Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Факультет математики і інформатики
Кафедра комп'ютерних наук та інформаційних технологій

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему «Розробка компактного картографу wifi мереж за допомогою мікроконтроллерів»

Захищено на засіданні ЕК № _____
протокол №_____від_.2024 р. Оцінка_
_____/ Голова ЕК

_____

Виконав:

студент 6 курсу, групи МФ62
Спеціальності: 122 Комп'ютерні науки

Кононенко Андрій Олександрович

Керівник: викладач Панченко А.С.
Рецензент _____

Харків-2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В.Н. Каразіна Факультет комп'ютерних наук

Кафедра моделювання систем і технологій

Рівень вищої освіти (освітньо-кваліфікаційний рівень) бакалавр Напрям підготовки 122 Комп'ютерні науки

Спеціальність Комп'ютерні науки

ЗАТВЕРДЖУЮ

Завідувач кафедри

підпис

_____ "" грудня

2024 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кононенко Андрій Олександрович

1. Тема роботи Розробка компактного картографу wifi мереж за допомогою мікроконтроллерів.

керівник роботи **викладач Панченко Артем Сергійович,**

затверджені наказом по університету від "" грудня 2024 року № 4101-5/895

2. Строк подання студентом роботи грудня 2024 року

Перелік питань, які потрібно розробити

1. Провести комплексний огляд літератури та документації з використання ESP8266 у режимі монітора для збору Wi-Fi Beacon Frames.
2. Аналізувати переваги та обмеження режиму монітора ESP8266 у порівнянні з іншими модулями для Wi-Fi сканування.
3. Розробити архітектуру програмного забезпечення для збору даних з Wi-Fi модулю ESP8266 та синхронізації з STM32.
4. Реалізувати алгоритм обробки Beacon Frames для аналізу та збереження ключових параметрів мережі.
5. Забезпечити інтеграцію GPS-модуля GP01 з STM32 для прив'язки координат до зібраних даних Wi-Fi.
6. Реалізувати систему запису даних на SD-карту через STM32 для зберігання великого обсягу інформації.
7. Спланувати оптимізацію енергоспоживання пристрою для роботи в польових умовах.
8. Спроектувати та протестувати схему обміну даними між STM32, ESP8266 та GPS через UART.
9. Розробити методику тестування пристрою, включаючи моделювання сценаріїв з високою щільністю мереж Wi-Fi.
10. Провести експерименти в реальних умовах для збору даних про Wi-Fi мережі у різних середовищах.
11. Проаналізувати отримані дані для оцінки якості роботи пристрою та точності фіксації мереж і координат.
12. Узагальнити результати роботи, підготувати рекомендації щодо використання розробленого пристрою та написати підсумковий звіт.

4. План роботи

№ з/п	Назви етапів роботи
1	Огляд літератури та аналіз існуючих рішень
2	Визначення технічних вимог та постановка задач
3	Розробка архітектури пристрою
4	Реалізація програмного забезпечення для ESP8266
5	Інтеграція GPS-модуля GP01 зі STM32
6	Реалізація зберігання даних на SD-карті через STM32
7	Тестування комунікації між модулями
8	Проведення експериментів у реальних умовах
9	Аналіз отриманих даних та вдосконалення пристрою
10	Написання звіту та підготовка документації

5. Дата видачі завдання 10 вересня 2024 року

Студент _____ Андрій Кононенко

Керівник роботи _____ Артем Панченко

Зміст

Вступ

1.1. Формулювання мети роботи та задач

Метою цієї дипломної роботи є розробка компактного картографа WiFi мереж для виявлення бездротових точок доступу шляхом використання мікроконтролера ESP (наприклад, ESP8266 або ESP32). Цей пристрій має забезпечити можливість збору інформації про доступні мережі WiFi без використання громіздкого обладнання, як, наприклад, автомобіль та потужна антена, і одночасно подолати обмеження сучасних смартфонів у цьому напрямку.

Задачі роботи:

1. Проаналізувати існуючі рішення для виявлення WiFi мереж (Wardriving) та їхні недоліки.
2. Визначити технічні вимоги до компактного пристрою для збору інформації про WiFi мережі.
3. Розробити прототип пристрою на основі мікроконтролера ESP, здатного працювати в режимі монітора для збору даних про бездротові мережі.Та використовуючи мікроконтроллер STM32 для обробки даних та комбінування даних з даними модуля GPS
4. Створити програмне забезпечення для зчитування та обробки даних з WiFi адаптера ESP та STM32, зокрема для фільтрації та візуалізації знайдених мереж на карті.
5. Провести тестування розробленого пристрою у реальних умовах для оцінки його ефективності та точності.
6. Оцінити можливість використання отриманих даних для підвищення безпеки бездротових мереж та їхньої оптимізації.

1.2. Стислий огляд відомих результатів в області дослідження

Wardriving — це практика, що полягає в активному пошуку бездротових мереж WiFi шляхом пересування на транспортному засобі або пішки. Використовуючи такі інструменти, як ноутбуки, смартфони, GPS-модулі та спеціалізоване програмне забезпечення, користувачі виявляють бездротові точки доступу та збирають інформацію про мережі. Суть wardriving полягає в тому, щоб вивчати навколишній простір на предмет доступних WiFi-мереж та отримувати відомості про їхні параметри, зокрема SSID (ім'я мережі), типи шифрування (WEP, WPA, WPA2) та потужність сигналу.

Wardriving може мати різні цілі, які значною мірою визначаються мотивами користувачів. Однією з основних причин використання цієї практики є аудит безпеки. Компанії або приватні особи можуть проводити такі перевірки для виявлення вразливостей у своїх мережах. Наприклад, можливо з’ясувати, чи не є мережа доступною з вулиці, чи правильно налаштовано шифрування, а також чи відсутні незахищені точки доступу, через які зловмисники можуть проникнути в систему.

Окрім перевірки безпеки, wardriving використовується для створення детальних карт бездротових мереж у певному районі. Ці дані можуть бути корисними для технічних цілей, таких як оптимізація роботи наявних мереж або планування встановлення нових точок доступу. Наприклад, телекомунікаційні компанії можуть аналізувати поширення мереж у різних частинах міста для подальшого розвитку своєї інфраструктури.

