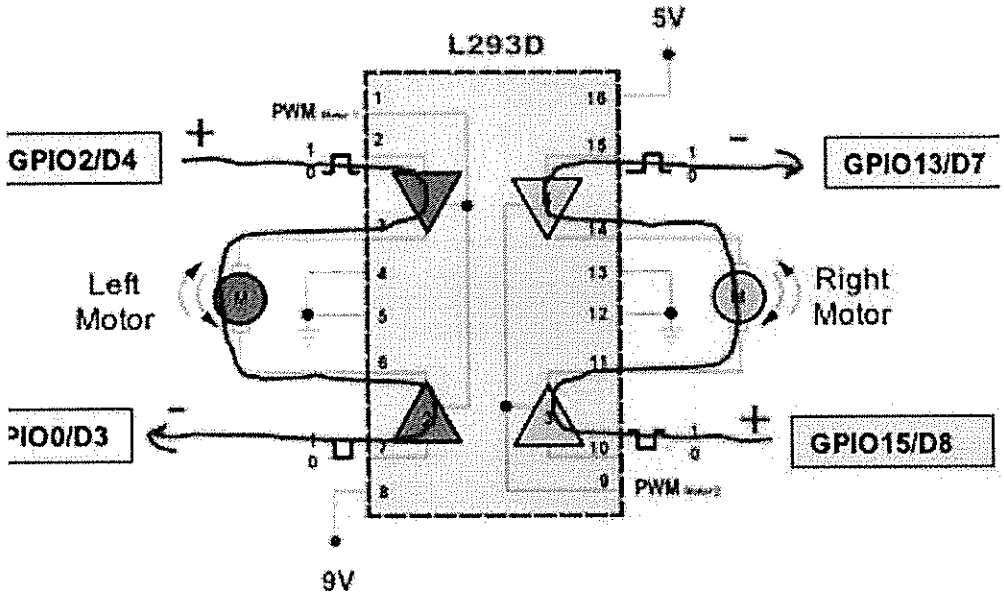


Рис. 3.3 L293D

Відповідно до його таблиці даних, пристрої L293 і L293D являють собою чотирикратні високострумові драйвери половини H. L293 розроблено для забезпечення двонаправлених струмів приводу до 1 А при напрузі від 4,5 В до 36 В. L293D розроблено для забезпечення двонаправлених струмів приводу до 600 мА при напрузі від 4,5 В до 36 В. Обидва пристрої на рис.3.4 є соленоїди, двигуни постійного струму та біполярні крокові двигуни, а також програми живлення.

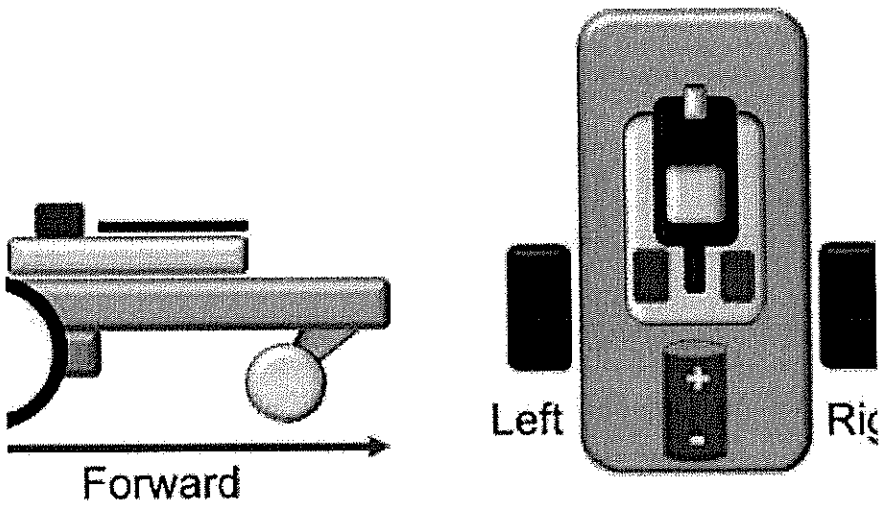


Рис. 3.4 Двигуни постійного струму

Будемо використовувати IC безпосередньо з NodeMCU, не використовуючи щит, який також є поширеним явищем. Робот має два колеса, які приводяться в рух 2 двигунами постійного струму.

Підключимо двигуни до H-мосту, як показано на схемі рис.3.3. NodeMCU матиме 6 GPIO, які керуватимуть цими двигунами.

int rightMotor2 = 13; // D7 - правий двигун –

int rightMotor1 = 15; // D8 - правий мотор +

int leftMotor2 = 0; // D3 - лівий двигун –

int leftMotor1 = 2; // D4 - лівий двигун +

int eneLeftMotor = 12; // D6 - увімкнути двигун ліворуч

int eneRightMotor = 14; // D5 - включити Motor Right

Наприклад, щоб рухати лівий двигун вперед, потрібно поставити:

- HIGH на контакті D4 (лівий двигун +);

- LOW на контакті D3 (лівий двигун -).

Для правого двигуна повинні зробити навпаки:

- HIGH на контакті D8 (правий двигун +);

- LOW на контакті D7 (лівий двигун -).

Завдяки тому, що двигуни зібрані, а робот рухається, наведена вище комбінація рухатиме обидва двигуни в одному напрямку, штовхаючи робота вперед.

Щоб правильно керувати H-Bridge, також повинні працювати з контактами дозволу. Наведена вище комбінація, яка рухатиме робота вперед, працюватиме, лише якщо контакти ввімкнення (eneLeftMotor і eneRightMotor) перебувають у високому рівні. Можемо підключити контакти L293D (1 і 9) безпосередньо до +VCC і забути про них. Але для крапки ці кегли повинні краще бути в LOW. Крім того, зв'язування контактів увімкнення з цифровими виходами ШІМ NodeMCU дозволить контролювати швидкість двигуна (використання цифрових значень як HIGH і LOW встановить швидкість на MAX і ZERO відповідно).

Отже, щоб створити функцію, яка рухатиме нашого робота вперед, повинні зібрати такий код:

```
void forwardMotor(void)
{
digitalWrite(eneLeftMotor,HIGH);
digitalWrite(eneRightMotor,HIGH);
digitalWrite(leftMotor1,HIGH);
digitalWrite(leftMotor2,LOW);
digitalWrite(rightMotor1,HIGH);
digitalWrite(rightMotor2,LOW);
}
```

У попередньому кроці дізналися, як можна рухати робота вперед, тепер подумаємо, як його рухати взагалі.

Визначимо 5 можливих наступних команд:

- стояти;
- повернутися вліво;
- повернутися вправо;
- зворотний хід;
- хід вперед.

Перша команда «СТОП» проста у виконанні. Усі входи H-Bridge мають бути LOW, таким чином двигуни не рухатимуться:

```
void stopMotor(void)
{
digitalWrite(eneLeftMotor,LOW);
digitalWrite(eneRightMotor,LOW);
digitalWrite(leftMotor1,LOW);
digitalWrite(leftMotor2,LOW);
digitalWrite(rightMotor1,LOW);
digitalWrite(rightMotor2,LOW);
}
```

Так само подумаємо про поворот робота в одному напрямку, скажімо вліво. Вважаємо, що робот рухається вперед, якщо хочемо повернути ліворуч, можемо мати дві ситуації:

- зупинити лівий двигун і продовжувати рухатися правий;
- повернути лівий двигун заднім ходом і продовжувати рухатися вправо.

У першій ситуації робот зробить траєкторію дуги вліво. На другому – робот поверне свою вісь ліворуч. Тепер будемо реалізовувати другий варіант.

```
void leftMotor(void)
{
digitalWrite(eneLeftMotor,HIGH);
digitalWrite(eneRightMotor,HIGH);
digitalWrite(leftMotor1,LOW);
digitalWrite(leftMotor2,HIGH);
digitalWrite(rightMotor1,HIGH);
digitalWrite(rightMotor2,LOW);
}
```

Інші команди слідують тій же логіці.

Дотримуємося наведеної на рис.3.5 схеми та підключимо Robot HW.

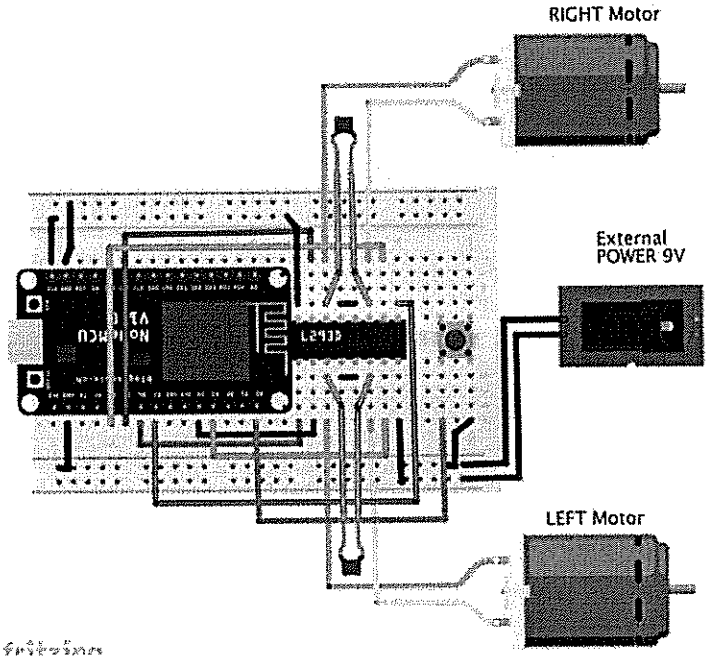


Рис. 3.5 Схема Robot HW

Можемо зробити прості тести, щоб переконатися, що код у порядку. Це добре для спрощення тестів, для введення «Кнопки» для запуску робота. Встановимо його на порт NodeMCU D0, як показано на схемі.

Коли натискаємо кнопку, робот починає виконувати рухи, визначені в loop(). він триватиме, доки не натиснемо «Скинути» на NodeMCU. При натисканні кнопки цикл повторюється.

Повний код можна завантажити з GitHub: https://github.com/Mjrovai/WiFi-Voice-Controlled

Robot/tree/master/WiFi_Robot_NodeMCU_Android_Voice_Motor_tests

3.3 Додаток для Android

Використовуватимемо MIT App Inventor на рис.3.6 для розробки програми Android. MIT App Inventor — середовище візуальної розробки android-застосунків, що вимагає від користувача мінімальних знань програмування.