Wardriving також має наукову або дослідницьку цінність. Дослідники можуть використовувати зібрані дані для вивчення тенденцій у використанні WiFi-мереж або аналізу популярності тих чи інших технологій бездротового зв’язку та типів шифрування в різних місцевостях.

Однак не завжди wardriving використовується з легітимними намірами. Деякі люди можуть шукати відкриті або слабкозахищені мережі з метою отримання доступу до інтернету без дозволу власників. Це може бути проблемою для тих, хто нехтує налаштуваннями безпеки своїх бездротових мереж. У деяких випадках інформація, зібрана під час wardriving, може бути використана хакерами для зламу мереж, які мають низький рівень захисту, особливо якщо використовується застаріле або вразливе шифрування, як-от WEP.

Слід розуміти, що хоч сам процес збору інформації про бездротові мережі не завжди є незаконним, його використання з метою несанкціонованого доступу до чужих мереж без дозволу їх власників порушує закони у багатьох країнах. Використання wardriving для злому або несанкціонованого підключення до мереж може мати серйозні правові наслідки.

Wardriving, як метод виявлення бездротових мереж, активно розвивається з початку 2000-х років. Одним із ключових інструментів для цього завжди було спеціалізоване обладнання, яке дозволяє ефективно сканувати мережі WiFi в різних умовах.

Історія розвитку **wardriving** починається з 1990-х років, коли зростання популярності бездротових мереж WiFi почало привертати увагу не лише звичайних користувачів, а й тих, хто цікавився безпекою та технологіями. Хоча сама концепція моніторингу радіочастот і сканування ефіру для виявлення мереж сягає ще радіоаматорських практик початку 20-го століття, wardriving як окрема діяльність виник разом з поширенням WiFi.

Перші кроки (кінець 1990-х)

Із середини 1990-х років бездротові технології почали впроваджуватися в повсякденне життя, і до кінця десятиліття стандарт WiFi (802.11) став все більш поширеним. Перша версія стандарту 802.11b (прийнята в 1999 році) дозволила швидше розповсюджувати технологію WiFi завдяки вищим швидкостям передачі даних (до 11 Мбіт/с). З початком масового впровадження бездротових мереж, на передній план вийшло питання їхньої безпеки. В ті часи більшість мереж використовували прості або взагалі відсутні механізми захисту, наприклад, старий і вже ненадійний алгоритм шифрування WEP.

На перших етапах wardriving часто здійснювався ентузіастами, які цікавились технологіями та мали за мету не лише знаходити бездротові мережі, а й перевіряти їхню безпеку. Для цього вони використовували ноутбуки з бездротовими картами, антенами та спеціальним програмним забезпеченням. Одним із перших інструментів для wardriving стала програма **NetStumbler**, яка автоматично виявляла точки доступу WiFi, збирала інформацію про їхні параметри і могла показати статус безпеки мережі.

Поширення практики (початок 2000-х)

На початку 2000-х термін "wardriving" вперше з’явився завдяки ентузіастам технологій і безпеки. Назва має свої корені в понятті "war dialing", що стосується практики набору випадкових телефонних номерів за допомогою модему для пошуку активних телефонних ліній, яка була популярною в 1980-х роках. Саме ідея активного сканування ресурсів, доступних у радіусі дії, стала основою для wardriving.

У цей період wardriving привернуло увагу не лише технічних ентузіастів, а й компаній та професіоналів з інформаційної безпеки. Безпека WiFi-мереж була під загрозою через слабкість стандарту WEP, що спонукало багатьох

до пошуку і перевірки мереж на вразливості. До популярних програм цього часу можна віднести **Kismet**, яка використовувалась для пасивного виявлення бездротових мереж і була більш потужною, ніж інші інструменти, оскільки дозволяла перехоплювати пакети даних і не вимагала активного підключення до мережі.

Wardriving стало масовим явищем у середовищі хакерів і технічних спільнот, що призвело до створення цілих рухів та змагань із виявлення найбільшої кількості мереж або найбільш вразливих точок доступу.

Професіоналізація (2000-ті роки)

У середині 2000-х років WiFi став стандартною технологією у багатьох країнах світу, і зросла як кількість мереж, так і необхідність забезпечення їхньої безпеки. Одночасно з цим, wardriving також еволюціонувало. З'явилися спеціальні антени для збільшення радіусу сканування, а також вдосконалені GPS-трекери, що дозволяли не тільки виявляти мережі, але й точно фіксувати їхнє географічне розташування. Це сприяло популяризації проектів на кшталт **WiGLE** — бази даних з інформацією про виявлені бездротові мережі по всьому світу, що дозволяло створювати карти покриття та поширення WiFi.

У цей же період питання безпеки бездротових мереж набуло особливої ваги. Стандарт WEP був визнаний небезпечним, оскільки був вразливим до атак, і на його заміну прийшли нові протоколи, такі як **WPA** та **WPA2**, які забезпечували значно вищий рівень захисту.

Сучасний стан та нові форми (2010-ті — теперішній час)

З 2010-х років wardriving залишається популярною практикою як серед ентузіастів, так і серед професіоналів. Сучасні технології дозволили зробити цей процес доступнішим і зручнішим: смартфони з вбудованими

WiFi-адаптерами та GPS-трекерами тепер можуть виконувати всі функції, які раніше вимагали великих пристроїв і додаткового обладнання. З'явилося більше програм, які дозволяють виявляти та аналізувати бездротові мережі за допомогою смартфонів.

Сучасне wardriving також стало частиною великих проектів із моніторингу бездротових мереж. Водночас ця практика стала більш професійною: її використовують у сфері інформаційної безпеки для перевірки корпоративних мереж і аналізу рівня загроз. Багато компаній та організацій використовують подібні методи для аудиту безпеки своїх мереж, а також для моніторингу активності у певних регіонах.

Хоча з розвитком технологій безпеки та нових стандартів шифрування (таких як **WPA3**) ризики для звичайних користувачів зменшились, wardriving досі залишається важливим інструментом у перевірці вразливостей, а також у створенні карт доступності бездротових мереж, що має як легальні, так і нелегальні застосування.