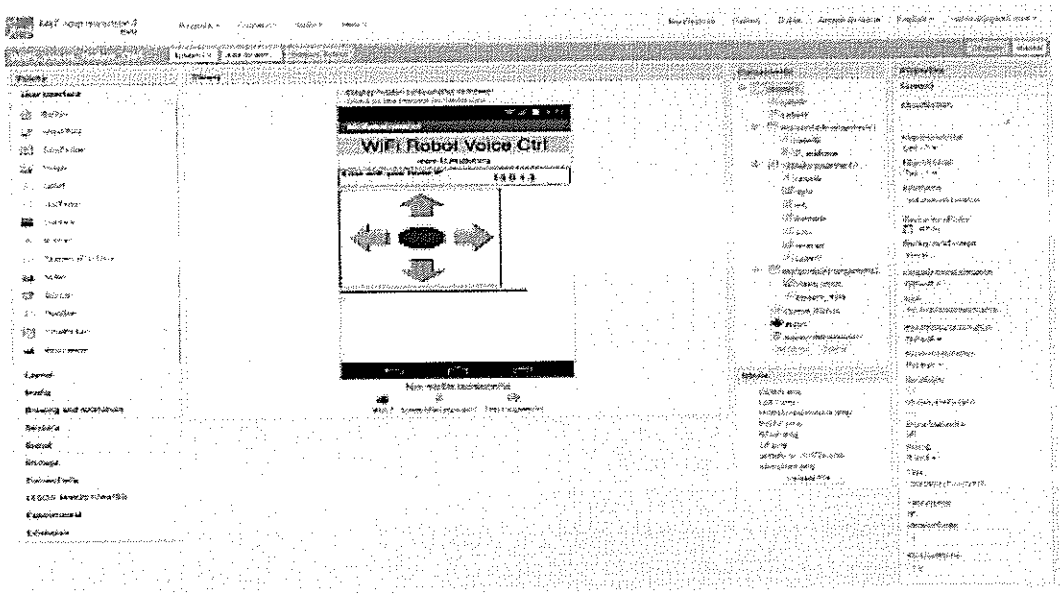


Рис. 3.6 MIT App Inventor

Повинні на вкладках Блоки створити 5 кнопок. Всі вони будуть відповідати структурі зображеної на рис.3.7.

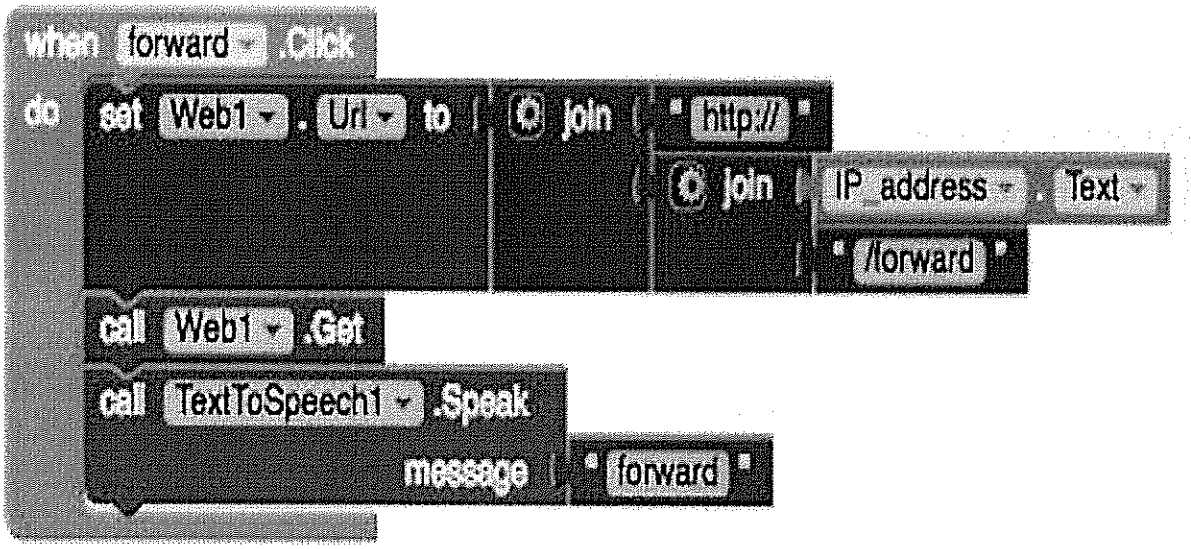


Рис. 3.7 Відповідні структури створення додатку

Цей блок кнопок викликається при натисканні кнопки «Вперед» («ВГОРУ»). Наприклад, коли натискаєте кнопку вперед, буде виконано 3 де Команда буде надіслана у форматі: http:/ip_address*/forward, потім очікується «відлуння» на тому ж форматі і програма прочитає звукове «повідомлення» у регістрі «вперед».
IP_Address буде тією, яку введемо на екрані. За замовчуванням 10.1.0.3, тому справжнє повідомлення буде таким: http:/10.0.1.3/forward.

Можемо використовувати будь-яке повідомлення, яке хочемо, або навіть видалити цей блок. Це необов'язково для проєкту.

Додаток для Android: Розпізнавання голосу

Зауважимо, що для будь-якої введеної голосової команди результатом буде команда в нижньому регістрі. Це полегшить декодування розпізнавання голосу на NodeMCU.

Наприклад, якщо хочемо просунути робота вперед, необхідно надіслати слово чи речення, щоб код NodeMCU їх точно розпізнав. Надішлемо команду

мовою, але повинні надіслати її своєю рідною мовою тією, яка налаштована на пристрої Android і правильно змінити код NodeMCU.

Отже, коли кажемо «переслати», програма надішле, наприклад, http:/10.0.1.10/forward , і NodeMCU візьме те, що отримано після «/», тобто команду «вперед». За допомогою цієї команди буде викликана функція forwardMotor().

Програма Android: маніпуляції помилками

Якщо сталася помилка, наприклад, коли вимовляємо голосову команду, яку не розпізнає NodeMCU, вищезгаданий блок запише деталі помилки в останній рядок (Comm_Status) програми, як показано на рис.3.8.

Тепер можемо створити свою програму крок за кроком, як показано на попередніх кроках, або завантажити повний проект (.aia) у MIT App Inventor, змінивши його відповідно до своїх потреб. Крім того, якщо немає досвіду розробки програм для Android, можна запустити файл .apk безпосередньо на своєму пристрої Android.

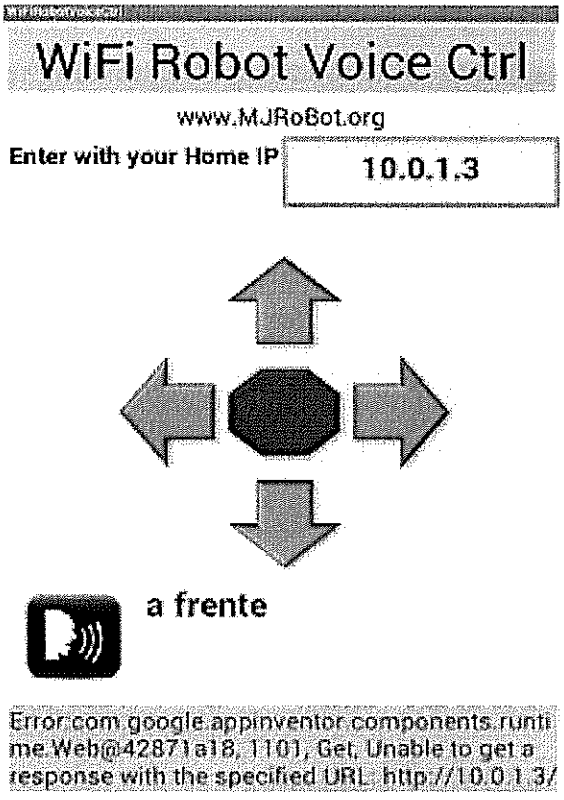


Рис. 3.8 Деталі помилки в останньому рядку (Comm_Status) програми

4 ЗАСОБИ БЕЗПЕКИ ТА ДОДАТКОВІ АВТОМОБІЛЬНІ ПРИСТРОЇ

4.1 Viper DS4

Viper DS4 — це система дистанційного запуску, яка включає БЕЗКОШТОВНЕ керування автомобілем через Bluetooth і статус автомобіля за допомогою мобільного додатку Viper SmartStart. Дистанційно запускайте, блокуйте або розблокуйте свій автомобіль за допомогою смартфона на відстані до 150 футів*. Не вимагає плану обслуговування Viper SmartStart.

Радіус дії понад 1 милю з додатковими комплектами дистанційного керування.

Дистанційний запуск, блокування, розблокування та перевірка стану автомобіля. Флагманська цифрова система Viper, яка захищає ваш автомобіль від сучасних крадіжок, додаючи додатковий рівень безпеки для автомобілів, які НЕ обладнані заводськими іммобілайзерами. Можна підключитися до Viper SmartStart Pro на рис.4.1, щоб додати місцезнаходження та глобальний діапазон.

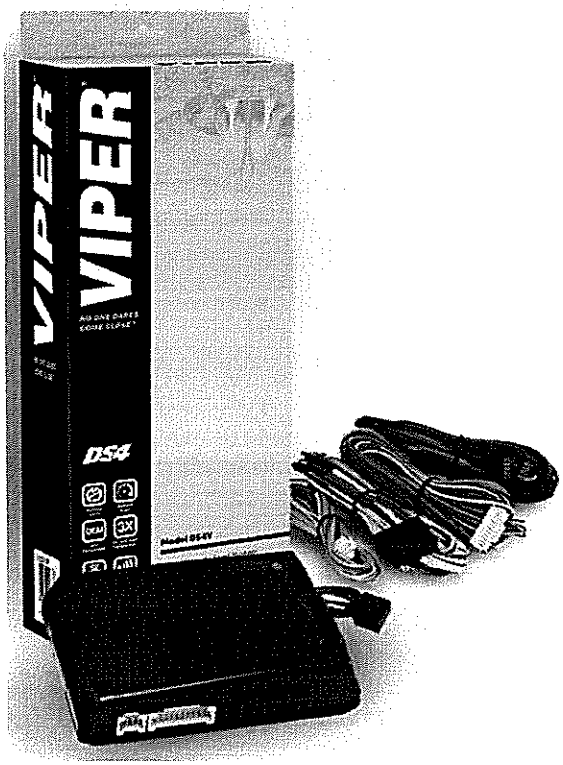


Рис. 4.1 Viper DS4

Радіус дії понад 1 милю з додатковими комплектами дистанційного керування. Дистанційний запуск, блокування, розблокування та перевірка стану автомобіля. Флагманська цифрова система Viper, яка захищає автомобіль від сучасних крадіжок, додаючи додатковий рівень безпеки для автомобілів, які не обладнані заводськими іммобілайзерами.

Потрібно підключіться до Viper SmartStart Pro, щоб додати місцезнаходження та глобальний діапазон.

Viper DS4 — це чотири ключові мобільні технології, інтегровані в один пристрій! Viper DS4 дає вам змогу дистанційно запускати автомобіль, щоб нагріти або охолодити його салон перед поїздкою ще до того, як ви сідете в нього! Він захищає ваш автомобіль за допомогою системи безпеки сирени. Інтерфейс включений, додаткова покупка не потрібна. І, нарешті, передова технологія Bluetooth Smart® робить ваш смартфон потужним розширенням вашого автомобіля. З Viper SmartStart Pro або Viper Connect розширте діапазон використання за межі Bluetooth через стільникову мережу, підключивши вас до вашого автомобіля практично з будь-якої точки світу!

Робочий діапазон базується на тестуванні прямої видимості та без перешкод в ідеальних умовах. Фактичний діапазон залежить від місцевих умов, включаючи, але не обмежуючись, навколишнє середовище, рельєф місцевості, фізичні перешкоди, розташування та орієнтацію автомобіля, перешкоди та інші можливі перешкоди.

Для глобального діапазону потрібен план обслуговування та Viper SmartStart Pro або Viper Connect (продаються окремо).

4.2 Протиугінна сигналізація ESP32

Розглянемо проект домашньої автоматизації, розумну протиугінну систему сигналізації, тобто сигналізацію, підключену до телефону та Alexa.

Сигналізація, може мати різні датчики відкривання дверей і вікон. Можемо додати багато датчиків до сигналізації, усі підключені до мережі WiFi.

За допомогою програми можемо вмикати та вимикати будильник за допомогою коду, і, звичайно, якщо будильник спрацьовує, отримуємо сповіщення на телефон. Сповіщення, які отримуємо, також показують, який датчик спрацював, що дуже корисно знати, які двері було відкрито.

Поверх дверного датчика також є ці світлодіоди, які можна запрограмувати, щоб вказувати різні речі, як статус сигналізації, тобто, чи вона увімкнена, чи щось її спрацювало, так і інші сповіщення від нашого розумного дому. Наприклад, можна встановити, ще один із цих світлодіодів увімкнеться, коли в будинку горить принаймні одне світло, тож коли виходимо з дому, можна одразу побачити, чи не забули вимкнути якесь світло. Той факт, що на ньому є світлодіоди, які вказують інші речі, дуже зручні, але не бачив цього в інших продуктах розумного будинку. Для цього проекту нам потрібні два основні компоненти, це плата ESP8266 або ESP32 - вона схожа на Arduino, але має набагато потужніший чіп і підключення до WiFi і магнітний перемикач - працює як перемикач, який при наближенні магніту замикає ланцюг. Для цього проекту магніт буде розміщено на дверях, а датчик на стіні, щоб визначити, коли двері відкриваються. Тоді нам знадобляться наступні речі:

- адресна світлодіодна стрічка WS2812B (4шт. світлодіодів);
- провід;
- нитка для 3D принтера;
- біле оргскло;
- паяльник;
- 3D принтер;
- ПК;
- гарячий клей.

Щоб створити цей проект, також потрібно встановити Home Assistant на Raspberry pi або на ПК (за допомогою віртуальної машини).

4.3 Домашній помічник і ESPhome

Подивимося на програмне забезпечення, яке буде працювати на платі ESP32. У наступних кроках також побачимо, як створити датчик відкриття дверей. Сигналізація буде підключена до Home Assistant. Home Assistant – це система домашньої автоматизації, яка працює локально, що дозволяє керувати всіма пристроями домашньої автоматизації, такими як розумні лампочки та розетки, з одного інтерфейсу на рис.4.1.

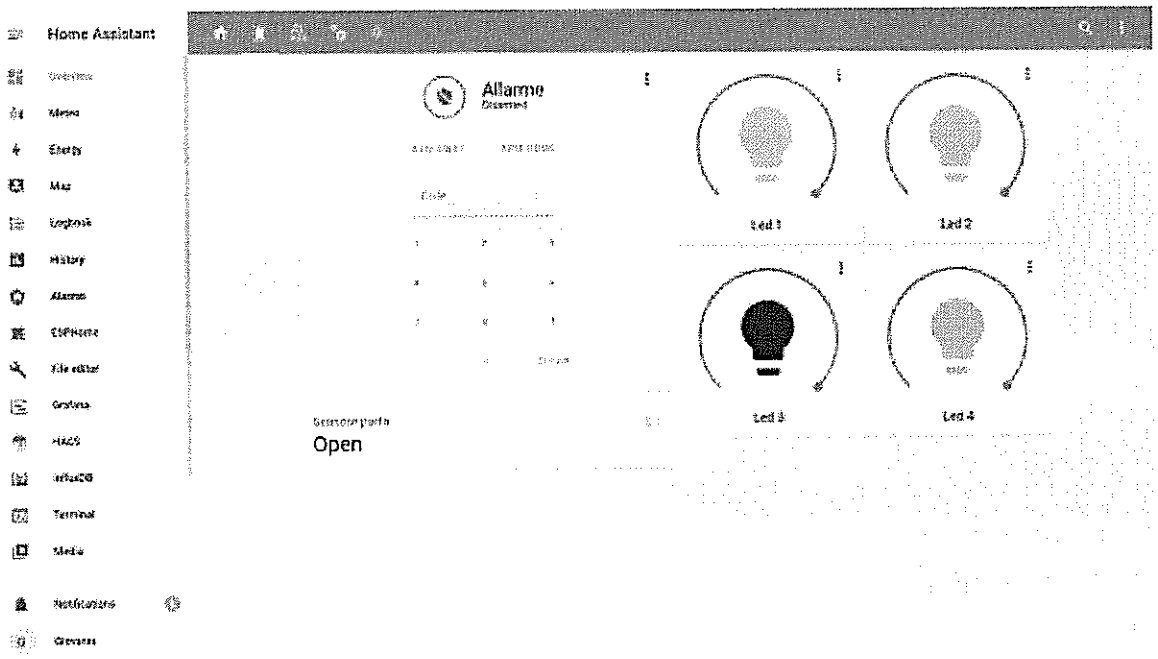


Рис. 4.2 Інтерфейс керування пристроями

Для запуску Home Assistant використовуємо ПК з Windows, на якому працює віртуальна машина, але якщо вона є, можемо використовувати Raspberry pi, яка споживає менше енергії. Щоб переглядати дані зі смартфона, можемо завантажити програму Home Assistant. Для підключення поза локальною мережею використовуємо Nabu Casa Cloud, це найпростіше рішення, але воно не безкоштовне. Є й інші рішення, але вони не зовсім безпечні.

Таким чином, у додатку Home Assistant зможемо вмикати та вимикати сигналізацію та отримувати сповіщення, коли будильник увімкнено.

Щоб підключити ESP32 до Home Assistant, будемо використовувати ESPhome. ESPhome — це доповнення, яке дозволяє підключати плати ESP до Home Assistant через WiFi. Щоб підключити ESP32-cam до ESPhome, потрібно виконати такі дії:

- встановити плагін ESPhome у Home Assistant;
- на інформаційній панелі ESPhome натиснути «Новий пристрій» і «Продовжити»;
- дати пристрою назву;
- обрати ESP32 або плату, яку використовували;
- скопіювати наданий ключ шифрування, він знадобиться пізніше;
- натиснути редагувати, щоб побачити код пристрою;
- у розділі wifi ввести ssid і пароль Wi-Fi.

Щоб зробити з'єднання більш стабільним, можемо надати платі статичну IP-адресу за допомогою такого коду:

```
wifi:
ssid: yourssid
password: yourwifipassword
manual_ip:
# Set this to the IP of the ESP
static_ip: 192.168.1.61
# Set this to the IP address of the router. Often ends with .1
gateway: 192.168.1.1
# The subnet of the network. 255.255.255.0 works for most home networks.
subnet: 255.255.255.0
```

У кінці коду вставимо наступні строки:

```
binary_sensor:
- platform: gpio
pin:
number: GPIO23
inverted: true
```

```
mode:
input: true
pulldown: true
name: "Sensore porta"
device_class: door
light:
- platform: fastled_clockless
chipset: WS2812B
id: light_fastled
pin: GPIO22
num_leds: 4
rgb_order: GRB
name: "Led sensore porta"
effects:
- pulse:
- platform: partition
name: "Led 1 sensore porta"
segments:
- id: light_fastled
from: 0
to: 0
effects:
- pulse:
- platform: partition
name: "Led 2 sensore porta"
segments:
- id: light_fastled
from: 1
to: 1
effects:
```

```
- pulse:
- platform: partition
name: "Led 3 sensore porta"
segments:
- id: light_fastled
from: 2
to: 2
effects:
- pulse:
- platform: partition
name: "Led 4 sensore porta"
segments:
- id: light_fastled
from: 3
to: 3
effects:
- pulse:
```

Перша частина коду визначає магнітний перемикач, який визначає, відкриті двері чи ні. Потім зі світлом визначаються адресні світлодіоди, якими керуватиме автоматика Home Assistant.

Після завершення коду можемо натиснути «Встановити», підключити ESP32 до комп'ютера за допомогою USB-кабелю та дотримуючись інструкцій на екрані завантажимо код.

Коли ESP32 підключено до Wi-Fi, можемо перейти до налаштувань Home Assistant, де, ймовірно, побачимо, що Home Assistant виявив новий пристрій.

Натискаємо «Налаштувати» та вставимо туди ключ шифрування, який скопіювали раніше.

Тепер, коли завантажили програму, можемо підключити магнітний контакт до ESP32. За допомогою двох проводів підключаємо магнітний контакт між 3,3 В ESP32 і контактом 23. Тепер під'єднуємо джерело живлення до ESP32, і на Home

Assistant бачимо, що двері закриті або відкриті, коли наближаємося або рухаємо магніт подалі від датчика.

Теоретично датчик для сигналізації працює і все б добре, але вирішено поставити світлодіоди на датчик. Можливо, наявність світлодіодів на датчику сигналізації може здатися трохи дивною, але насправді, це дуже зручно. Насправді ці світлодіоди можна запрограмувати на сигналізацію стану сигналізації та стану інших пристроїв домашньої автоматизації. Так, наприклад, коли виходимо за двері, можемо одразу побачити, чи забули вдома світло, тому що буде світлодіод, який сигналізує про це на рис.4.3.