Традиційне обладнання для wardriving за інформацією з ресурсу **wardriving.com** включає:

1. **Комп'ютер:** Як мінімум з процесором Pentium 100, який повинен мати слот PCMCIA для підключення мережевої карти та послідовний порт для GPS-приймача. Це обумовлюється вимогами до обробки великого обсягу даних про бездротові мережі та їх географічного положення.
2. **Бездротова карта Ethernet (802.11b):** Використовується для виявлення точок доступу WiFi. Залежно від потреб, також застосовують більш потужні антени для збільшення радіусу сканування.

3. **GPS-приймач:** Важливий для запису геолокаційних координат знайдених точок доступу, що дозволяє точно картографувати їх розташування.
4. **Засоби пересування:** Найчастіше для wardriving використовують автомобілі, що дозволяє сканувати великі території, однак, іноді це роблять пішки, на велосипеді або використовуючи громадський транспорт (автобус, метро).
5. **Програмне забезпечення:** Для управління скануванням та збору даних використовують різноманітні ОС (Linux, BSD, Windows, Mac) та спеціалізовані програми, які можуть працювати з бездротовими мережами в режимі монітора.

Чому використовуються додаткові плати?

1. Підтримка режиму монітора та інжектування пакетів

– Додаткові WiFi-плати, такі як ті, що побудовані на базі чипів **Atheros**, **Ralink**, або **Realtek**, часто підтримують режим монітора та інжектування пакетів, що дозволяє сканувати мережі, перехоплювати пакети даних та виконувати стратегії аналізу бездротових мереж.

– Стандартні вбудовані WiFi-адаптери в більшості ноутбуків або смартфонів зазвичай не мають цих можливостей. Вони призначені для звичайного підключення до мережі і не можуть працювати в низькорівневих режимах для збору або аналізу інформації.

2. Підтримка більших антен

– Додаткові плати WiFi дозволяють підключати зовнішні антени з більшим коефіцієнтом підсилення. Це важливо для **wardriving**, де потрібна здатність виявляти мережі на великій відстані.

Використання потужних антен дозволяє значно розширити радіус дії і кількість мереж, які можна виявити.

– Деякі плати WiFi мають дво- або тривікові антени, що дозволяє краще працювати в умовах зі складними радіочастотними перешкодами, підвищуючи точність сканування.

3. Можливість роботи на різних частотах

– Багато сучасних WiFi-плат підтримують одночасну роботу на частотах **2.4 ГГц і 5 ГГц**, що дозволяє проводити аналіз не тільки старіших стандартів WiFi (802.11b/g/n), але й нових (802.11ac/ax).

– Додаткова плата може також мати підтримку **802.11ax** (WiFi 6), що дозволяє збирати інформацію про мережі нового покоління.

4. Покращена чутливість та потужність передачі

– Додаткові WiFi-плати часто мають більшу потужність передачі (Tx power) і кращу чутливість приймача, що забезпечує більш стабільний сигнал та збільшує дальність роботи. Це важливо, коли необхідно виявляти слабкі сигнали WiFi мереж на великих відстанях або через перешкоди, такі як стіни чи природні бар’єри.

Ця конфігурація обладнання дозволяє збирати дані про бездротові мережі, визначати рівень їхнього сигналу, ідентифікувати SSID, канали зв'язку та інші параметри, а також поєднувати ці дані з географічними координатами. Проте таке рішення є досить громіздким і вимагає значних апаратних ресурсів та фізичного простору для транспортування і розміщення.

Незважаючи на високу ефективність, цей підхід має недоліки: громіздкість системи, необхідність використання зовнішнього обладнання (машина, антени) та обмежена мобільність. Це стимулює розвиток нових, компактних рішень, таких як використання мікроконтролерів ESP для створення мобільних пристроїв, здатних виконувати ті ж функції з мінімальними витратами ресурсів і зусиль.

1.3 Обґрунтування актуальності теми:

Тема розробки компактного картографа WiFi мереж є актуальною через зростаючу потребу в інструментах для аналізу бездротових мереж та підвищення їхньої безпеки. На сьогоднішній день більшість рішень у сфері виявлення WiFi мереж базуються на громіздких системах, які включають автомобіль та потужну антену, що робить їх незручними для використання в побутових умовах. У той же час, використання смартфонів для таких цілей обмежується апаратними і програмними бар'єрами, зокрема неможливістю роботи в режимі монітора.

Використання мікроконтролерів ESP надає нові можливості для створення компактних, ефективних і мобільних рішень для картографування WiFi мереж. Це дозволяє спростити процес збору даних про мережі, зменшити витрати на обладнання та підвищити зручність експлуатації таких пристроїв для дослідження та моніторингу бездротових мереж.

Основна частина

2 Протоколи що використовувалися у проекті

Для реалізації компактного маппера Wi-Fi мереж, що базується на STM32 та ESP8266, важливо детально розглянути принципи роботи ключових протоколів — Wi-Fi та GPS. Вони забезпечують зв'язок і визначення географічного положення пристрою.

2.1 GPS

Протокол GPS (Global Positioning System) забезпечує точне визначення географічного положення, що є критично важливим для прив'язки даних про Wi-Fi мережі до координат на карті. GPS базується на мережі супутників, що обертаються навколо Землі, та приймачі, який обробляє їхні сигнали.

GPS працює за принципом трилатерації: приймач отримує сигнали від щонайменше трьох супутників, аналізує час їхнього надходження та визначає положення пристрою в тривимірному просторі. Сигнали передаються на двох частотах: L1 (цивільна) і L2 (військова).

Основні компоненти GPS:

- **Супутники:** 24 основні супутники, які постійно передають дані про своє місцеположення та час.

- **Приймач:** Пристрій, що приймає сигнали, розраховує затримку і визначає координати.

- **Ефемериди:** Дані про траєкторію руху супутників, які приймач використовує для уточнення розрахунків.

GPS-сигнали містять три типи інформації:

- **Навігаційні дані:** Координати супутника, його орбіта, час.

- **Часовий сигнал:** Точний час передачі сигналу.

- **Корекції:** Інформація про помилки, що покращує точність позиціонування.

Переваги GPS:

- Висока точність визначення місця розташування.

- Можливість роботи в глобальному масштабі.

- Широка інтеграція в сучасні пристрої.

Недоліки:

- Вразливість до слабких сигналів у містах або закритих приміщеннях.

- Залежність від часу першого "холодного старту".