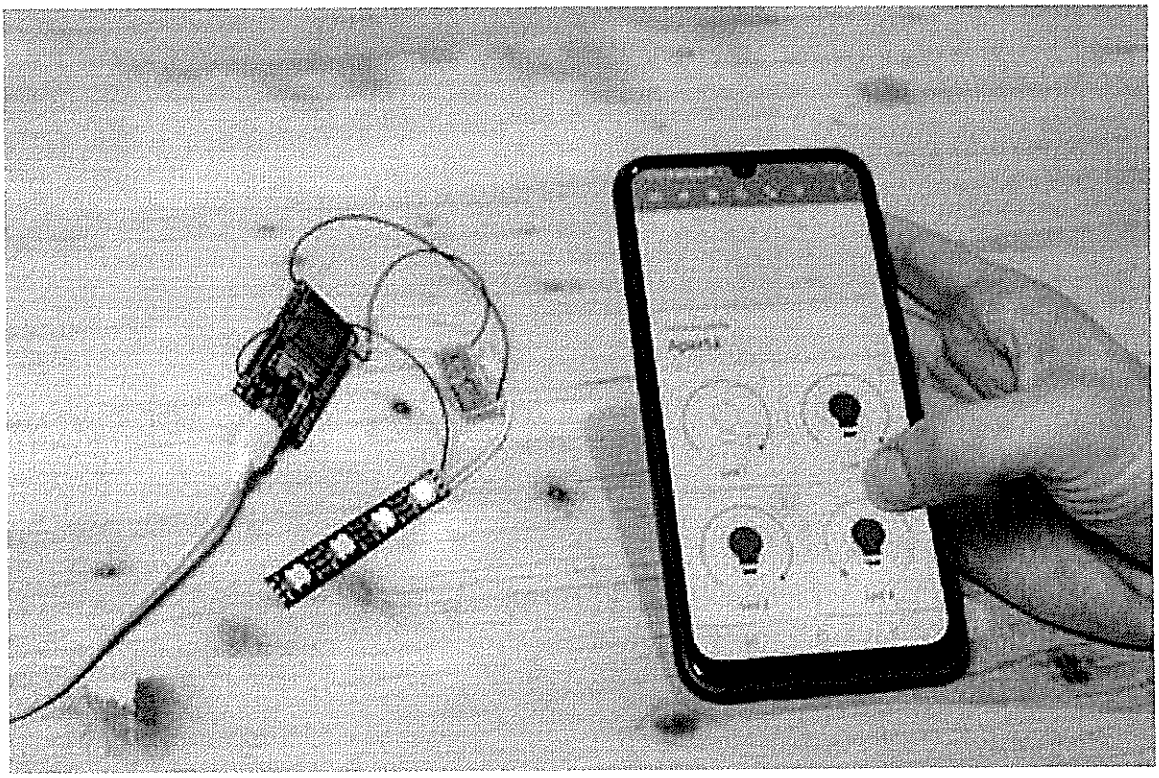


Рис. 4.3 Світлодіодна сигналізація

Світлодіоди, які використовуватимуться для додавання цієї функції, є індивідуально адресованими світлодіодами rgb, що на рис.4.4. Ці світлодіодні стрічки не мають звичайних світлодіодів rgb, оскільки ви можете керувати кольором кожного світлодіода окремо, підключивши один провід для даних за допомогою Arduino або подібної плати. Для цього проекту я вирізав частину з 4

світлодіодів. Я припаяв три дроти до світлодіодної стрічки, два для живлення і один для входу даних, який позначений стрілкою. Я під'єднав джерело живлення світлодіодної стрічки до 5 В і GND esp32, а дані – до контакту 22. Тож тепер із Home Assistant я також можу вмикати та вимикати кожен світлодіод, а також змінювати колір. Пізніше ми також побачимо, як підключити ці світлодіоди до автоматики.

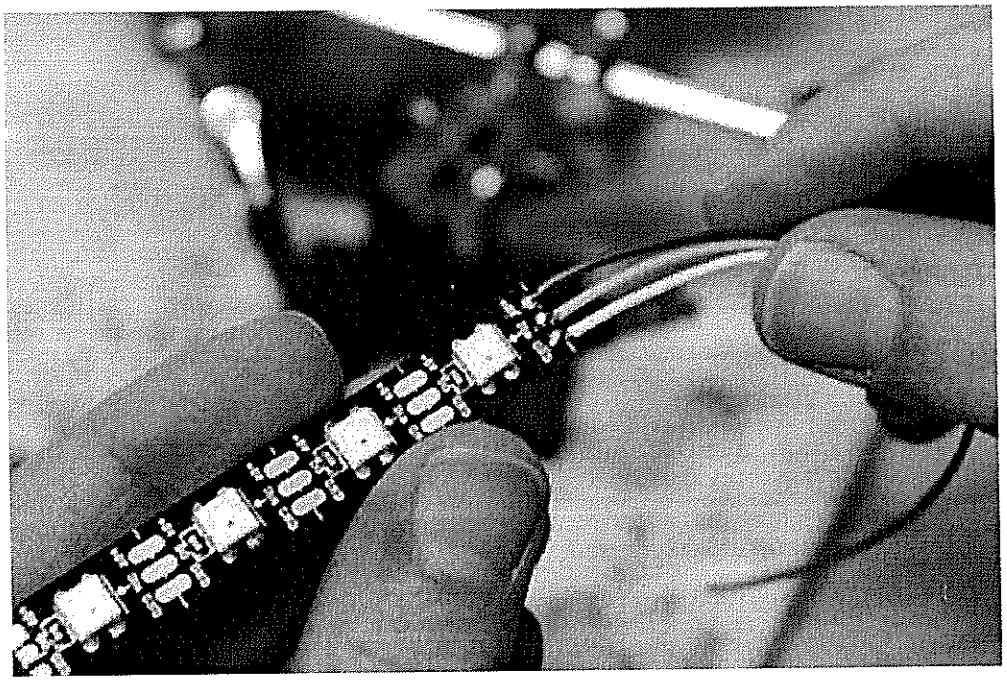


Рис. 4.4 Адресовані світлодіоди rgb

Тепер схему закінчено, але їй все ще бракує коробки, щоб її поставити. Тож можна розробити і надрукувати на 3D невелику коробку з кришкою. Щоб розсіяти світло світлодіодів, будемо використовувати непрозоре оргскло, тому виріжемо шматок і приклеїмо його під отвір у кришці коробки. Знизу покладемо шматок світлодіодної стрічки. Потім покладемо ESP32 у коробку, вирівнявши порт USB з отвором. Потрібно приклеїти магнітний контакт біля стінки ящика, щоб магніт міг його активувати. Закриваємо коробку 4 гвинтами.

Для живлення датчика використовується блок живлення USB. І датчик відкриття дверей, і світлодіоди працюють добре, тому можемо встановити датчик на двері.

Тепер потрібно перетворити датчик на справжню сигналізацію. Для цього скористаємося інтеграцією Alarmo Home Assistant. Ця інтеграція дозволяє створити справжню систему сигналізації з різними датчиками, підключеними до Home Assistant.

Щоб завантажити цю інтеграцію, можемо скористатися Home Assistant Community Store (HACS). Встановити його дуже просто, оскільки він ним користується.

Після того, як відкрили сторінку налаштувань інтеграції, на вкладці «Загальні» можемо встановити різні режими будильника («Озброєний у гостях», «Озброєний вдома», «Озброєний у відпустку»), кожен зі своїми налаштуваннями. У кожному режимі будильника можна встановити затримку на вихід і вхід.

На вкладці «Датчики» можемо додати до системи сигналізації різні датчики, підключені до Home Assistant наприклад додати присутність датчика, який щойно створили.

На вкладці «Коди» ви можете встановити різні коди для постановки/зняття з охорони сигналізації, призначеної різним користувачам.

У вкладці «Дії» можемо налаштувати отримання сповіщень на телефон про спрацьовування будильника, а також у сповіщенні додати назву датчика, який спрацював, дату та час — ця інформація дуже корисна.

На вкладці «Дії» також можемо створити певну автоматизацію на основі стану тривоги (наприклад, увімкнути сирену), але вони ще не пропонують багато функцій. Інтеграція Alarmo також надає картку для інформаційної панелі Home Assistant.

Щоб керувати світлодіодами, які поставили на датчик, можемо використовувати класичну автоматизацію Home Assistant. Наприклад, обираємо, щоб перші два світлодіоди вказували на стан тривоги різними кольорами: коли будильник вимкнено, світлодіоди були синіми, коли поставлено на охорону, вони світилися зеленим, коли будильник вимкнено, світлодіоди блимали червоним, а коли таймер, після якого спрацьовує будильник, вони жовті. Різні статуси тривоги доступні як умови в автоматизації, тому зробити цю автоматизацію дуже просто.

Третій світлодіод вмикається, коли в будинку горить принаймні одне світло, тож, коли виходимо, одразу бачимо, чи не забули вимкнути якесь світло.

Тепер, коли все запрограмували, залишається лише перевірити, чи працює сигналізація на рис.4.5.

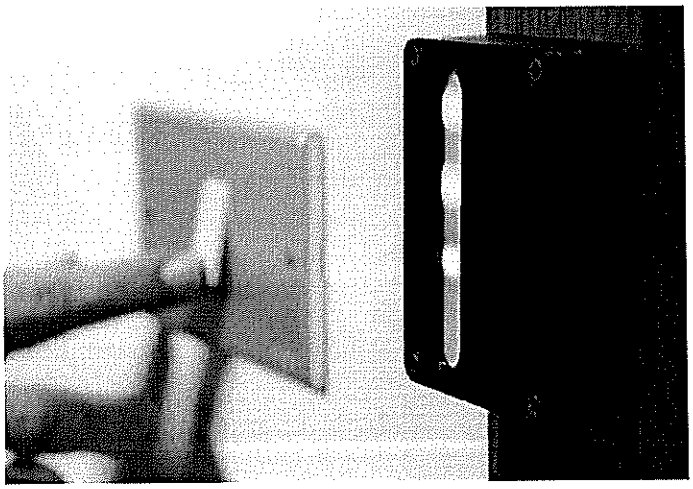


Рис. 4.5 Перевірка роботи сигналізації

4.4 Автомобільний резервний датчик

Розглянемо базову схему Arduino Uno для резервного датчика автомобіля. Схема на рис.4.6 використовуватиме ультразвукові датчики для виявлення перешкод позаду автомобіля та надання зворотного зв'язку водієві.

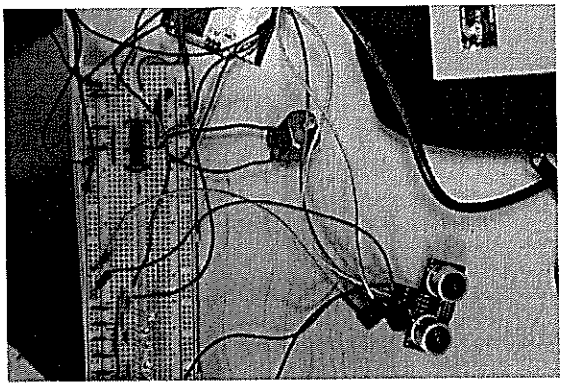


Рис. 4.6 Схема виявлення перешкод позаду автомобіля

Для створення такої схеми необхідні наступні компоненти:

- плата Arduino Uno;
- ультразвукові датчики (HC-SR04);
- перемички;
- двигун h-міст;
- температурний сенсор;
- LDR;
- 3 резистори по 1кОм;
- 2 резистора 220 Ом;
- зумер або світлодіод (для зворотного зв'язку).

4.5 Створення концепції керування

Для з'єднання ланцюгів потрібно підключити контакт VCC ультразвукового датчика до контакту 5 В на Arduino Uno, підключити контакт GND ультразвукового датчика до контакту GND на Arduino Uno, а контакт TRIG ультразвукового датчика до будь-якого цифрового контакту (наприклад, Pin 2) на Arduino Uno. Потім підключитиь контакт ECHO ультразвукового датчика до іншого цифрового контакту (наприклад, Pin 3) на Arduino Uno.

Підключити плюсову клему зумера або анода світлодіода до цифрового контакту (наприклад, Pin 4) на Arduino Uno і мінусову клему зумера або катода світлодіода до контакту GND на Arduino Uno. Підключити живлення та заземлення до моста h і підключити його до arduino. Нарешті підключити датчик температури до живлення та заземлення та до arduino.

Є стаття на Хабре про кермо, де торкнулися теми steer-by-wire. Народ у коментарях висловив сумніви щодо надійності такого рішення. Адже насправді, що робити, якщо у якогось ECU раптово пропаде живлення, перетереться проводок чи підвисне софт? Як виробники борються із такими ризиками? І навіщо відмовлятися від надійного механічного зв'язку?

Почнемо з короткого огляду серійних моделей, в які встановлюють кермо по проводах. Першим і поки що єдиним автовиробником з подібною технологією на ринку є компанія Nissan з технологією Direct Adaptive Steering (DAS) на рис.4.7, яка застосовується в деяких моделях Infinity: Infinity Q50, Infinity Q60. Перші автомобілі з DAS вийшли в далекому 2013 році. У маркетингових матеріалах компанія вказує на ключові переваги: швидкість реакції, конфігурованість та можливість повністю прибрати вібрації на рульовому колесі.

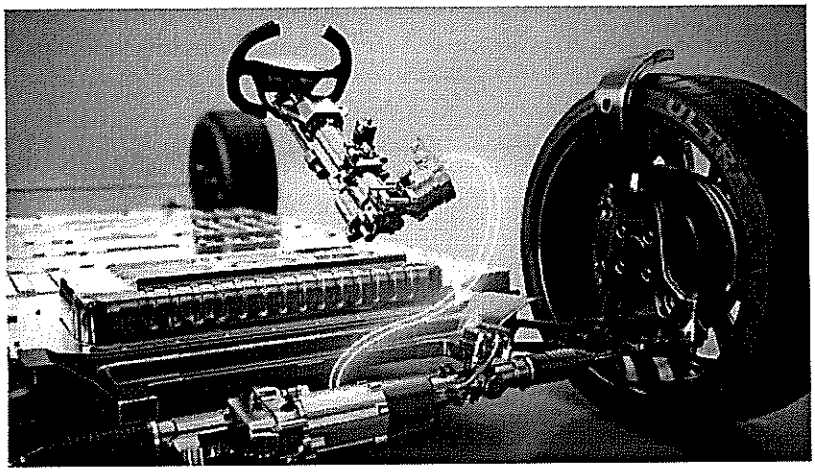


Рис. 4.7 Технологія Direct Adaptive Steering (DAS)

Tesla анонсувала появу steer-by-wire вже 2023 року. Крім інших переваг, це дозволить зробити кермо-штурвал зручнішим за рахунок збільшення кута повороту при низьких швидкостях. Тоді кут повороту керма можна обмежити 150 градусами. Компанія Toyota анонсувала технологію One-motion grip, яку планують встановлювати як моделі Lexus, так і моделі Toyota. Почати продажі обіцяли вже 2024 року. Що примітно, такою системою комплектуватиметься кермо-штурвал. Інформацію про steer-by-wire рішення можна знайти і у найбільших виробників автомобільних компонентів: Bosch, ZF, Conti. До переваг такого підходу відносять:

- велику свободу у проектуванні інтер'єрів;
- зниження складності розробки, збирання та обслуговування автомобіля;
- зменшення ваги автомобіля;

- підвищення надійності рахунок спрощення чи виключення деяких механічних вузлів;

- конфігурованість: можна змінювати передавальне число повороту кермового колеса та налаштовувати “зворотний зв'язок”;

- підвищення безпеки за рахунок впровадження розвинених систем допомоги водієві.

Тобто розробка та використання йде повним ходом. Провідні виробники докладають своїх зусиль. Схема "кермо по дротах" виглядає дуже просто. Зібрати прототип на простому МК з Алі можна за вечір! Так ще й переваг маса! Але Infinity, яка вже 10 років використовує цю технологію, ставить її лише на кілька своїх седанів. Інноваційна Tesla тільки обіцяє зробити steer by wire цього року. То в чому ж проблема?

Кермо через вал і кермовий механізм жорстко пов'язане з колесами. Водій повністю контролює ситуацію і може навіть завадити розумній електроніці втрутитися у керування. Але така схема вносить і певні складнощі. Необхідність розмістити громіздку конструкцію накладає обмеження на компонування автомобіля. Велика кількість рухомих і тертьових між собою елементів знижує ККД кермового механізму і підвищує знос деталей. Вимоги безпеки змушують вбудовувати поршневі механізми, що складаються в рульову колонку, ще більше ускладнюючи конструкцію. Гідропідсилювач керма помітно збільшує витрату палива. Електропідсилювач суттєво зменшує інформативність керма. При цьому через жорсткий зв'язок із колесами дуже складно прибрати вібрації на рульовому колесі. Але подібна схема має важливу перевагу - вона перевірена часом, досить проста і надійна, а також дуже безпечна. Щоб краще розібратися в такому банальному понятті як безпека, спробуємо звернутися до сучасних світових стандартів.

ISO 26262 – це об'ємний документ, що описує весь життєвий цикл як окремих вузлів, так і всього автомобіля загалом. Стандарт трохи більше 10 років, часто він не є обов'язковим, але в індустрії його поважають і прагнуть виконувати, хоч це і робить процес розробки сильно бюрократизованим і неповоротким. Крім того,

відповідність процесів стандарту ISO 26262 може полегшити відповідальність розробника у разі аварії через відмову системи. Але ми зараз не будемо глибоко занурюватися у вивчення документа, а наведемо лише ключові для нас концепції.

На ранній стадії проекту ISO 26262 вимагає аналіз небезпек і оцінку ризику виникнення такої небезпеки. Для кожної небезпеки визначається мета безпеки. Простіше кажучи, є небезпека того, що з датчика кута повороту керма випаде конектор. Значить мета безпеки - мінімізувати ймовірність такої події, швидко виявити випадання конектора та вжити заходів. Для ранжування вимог безпеки ввели рівні ASIL (Automotive Safety Integrity Level). Є 4 рівні, від A до D, де D - найвищий необхідний рівень безпеки.

Спрощено, рівень залежить від тяжкості наслідків у разі відмови, допустимої частоти виникнення відмов і можливості контролювати систему у разі відмови. Відмова кермового управління з великою ймовірністю може призвести до загибелі людей. Така небезпека відповідає рівню ASIL-D і допускає не більше однієї відмови на 100 млн годин роботи. Такі системи, як кермо, гальма, ABS, подушки безпеки повинні відповідати ASIL-D рівню. А для камери заднього виду та стоп-сигналів достатньо рівня ASIL-B як показано на рис. 4.8.

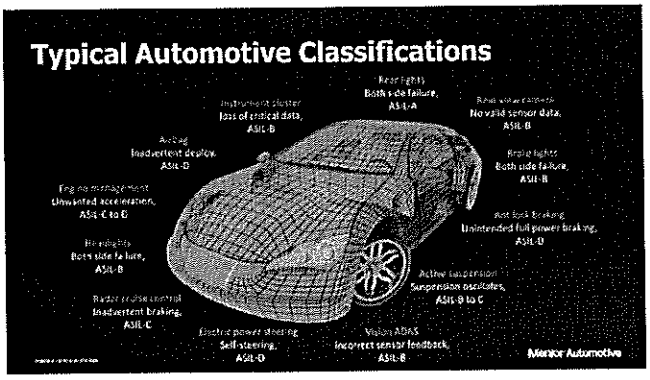


Рис. 4.8 Проект ISO 26262

Так, із рівнями безпеки начебто розібралися. Але як зрозуміти, що система задовольняє потрібний рівень безпеки? Можна зробити 5000 екземплярів своєї системи і експлуатувати її в різних умовах протягом десяти років, а потім

проаналізувати всі відмови, що виникли. Але, мабуть, автовиробники роблять не зовсім так.

Сучасні системи зазвичай розробляють за стандартами безпеки, що є доказом безпеки системи. Тобто там застосовуються всі етапи життєвого циклу, які включають аналіз небезпек та ризиків, розробку концепції функціональної безпеки, а також валідацію. Аргументи функціональної безпеки, це не тільки демонстрація надійності під час експлуатації, але також функціональні рішення, що забезпечують захист від проаналізованих небезпек.

Іншими словами, якщо у є документ із переліком небезпек та ймовірностей їх виникнення, і для кожної небезпеки прораховано, як цю небезпеку уникаємо, а також можемо підтвердити цю функціональність тестами, можемо вважати нашу систему досить надійною та безпечною.

Наступна важлива для нас концепція – безпечна система має складатися з безпечних компонентів, або повинна контролюватись безпечними компонентами. А значить, у випадку зі steer-by-wire, рівню ASIL-D повинні відповідати датчик кута повороту керма, датчик крутного моменту, і чіп в ECU, софт, канал зв'язку між датчиками, ECU та двигунами кермового механізму, і самі мотори. Виходить, що все-таки не вдасться сертифікувати steer-by-wire на першому МК, що трапився, з Алі. Прийде попрацювати і знайти чіп із сейфіті, що дозволяє реалізовувати функції з рівнем безпеки ASIL-D.

Ну і останній елемент пазла – це принцип розкладання ASIL. У нашому випадку його можна спростити до звичайного дублювання критичної функціональності та встановлення зовнішнього супервізора (або кількох супервізорів). Є у нас кермо з рівнем ASIL-D, для якого потрібно використовувати датчик повороту керма рівня ASIL-D, МК рівня ASIL-D, софт рівня ASIL-D, CAN рівня ASIL-D і так далі. Чим вище рівень ASIL, тим складніше і дорожче розробка, тим важче знайти компоненти та підсистеми. Але якщо, наприклад, ми встановлюємо два датчики повороту керма, які працюють незалежно, вимоги до безпеки цих датчиків знижуються.