- Енергоспоживання, що може бути проблемою для малих пристроїв.

Розуміння принципів роботи протоколів Wi-Fi та GPS є основою для успішної реалізації маппера мереж, адже вони визначають функціональність і точність зібраних даних.

2.2 Wi-Fi

Протокол Wi-Fi є одним із найпоширеніших бездротових протоколів, що дозволяє пристроям підключатися до Інтернету через бездротовий зв’язок. Він функціонує на частотах 2,4 ГГц і 5 ГГц та використовується у багатьох пристроях, зокрема дронах. На низькому рівні Wi-Fi базується на стандарті

IEEE 802.11, що визначає основні принципи передачі даних у бездротових мережах.

Wi-Fi фрейм (або кадр IEEE 802.11) — це структурована одиниця даних, яка використовується для передачі інформації через бездротову мережу. Його побітова структура включає:

– **Преамбулу (Preamble)** — 56 біт. Забезпечує синхронізацію передачі та встановлення зв’язку між передавачем і приймачем.

– **Заголовок керування (Frame Control)** — 16 біт. Містить інформацію про тип фрейму, адреси джерела і призначення, а також контрольні біти.

– **Довжину (Length)** — 16 біт. Визначає загальну довжину фрейму, включаючи заголовок та корисні дані.

– **Адресу одержувача (Receiver Address)** — 48 біт. Вказує MAC-адресу приймача, якому призначений кадр.

– **Адресу передавача (Transmitter Address)** — 48 біт. Вказує MAC-адресу відправника фрейму.

– **Додаткові адреси (Address 1, Address 2, Address 3)** — кожна по 48 біт. Застосовуються для передачі додаткових адресних даних, залежно від типу фрейму.

– **Послідовності (Sequence Control)** — 16 біт. Служить для нумерації та управління порядком передавання кадрів.

– **Заголовок даних (Data)** — змінна довжина (0–2312 біт). Містить корисну інформацію (наприклад, IP-пакети).

– **Контрольну послідовність (FCS, Frame Check Sequence)** — 32 біти. Використовується для перевірки цілісності даних у кадрі.

Структура кадру Wi-Fi змінюється залежно від типу. Найпоширенішими є менеджерські, керуючі та дані фрейми.

Менеджерські кадри (Management Frames) використовуються для керування мережею, обміну інформацією між точками доступу і клієнтськими пристроями та підтримки з'єднання. Наприклад, Beacon Frames розсилають параметри мережі, Probe Request — шукають доступні мережі, Probe Response — відповідають на запити клієнтів. Authentication Frames забезпечують аутентифікацію, а Association Request і Response використовуються для асоціації клієнтів із мережею.

Керуючі кадри (Control Frames) забезпечують регулювання передачі даних. Наприклад, кадри ACK (Acknowledgment) підтверджують отримання даних, RTS (Request to Send) та CTS (Clear to Send) мінімізують колізії в мережі.

Кадри даних (Data Frames) передають корисну інформацію, таку як текст, файли чи мультимедіа.

Deauthentication Frames є менеджерськими кадрами, призначеними для деаутентифікації клієнта з мережі. Їх відправляють точки доступу (AP), щоб повідомити клієнта про відключення. Вони містять Reason Code, який визначає причину відключення. Основні причини можуть включати:
– невказану причину;
– втрату актуальності попередньої аутентифікації;
– відключення клієнта через його вихід із мережі;
– неактивність клієнта;
– перевантаження точки доступу;
– отримання некоректного кадру від неавторизованого або неасоційованого пристрою.

Деаутентифікація відіграє важливу роль у підтримці безпеки та стабільності мереж Wi-Fi. Правильна інтерпретація цих кадрів допомагає

забезпечити ефективну роботу мережі та захист від несанкціонованого доступу.

Beacon Frame — це тип менеджерського фрейму (Management Frame) у протоколі Wi-Fi, який використовується для передачі основної інформації про бездротову мережу. Ці фрейми відіграють ключову роль у функціонуванні Wi-Fi мереж, забезпечуючи інформування клієнтських пристроїв про наявність мережі та її параметри. Beacon Frames генеруються точками доступу (Access Point, AP) і розсилаються періодично, зазвичай кожні 100 мс (цей інтервал може бути змінений налаштуваннями).

2.3 Що таке режим монітора?

Режим монітора дозволяє ESP8266 приймати пакети на фізичному рівні (PHY), перш ніж вони будуть оброблені стеком протоколів Wi-Fi. Це означає, що пристрій може отримувати:

Beacon Frames (маячкові кадри) від точок доступу, які розсилають інформацію про мережу.

Probe Request/Response кадри, які використовуються для пошуку мереж.

Інші кадри, включаючи Broadcast та Multicast пакети.

У цьому проєкті **режим монітора** використовується для прийому **Beacon Frames**, що містять ключову інформацію про мережу, таку як:

SSID (ім’я мережі).

MAC-адресу точки доступу.

Рівень сигналу (RSSI).

Частотний канал і тип шифрування.

2.4 Beacon frames

Основне завдання Beacon Frames — це:

1. **Оголошення наявності мережі:** Beacon Frame є "маяком", який повідомляє клієнтські пристрої про існування Wi-Fi мережі.
2. **Передача параметрів мережі:** Beacon містить інформацію про SSID (ім'я мережі), тип шифрування, підтримувані швидкості та інші параметри, необхідні для підключення до мережі.
3. **Синхронізація:** Ці кадри допомагають синхронізувати годинники клієнтських пристроїв з точкою доступу, що важливо для коректної роботи бездротових протоколів.
4. **Індикація навантаження мережі:** Beacon може містити інформацію про завантаженість точки доступу, що дозволяє клієнтам вибирати оптимальну точку для підключення.

Структура Beacon Frame

Beacon Frame складається з кількох полів, кожне з яких виконує певну функцію:

1. **Заголовок кадру (Frame Control):** Визначає тип фрейму (Management Frame) і вказує, що це Beacon.
2. **Адресні поля:** Beacon містить MAC-адресу точки доступу (Transmitter Address) та адреси одержувачів.
3. **Поле часу (Timestamp):** Використовується для синхронізації годинників клієнтських пристроїв з годинником точки доступу.