ВИСНОВКИ

Протокол WiFi у системі центрального керування транспортним засобом є важливим компонентом сучасних систем центрального керування транспортним засобом. З'єднуючи центральну систему керування та інші пристрої через безпроводову мережу, це забезпечує такі функції, як підключення до мережі, передача мультимедіа, діагностика автомобіля, дистанційне керування тощо.

З розвитком технологій безпроводоої мережі та популярністю центральних систем керування автомобілями, протокол Wi-Fi у центральній системі керування автомобілем матиме вищу швидкість передачі даних, ширші сценарії застосування, сильнішу безпеку та глибоку інтеграцію з автономним керуванням у майбутньому. Це забезпечить користувачам кращий досвід водіння та підвищить безпеку водіння.

Стандарт 802.11ac обіцяє допомогти розв'язати низку нових додатків у наших автомобілях. Виробники автомобілів і вторинного ринку прагнуть якомога швидше вивести свою продукцію на ринок.

Наявність компактних багатодіапазонних радіомодулів і допоміжних комплектів оцінки та драйверів забезпечать інженерам інструменти для досягнення таких цілей у найкоротший доступний час.

ПЕРЕЛІК ПОСИЛАНЬ

1. Andrew Patterson. Automotive infotainment systems: Open source drives innovation. Embedded Computing. Accessed: 2015-03-12. [Online]. Available: http://embedded-computing.com/articles/automotive-source-drives-innovation/.

2. BMW Case Study. GENIVI Alliance. Accessed: 2015-02-19. [Online]. Available: http://www.genivi.org/sites/default/files/BMW Case Study Download 040914.pdf.

3. An Architecture for In-Vehicle Infotainment Systems. Dr. Dobb's. Accessed: 2020-11-23. [Online]. Available: http://www.drdobbs.com/ embeddedsystems/anarchitecture-for-in-vehicle-infotainm/222600438.

4. Application software. Accessed: 2020-11-23. [Online]. Available: http://www.drdobbs.com/embedded-systems/Application software.

5. Concepts of the Middleware. Accessed: 2020-11-23. [Online]. Available: http://www.drdobbs.com/Middleware.

6. W. J. Zhang, S. X. Yu, Y. F. Peng, Z. J. Cheng, and C. Wang, "Driving habits analysis on vehicle data using error backpropagation neural network algorithm," in Computing, Control, Information and Education Engineering, vol. 55, CRC Press, Guilin, China, 2015.

7. H. Drucker, J. C. Chris, L. Kaufman, A. Smola, and V. Vapnik, "Support vector regression machines," in Advances in Neural Information Processing Systems, MIT Press, Cambridge, MA, USA. pp. 155–161, 1997.

8. H.-l. Feng, "Study on prediction model of ecological security index in Chongqing city based on SVR model," Computer Science, vol. 40, no. 8. 2013. pp. 245–248.

9. Andrew Patterson. Automotive infotainment systems: Open source drives innovation. Embedded Computing. Accessed: 2015-03-12. [Online]. Available: http://embedded-computing.com/articles/automotive-source-drives-innovation/.

10. Michael Kerrisk (2012-08-8). GENIVI: Moving an industry to open source. Accessed: 2015-02-11. [Online]. Available: http://www.genivi.org /sites/ default /files / in-the-news/2012 08 08 GENIVI%20 Moving% 20to%20Open %20Source %20-%20Michael%20Kerrisk.pdf.

11. BMW Case Study. GENIVI Alliance. Accessed: 2015-02-19. [Online]. Available: http://www.genivi.org/sites/default/files/BMW Case Study Download 040914.pdf.

12. An Architecture for In-Vehicle Infotainment Systems. Dr. Dobb's. Accessed: 2020-11-23. [Online]. Available: http://www.drdobbs.com/embeddedsystems/anarchitecture-for-in-vehicleinfotainm/22260043

13. Application software. Accessed: 2020-11-23. [Online]. Available: http://www.drdobbs.com/embedded-systems/Application software.

14. Concepts of the Middleware. Accessed: 2020-11-23. [Online]. Available: http://www.drdobbs.com/Middleware.

15. Theoretical Concepts of the Operating system. Accessed: 2020-11-23. [Online]. Available: http://theoretic_os.org/operating system.

16. Analyze of the Board Support Package. Accessed: 2020-11-23. [Online]. Available: http://articles.bsp.org/board_support_package.

17. Modern Device driver. Accessed: 2020-11-23. [Online]. Available: http://articles.bsp.org/Device driver.

18. Doug Newcomb. The next big OS war is in your dashboard. Wired. Accessed: 2015-03-12. [Online]. Available: http://www.wired.com/2012/12/automotive-oswar/all/ 50

ДЕМОНСТРАТИВНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра Мобільних та відеоінформаційних технологій

«Метод зовнішнього безпроводового керування автомобілем»

Виконав: здобувач вищої освіти
групи АРДМ-61
Землянікін Андрій

Мета роботи – є доведення ефективності використання технології Wi-Fi для реалізації керування автомобілем.

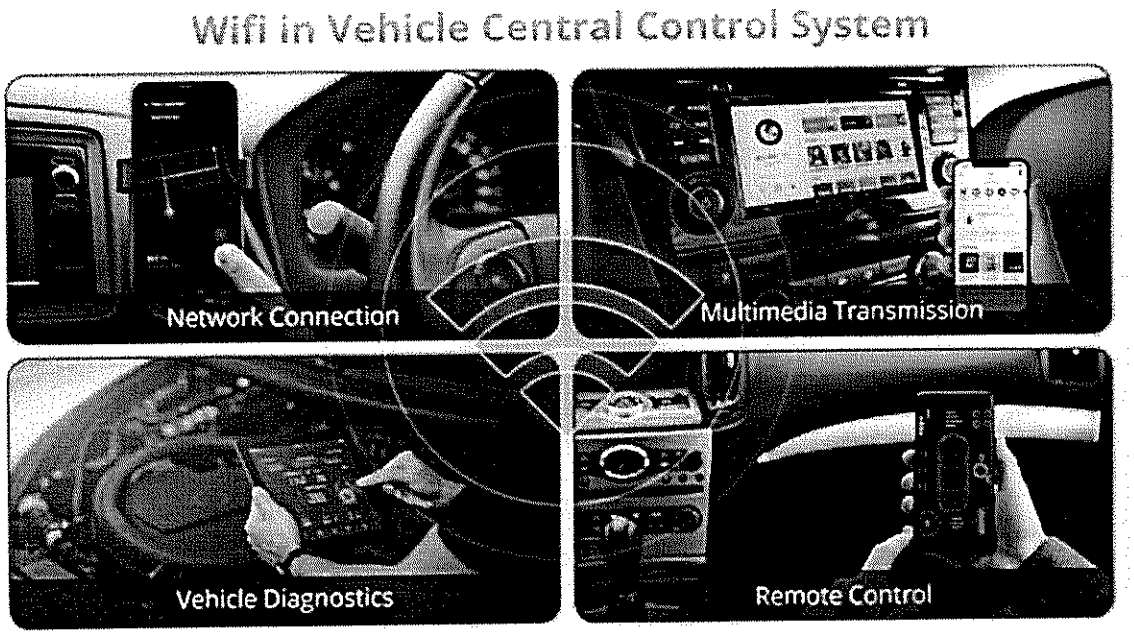
Об’єкт дослідження – процеси, системи та пристрої використовуючі технології Wi-Fi.

Предмет дослідження – принципи, моделі та методи використання технології Wi-Fi.

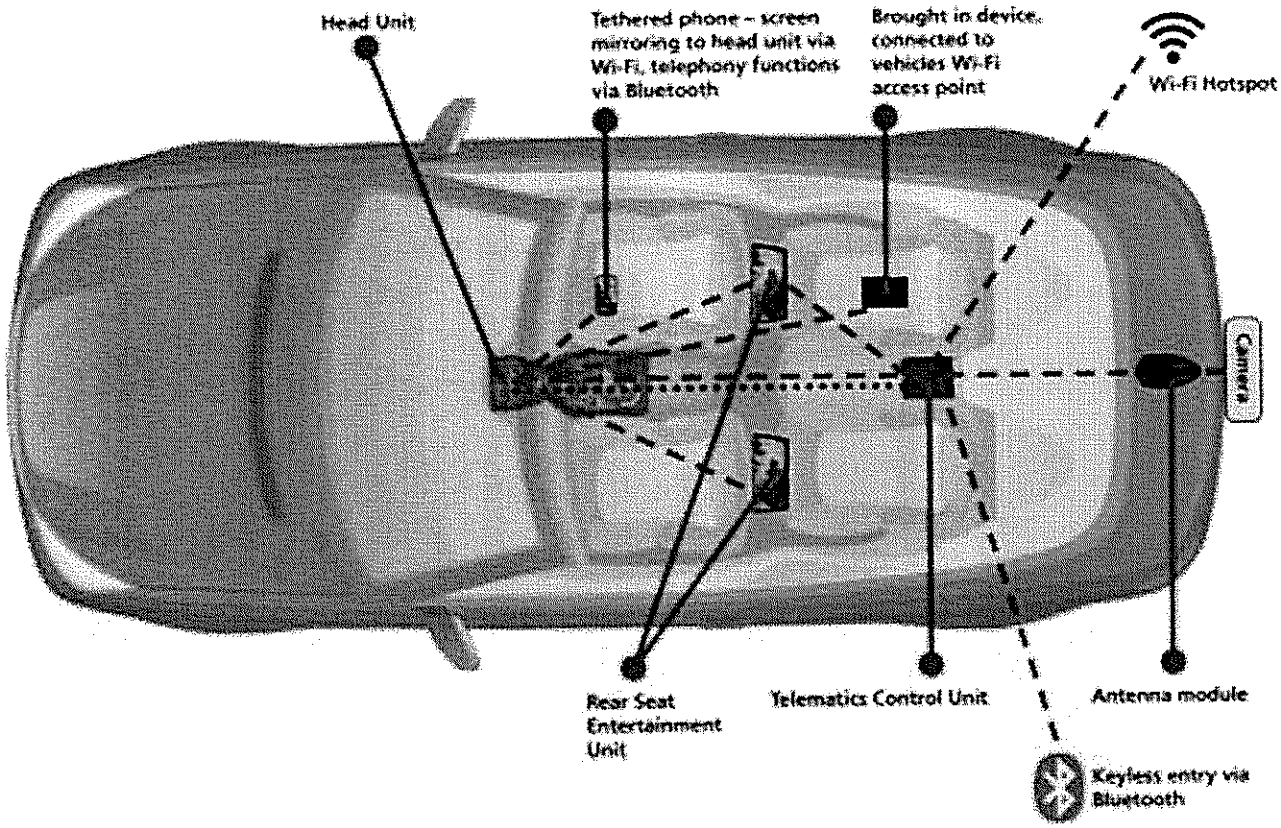
Застосування протоколу WiFi в центральній системі керування транспортним засобом

Принципи протоколу WiFi включають такі аспекти:

- забезпечити більш високі швидкості передачі та стабільніші з'єднання;
- забезпечує безпеку під час передачі даних;
- використовує для шифрування алгоритм WPA2 даних, запобігаючи несанкціонованому доступу та підробці даних;
- має різні застосування в практичних сценаріях;
- використовувати для передачі мультимедіа;
- для діагностики автомобіля;
- дистанційно керувати транспортним засобом.