4. **Інтервал маяків (Beacon Interval):** Визначає періодичність, з якою точка доступу надсилає Beacon Frames. Зазвичай це значення становить 100 мс.
5. **Кампанії (Capability Information):** Це поле містить інформацію про характеристики мережі, такі як підтримка шифрування, дозволені режими роботи, використання енергозберігаючих функцій тощо.
6. **SSID (Service Set Identifier):** Ідентифікатор мережі, тобто її ім'я, яке відображається на пристроях під час пошуку мереж. Якщо мережа є прихованою (Hidden SSID), це поле буде порожнім.
7. **Підтримувані швидкості (Supported Rates):** Список швидкостей передачі даних, які підтримує точка доступу.
8. **Додаткові параметри:** Це можуть бути поля, що описують розширені функції мережі, такі як підтримка нових стандартів (наприклад, Wi-Fi 6), інформація про шифрування (WPA, WPA2, WPA3) тощо.

Механізм роботи Beacon Frames

1. **Періодична передача:** Beacon Frames передаються точкою доступу через однакові проміжки часу. Цей інтервал може бути налаштований, але найчастіше він дорівнює 100 мс.
2. **Охоплення радіуса дії:** Вони транслюються в межах покриття точки доступу і приймаються всіма пристроями, які знаходяться в зоні дії.
3. **Фільтрація клієнтом:** Клієнтські пристрої аналізують отримані Beacon Frames і приймають рішення про підключення на основі параметрів мережі (наприклад, SSID, рівня сигналу, типу шифрування).
4. **Сканування мереж:** Коли пристрій сканує доступні мережі, він виявляє їх завдяки Beacon Frames.

Важливість Beacon Frames

Beacon Frames є основою функціонування Wi-Fi мережі. Вони забезпечують:

- **Доступність мережі:** Завдяки цим кадрам пристрої дізнаються про наявність і параметри мережі.
- **Зручність підключення:** Користувачі можуть бачити список доступних мереж і вибирати потрібну.
- **Ефективність роботи:** Точки доступу можуть інформувати клієнтські пристрої про свій стан і поточні можливості, що дозволяє оптимізувати підключення та використання ресурсів мережі.

Обмеження та загрози Beacon Frames

Beacon Frames, хоча і важливі, можуть бути вразливими до атак:

- **Витік інформації:** Вони містять відкриту інформацію про мережу, яку зловмисники можуть використовувати для атак.
- **Атаки з підміною:** Зловмисники можуть створювати підроблені Beacon Frames (атака "Evil Twin"), щоб змусити клієнтів підключатися до фальшивих точок доступу.
- **Перевантаження мережі:** Надлишок Beacon Frames у щільних мережах може створювати додаткове навантаження, знижуючи пропускну здатність.

2.5 Опис основних компонентів та функцій приладу

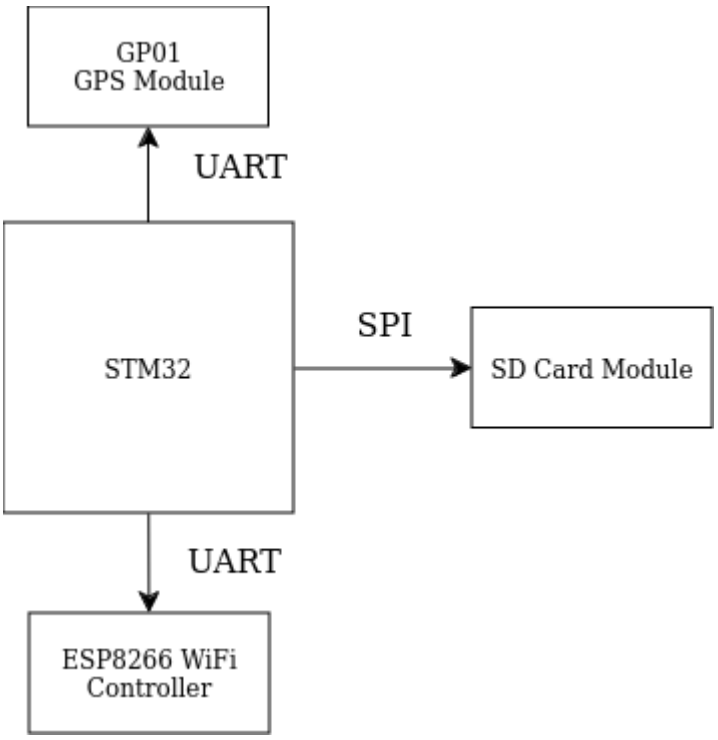

Рисунок 1 Абстрактна схема приладу

Компоненти:

1. **STM32 мікроконтролер:**

   – **Функція:** Виконуватиме роль центрального процесора, керуючи роботою всіх інших модулів.

   – **Задачі:** Прийом даних від ESP8266 та GPS модуля, обробка інформації, запис даних на SD-карту. Завдяки високій продуктивності та багатозадачності STM32, він зможе ефективно координувати всі підключені компоненти.

2. **ESP8266 мікроконтролер (WiFi модуль):**

   – **Функція:** Використовуватиметься для сканування WiFi-ефіру, зокрема для збору даних про **beacon frames** (кадри маяка) та **data frames** з SSID від підключених пристроїв.

– **Задачі:** Працюватиме в режимі монітора для виявлення бездротових мереж і перехоплення кадрів, які розсилаються маршрутизаторами та клієнтами WiFi. Зібрані дані будуть передаватися на STM32 для подальшої обробки.

– **Переваги:** ESP8266 підтримує режим монітора, що дозволяє ефективно збирати інформацію про всі доступні мережі, не передаючи власних запитів на з'єднання, що знижує ймовірність детекції самого пристрою.

3. **GP01 GPS модуль:**

– **Функція:** Здійснюватиме запис координат місця розташування приладу під час сканування WiFi мереж.

– **Задачі:** Передаватиме геолокаційні дані на STM32, які будуть прив'язані до кожної знайденої WiFi мережі, дозволяючи створити карту точок доступу з їхнім місцем розташування.

4. **Модуль SD-карти:**

– **Функція:** Використовуватиметься для зберігання даних, отриманих з WiFi модуля та GPS. Ці дані включатимуть SSID мереж, MAC-адреси точок доступу, рівні сигналу, а також координати, отримані з GPS модуля.

Задачі: Запис структурованих даних на SD карту

Схема роботи пристрою:

1. **Сканування WiFi мереж:**

– **ESP8266** постійно прослуховуватиме WiFi ефір у режимі монітора. Він фіксуватиме **beacon frames** від маршрутизаторів — це системні кадри, які містять SSID, MAC-адресу маршрутизатора, канал, тип шифрування та інші дані.

– Крім того, він збиратиме **data frames**, які передаються між пристроями в мережі. Це може включати дані про підключені пристрої та їхні SSID.

2. **Збір геолокаційних даних:**

– Паралельно **GP01 GPS модуль** надаватиме координати місця розташування кожної знайденої WiFi мережі.

– Ці координати будуть передаватися на STM32 та прив'язуватися до відповідних WiFi даних, щоб точно зафіксувати місце розташування точок доступу.

3. **Обробка та зберігання даних:**

– **STM32** оброблятиме дані, отримані від ESP8266 та GPS модуля, і записуватиме їх на **SD-карту**. Дані будуть організовані у вигляді записів, що містять SSID, MAC-адресу, рівень сигналу (RSSI), частоту (канал), тип шифрування та координати GPS.

4. **Аналіз даних:**

– Після збору даних, вони можуть бути зчитані з SD-карти та імпортовані в програмне забезпечення для візуалізації, таке як **Google Maps** або спеціалізовані інструменти для аналізу WiFi мереж. Це дозволить створити карту точок доступу з інформацією про розташування та властивості кожної мережі.

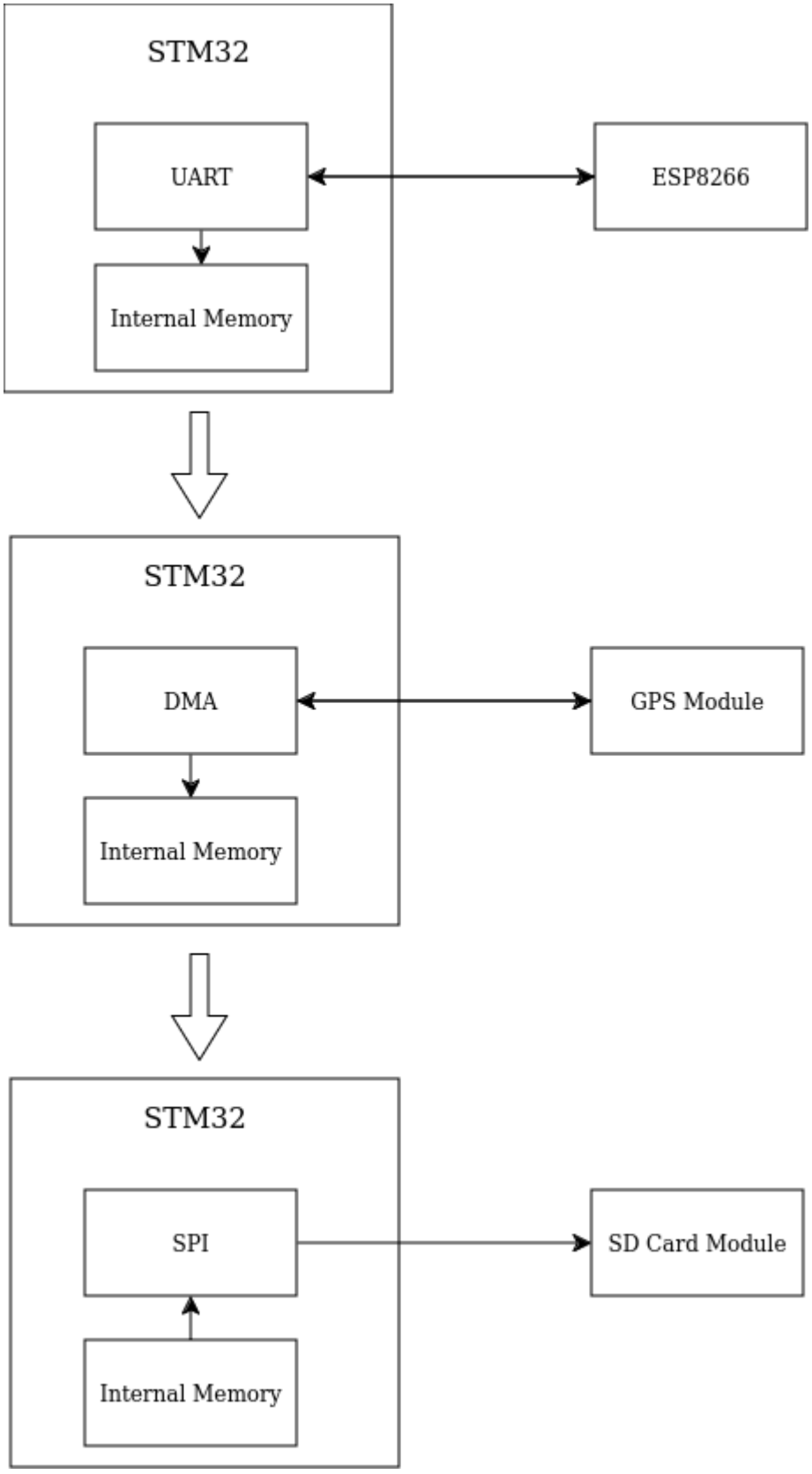

Рисунок 2 схема роботи приладу

Основні переваги:

– **Компактність:** Використання ESP8266 для сканування WiFi та невеликого STM32 як контролера дозволить створити компактний і енергоефективний пристрій, який можна легко переносити або навіть використовувати в автомобілі чи на велосипеді.

– **Автономність:** Пристрій зможе працювати незалежно від інших систем, записуючи всі дані на SD-карту для подальшого аналізу.

– **Широка функціональність:** Можливість одночасно збирати дані про WiFi мережі та їхнє географічне розташування робить пристрій корисним для аналізу бездротових мереж на великих територіях.

В ході написання цієї дипломної роботи було виконано роботу, спрямовану на створення пристрою для картографування Wi-Fi мереж. Основною метою було розробити автономний пристрій, здатний сканувати бездротові мережі, отримувати географічні координати їхнього розташування та записувати дані для подальшого аналізу.