Приклади застосування Wi-Fi у автомобілі



Комбіноване рішення Cypress CYW89650 Wi-Fi 6 і Bluetooth 5.0



Автомобільні точки доступу Wi-Fi





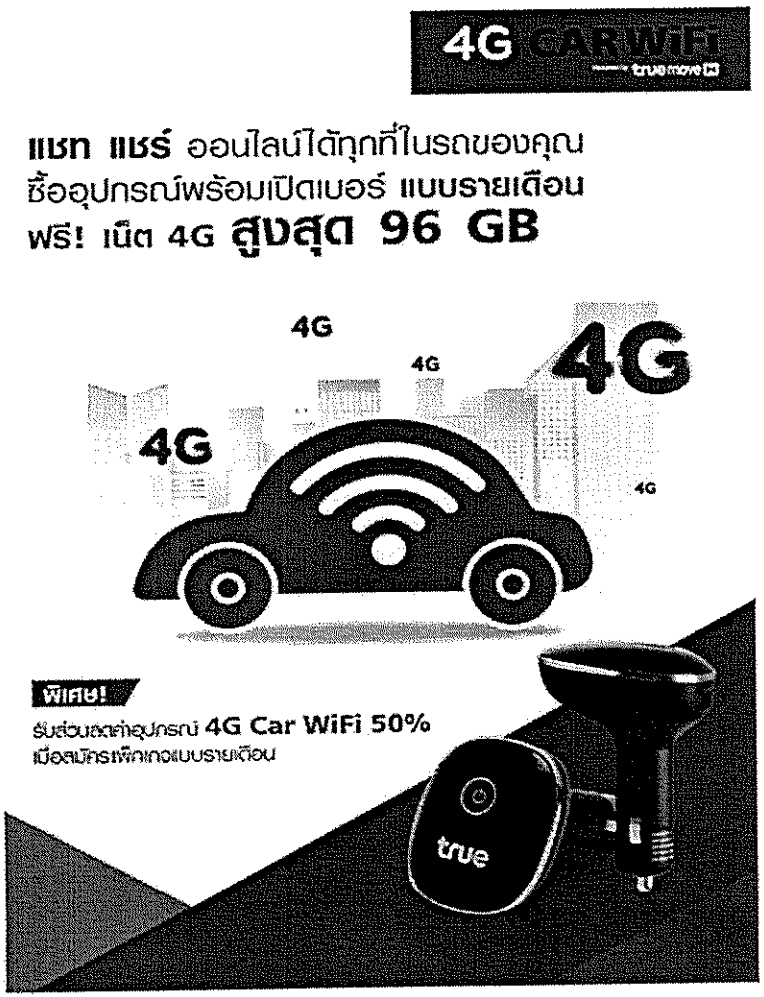


Декілька видів підключеної автомобільної електроніки

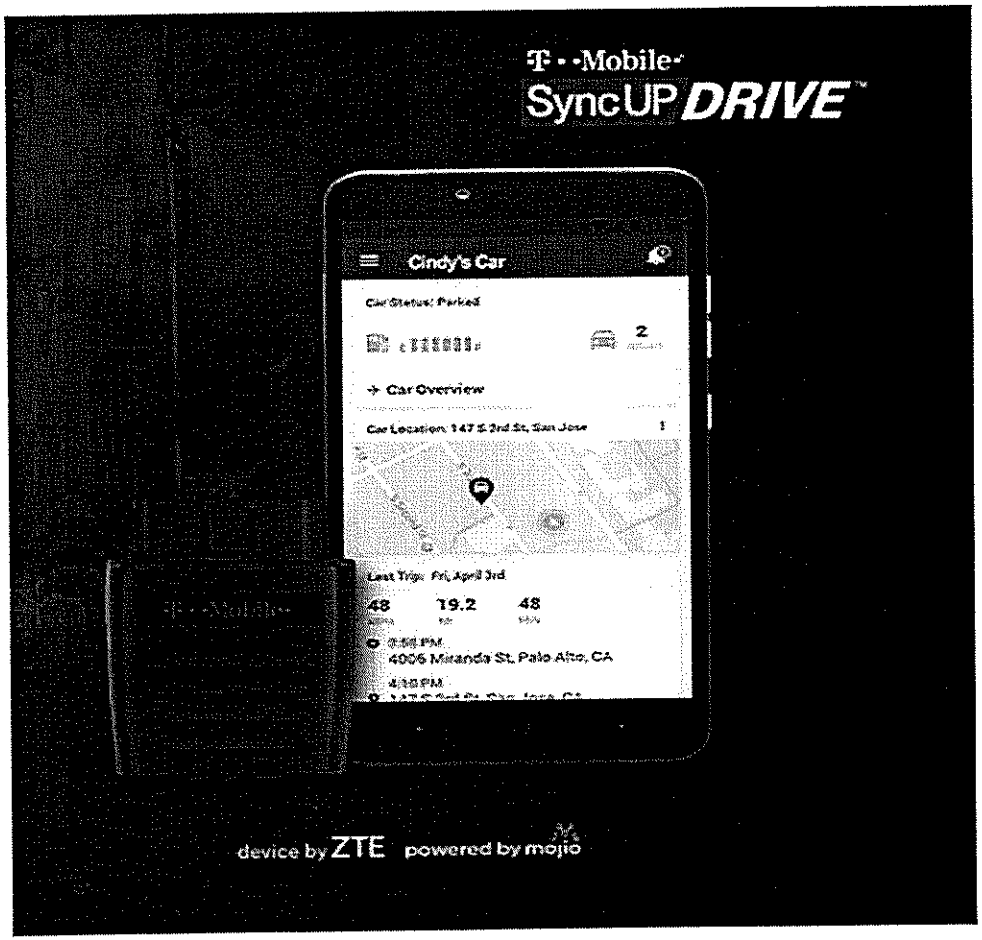
- **підключеня дзеркала Wi-Fi**
- **підключеня Wi-Fi гарнітури**
- **Wi-Fi відеореєстратори**



Huawei CarFi



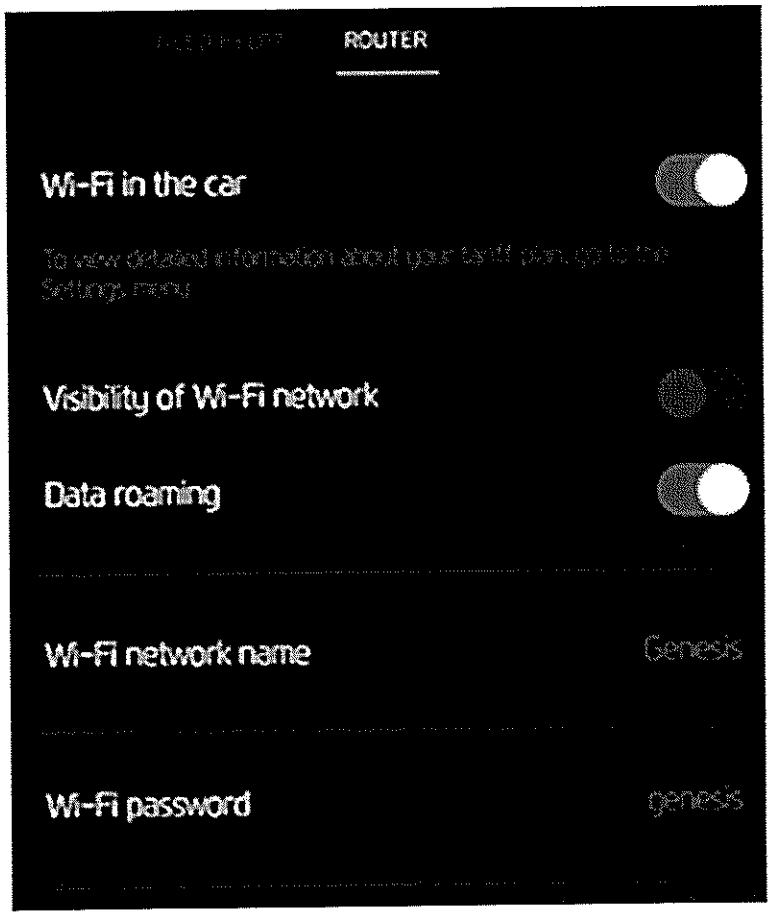
ZTE OBD



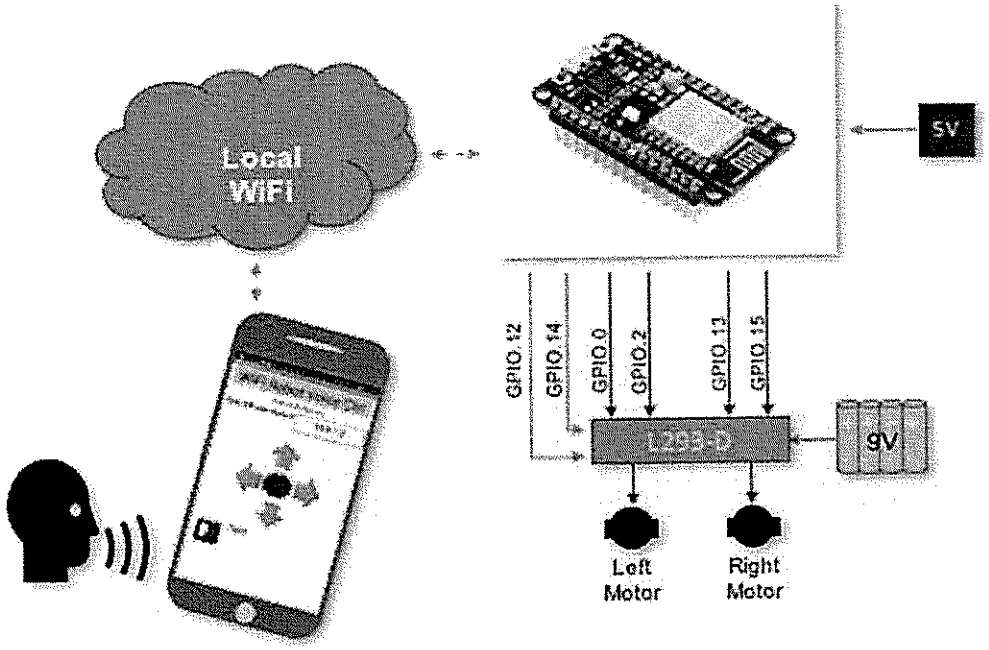
Мобільний додаток Genesis G90 для iOS та Android