2.6 GP01

GPS-приймач GP01 — це надійне, просте у використанні рішення для навігації та позиціонування, яке підходить для широкого спектру завдань у сучасних проєктах. Його функціональні можливості забезпечують високу точність і стабільність, роблячи його ідеальним вибором для цього проекту

1. **Архітектура та чіпсет:**

   GP01 використовує високопродуктивний GNSS-чіпсет (зазвичай на

основі U-Blox або MTK). Цей чіпсет забезпечує швидкий "гарячий старт" і високу точність навіть у складних умовах.

2. **Сумісність зі стандартами:**

   Підтримує глобальні навігаційні системи, такі як:

- **GPS (Global Positioning System):** основна американська система навігації.
- **ГЛОНАСС:** російська система, що забезпечує додаткову надійність у зонах із поганим прийомом сигналу GPS.
- **SBAS (WAAS, EGNOS):** системи для підвищення точності сигналу.

3. **Чутливість:**

   GP01 має високу чутливість, що дозволяє отримувати сигнал навіть у зоні слабкого покриття (між будівлями, у густих лісах або в транспортних засобах).

4. **Інтерфейси зв'язку:**

   Підтримує **UART** або **I2C** інтерфейси для обміну даними з мікроконтролерами або іншими пристроями. UART часто використовується для передачі стандартних NMEA (National Marine Electronics Association) повідомлень, які містять дані про місцезнаходження, швидкість і час.

5. **Енергоспоживання:**

   Модуль споживає дуже мало енергії (приблизно 20-30 мА при роботі), що робить його ідеальним для застосування в енергоефективних пристроях, таких як портативні трекери.

6. **Компактний дизайн:**

   Розміри GP01 дозволяють інтегрувати його в пристрої з обмеженим простором. Часто вбудований керамічний чип-антена забезпечує якісний прийом сигналу без потреби у зовнішніх антенах.

7. **Точність:**

   GP01 забезпечує точність місцезнаходження до 2,5 метрів у

звичайних умовах і навіть до 1 метра при використанні системи SBAS.

Принцип роботи GPS-приймача GP01

1. **Прийом супутникового сигналу:**

   GP01 отримує сигнали від супутників GPS (або інших систем GNSS). Для визначення координат модуль використовує принцип триангуляції, обробляючи сигнали від щонайменше чотирьох супутників.

2. **Обробка даних:**

   Прийняті сигнали аналізуються вбудованим процесором, який розраховує:

   Координати (широта, довгота): місцезнаходження у глобальній системі координат WGS84.

   Швидкість: швидкість руху пристрою, якщо він переміщується.

   Висота: над рівнем моря.

   Час: високоточний час, синхронізований із супутниками.

3. **Передача інформації:**

   Оброблені дані передаються через UART у стандартному форматі NMEA. Найбільш поширені повідомлення NMEA:

   GGA: географічне положення та якість сигналу.

   RMC: рекомендовані мінімальні дані, що включають дату, час, швидкість та курс.

   GSV: інформація про видимі супутники.

Переваги використання GP01

1. **Простота інтеграції:**

   Завдяки стандартним інтерфейсам і компактному дизайну, GP01 легко інтегрується у будь-який проєкт.
2. **Висока точність:**

   Використання додаткових систем SBAS дозволяє отримувати координати з мінімальними похибками.
3. **Швидкий старт:**

   GP01 має три режими старту:

   Гарячий старт (Hot Start): швидке відновлення зв’язку після короткочасної втрати сигналу (1-2 секунди).

   Теплий старт (Warm Start): використання попередньо збережених даних для пошуку супутників (20-30 секунд).

   Холодний старт (Cold Start): повний пошук супутників, якщо попередні дані недоступні (30-60 секунд).
4. **Ефективність роботи в складних умовах:**

   GP01 може працювати у зонах із високими перешкодами завдяки високій чутливості приймача.

Практичне застосування GP01

1. **GPS-трекери:**

   Використовується у пристроях для відстеження місцезнаходження транспортних засобів, домашніх тварин або персоналу.
2. **Дрони та роботи:**

   GP01 забезпечує точне позиціонування та маршрутизацію у реальному часі.

3. **Навігаційні пристрої:**

   Встановлюється в портативні або автомобільні навігатори для визначення маршруту.
4. **Інтернет речей (IoT):**

   Служить у "розумних" пристроях, які потребують функції геолокації, наприклад, у смарт-годинниках або датчиках.

Обмеження GP01

1. **Залежність від сигналу:**

   У приміщеннях або під землею (наприклад, у тунелях) сигнал від супутників може бути значно ослаблений або відсутній.
2. **Затримка холодного старту:**

   У разі холодного старту модуль потребує більше часу для отримання координат.
3. **Обмежений функціонал:**

   GP01 не має розширених функцій, таких як обробка RTK (Real-Time Kinematic) для сантиметрової точності.

Типовий приклад підключення GP01 до мікроконтролера (STM32)

Підключення:

TX GP01 → RX STM32

RX GP01 → TX STM32

VCC GP01 → 3.3V STM32

GND GP01 → GND STM32

Програмне забезпечення:

Використовується UART-інтерфейс для прийому повідомлень

NMEA. Наприклад, за допомогою бібліотеки HAL у STM32 можна розпарсити дані про координати та використовувати їх у додатку.

2.7 ESP8266

ESP8266 — це потужний і економічний Wi-Fi модуль, розроблений компанією Espressif Systems. Він дозволяє вбудовувати можливості бездротового підключення до інтернету в різні пристрої, включаючи мікроконтролери, розумні пристрої, датчики, робототехніку, дрони та інші системи.

Основні характеристики ESP8266

1. **Процесор і пам'ять:**

   Процесор: 32-бітний RISC-процесор на основі ядра Tensilica L106 з тактовою частотою до 160 МГц.

   Пам'ять: 512 KB флеш-пам'яті для зберігання програмного забезпечення і даних.

   Оперативна пам'ять (RAM): 160 KB, з яких частина використовується для роботи мережевих стеків, а інша — для виконання програм.

2. **Модуль Wi-Fi:**

   Підтримка стандартів IEEE 802.11 b/g/n.

   Працює в діапазонах частот 2,4 ГГц.

   Підтримка WEP, WPA/WPA2 шифрування для забезпечення безпеки.