Genesis G90 дозволяє користувачам:

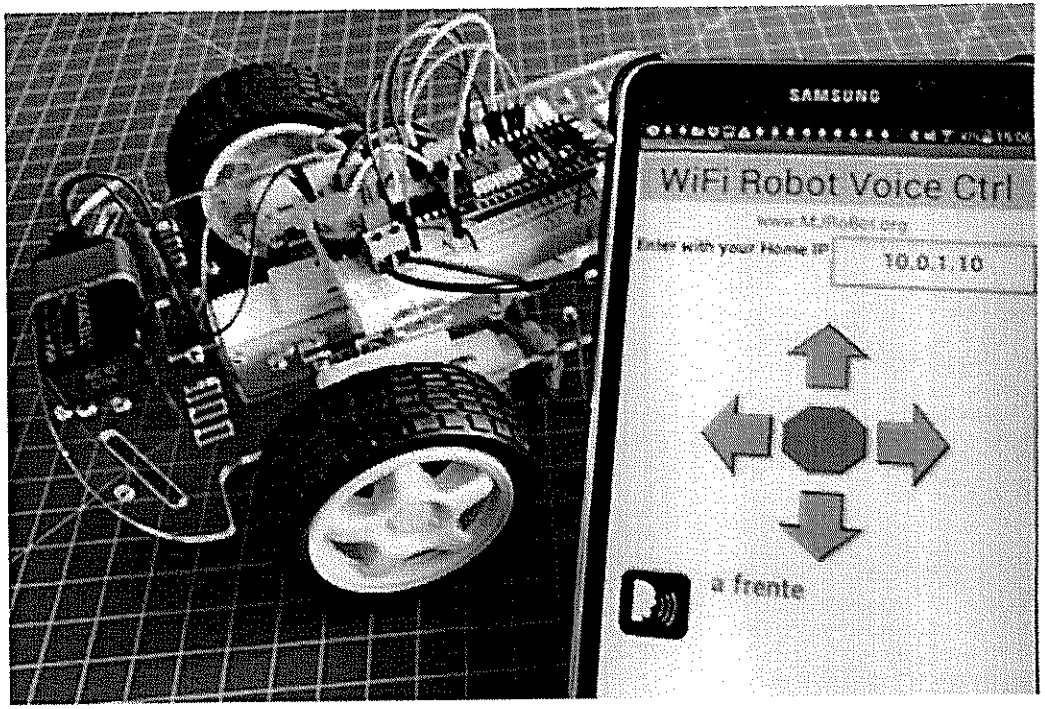
1.Відкривати/закривати центральний замок;
2. Запускати/зупиняти двигун;
3. Перевіряти стан дверей;
4. Відкривати багажник;
5.Стежити за швидкістю автомобіля;
6.Отримувати показники внутрішньої та зовнішньої температури.



ГОЛОСОВЕ КЕРУВАННЯ ЧЕРЕЗ WIFI І NODEMCU

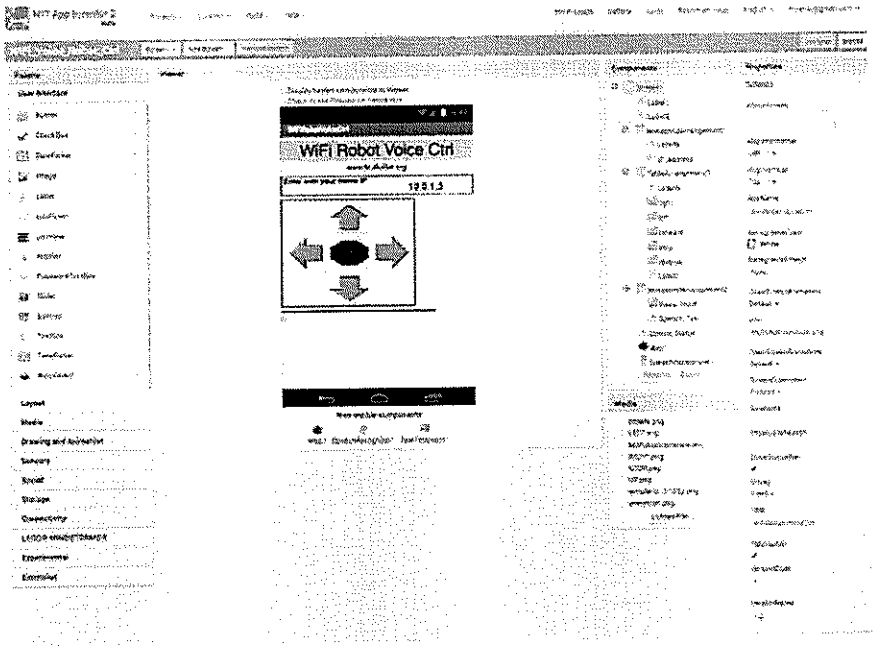


Блок-схема WiFi Voice Controlled Robot

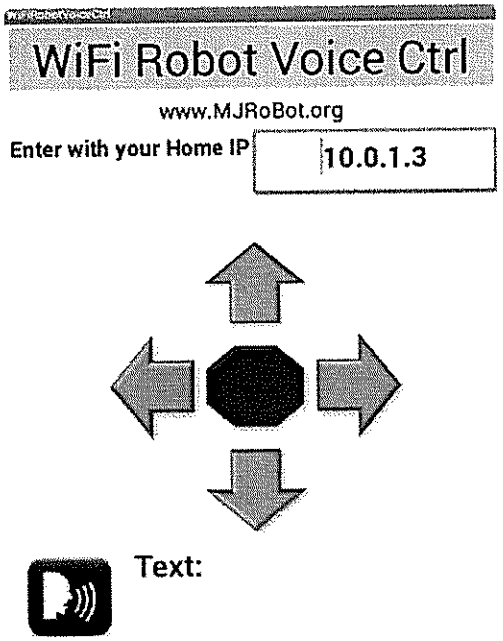


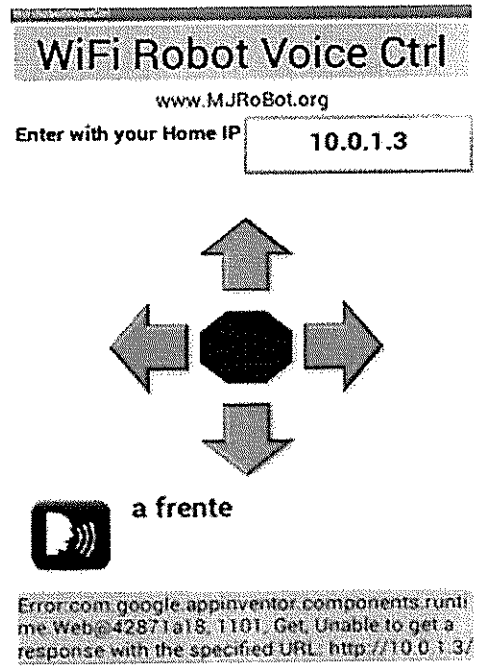
WiFi Voice Controlled Robot

Додаток для Android

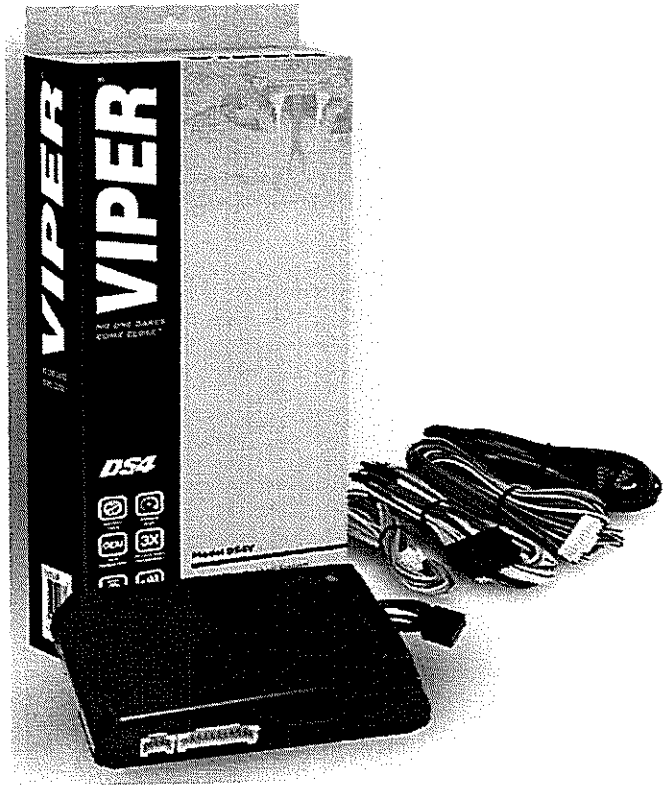


Програма Android





ЗАСОБИ БЕЗПЕКИ



Viper DS4 — це система дистанційного запуску, яка включає БЕЗКОШТОВНЕ керування автомобілем через **Bluetooth** і статус автомобіля за допомогою мобільного додатку Viper SmartStart.

Дистанційно запускайте, блокуйте або розблокуйте свій автомобіль за допомогою смартфона на відстані до 150 футів*. Не вимагає плану обслуговування Viper SmartStart.

ВИСНОВКИ

Протокол WiFi у системі центрального керування транспортним засобом є важливим компонентом сучасних систем центрального керування транспортним засобом. З'єднуючи центральну систему керування та інші пристрої через бездротову мережу, це забезпечує такі функції:

- підключення до мережі;
- передача мультимедіа,;
- діагностика автомобіля;
- дистанційне керування тощо.

З розвитком технологій бездротової мережі та популярністю центральних систем керування автомобілями, протокол Wi-Fi у центральній системі керування автомобілем матиме:

- вищу швидкість передачі даних;
- ширші сценарії застосування;
- сильнішу безпеку;
- глибоку інтеграцію з автономним керуванням у майбутньому.

Це забезпечить користувачам кращий досвід водіння та підвищить безпеку водіння.

ДЯКУЮ ЗА УВАГУ!

Протокол аналізу звіту подібності науковим керівником

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

Автор: Андрій Землянікін

Назва: Метод зовнішнього безпроводового керування автомобілем

Координатор: Лариса Дакова

Підрозділ: ННІТ

Коефіцієнт подібності 1:32.9

Коефіцієнт подібності 2:29.8

Тривога: 2

Після аналізу Звіту подібності констатую наступне:

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

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

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

…… ……

Дата *Підпис Наукового керівника*