Можливість роботи як у режимі станції (STA), так і в режимі точки доступу (AP).

Максимальна швидкість передачі даних до 72,2 Мбіт/с в залежності від каналу та стандарту.

3. **Інтерфейси вводу/виводу:**

   GPIO (General Purpose Input/Output) — до 17 цифрових пінів, з яких деякі можна використовувати як PWM, I2C, SPI, UART, ADC (аналогові входи).

   Підтримка апаратного UART для серійної передачі даних.

   SPI, I2C, та інших інтерфейсів для взаємодії з іншими мікросхемами та сенсорами.

4. **Енергоспоживання:**

   ESP8266 має кілька режимів енергозбереження, що дозволяє значно знизити споживання енергії, зокрема в режимі сну (Deep Sleep Mode).

   В залежності від використаних режимів та навантаження, споживана потужність може варіюватися від 70 мА в режимі активної передачі до менше 1 мА в режимі сну.

5. **Мережеві можливості:**

   Підтримка статичних і динамічних IP-адрес.

   DHCP сервер/клієнт для автоматичного отримання або видачі адрес в мережі.

TCP/IP стек для роботи з різними протоколами, включаючи HTTP, FTP, MQTT тощо.

6. **Програмування:**

   ESP8266 підтримує програмування через різні середовища, включаючи **Arduino IDE**, **PlatformIO**, **NodeMCU**, **Lua**.

   Програмування може здійснюватися через UART або програматор (FTDI).

   ESP8266 можна легко налаштувати та управляти через прості бібліотеки, які дозволяють швидко вбудувати бездротове підключення в проекти.

Режими роботи ESP8266

ESP8266 може працювати в кількох режимах в залежності від вимог проекту:

1. **Режим станції (STA):** В цьому режимі ESP8266 підключається до існуючої Wi-Fi мережі, діючи як клієнт (наприклад, смартфон чи комп'ютер). Це дозволяє підключати пристрій до інтернету для передачі даних через мережу.
2. **Режим точки доступу (AP):** ESP8266 може працювати як точка доступу (Access Point, AP), до якої можуть підключатися інші пристрої. В цьому режимі пристрій створює свою власну мережу Wi-Fi, що дозволяє іншим підключатися до нього.
3. **Режим об'єднаної точки доступу/станції (AP+STA):** У цьому режимі ESP8266 може одночасно діяти як точка доступу та клієнт, що підключається до іншої Wi-Fi мережі. Це дає можливість

одночасно підключати інші пристрої до ESP8266, а також отримувати доступ до Інтернету через іншу точку доступу.

4. **Режим монітора (Promiscuous Mode):** Режим монітора дозволяє ESP8266 прослуховувати всі бездротові пакети, що передаються в його радіусі. Це корисно для аналізу мережі, зокрема для прийому Beacon Frames, Probe Requests/Responses та інших пакетів. В рамках цього проекту ESP8266 в режимі монітора використовуватиметься для збору Beacon Frames від точок доступу.

Технічна реалізація режиму монітора на ESP8266

ESP8266 SDK, наданий компанією Espressif, підтримує Promiscuous Mode через функції в API. Використовуючи **NodeMCU (або Arduino Core)**, можна увімкнути цей режим і налаштувати прийом кадрів.

1. **Увімкнення режиму монітора** Для активації режиму монітора використовується функція `wifi_promiscuous_enable(1)`, яка налаштовує ESP8266 для прийому всіх кадрів.
2. **Обробка даних** При отриманні пакета SDK викликає функцію зворотного виклику (callback), яка обробляє інформацію з кадру. У Beacon Frame можна вилучити такі дані:

    SSID: Частина корисного навантаження фрейму.

    MAC-адреса точки доступу: Знаходиться в заголовку кадру.

    RSSI: Інформація про рівень сигналу, яку надає фізичний шар.

Використання ESP8266 у проекті Wi-Fi мапінгу для прийому Beacon Frames

У цьому проекті **ESP8266** буде працювати в **режимі монітора** для прийому Beacon Frames від точок доступу, що дозволить отримати інформацію про мережі, що знаходяться в радіусі дії пристрою. Це дозволяє ефективно картографувати Wi-Fi мережі, що буде корисно для завдань, пов'язаних із моніторингом і оптимізацією бездротових мереж.

ESP8266 прийматиме Beacon Frames, які містять:

SSID (ім’я мережі),

MAC-адресу точки доступу,

Канал, на якому працює точка доступу,

Рівень сигналу (RSSI),

Параметри шифрування (WEP, WPA, WPA2).

Прийняті кадри обробляються програмно для виділення необхідної інформації, після чого вона передається на основний мікроконтролер (у нашому випадку на STM32), використовуючи UART, SPI або I2C.

2.8 STM32F3

STM32F3 — це серія мікроконтролерів на базі архітектури ARM Cortex-M4, розроблена компанією STMicroelectronics. Мікроконтролери цієї серії призначені для застосувань, де необхідна висока продуктивність, точність обробки сигналів і низьке споживання енергії. Серія F3 ідеально підходить для застосувань в різних сферах, таких як обробка аналогових сигналів, вимірювання, управління, робототехніка, бездротові технології та багато інших.

Мікроконтролери STM32F3 використовують ядро ARM Cortex-M4 з підтримкою операцій з плаваючою точкою (FPU) та великими

можливостями для роботи з аналоговими сигналами, що робить їх ідеальними для обробки аналогових сигналів, фільтрації, чисельних розрахунків та багатьох інших застосувань.

Основні характеристики STM32F3

1. **Ядро та архітектура:**

   Ядро: ARM Cortex-M4 (32-бітна архітектура).

   Тактова частота: до 72 МГц.

   Підтримка FPU: Апаратор для роботи з плаваючою точкою для покращеної продуктивності в обчисленнях з дійсними числами.

   Інструкції: Система підтримує інструкції з прискоренням обробки сигналів, що дозволяє використовувати її для цифрової обробки сигналів (DSP).

2. **Пам'ять:**

   Flash пам'ять: Від 16 KB до 512 KB залежно від моделі мікроконтролера.

   Оперативна пам'ять (SRAM): Від 4 KB до 128 KB.

   Підтримка **External Memory Interface (FMC)** для підключення зовнішніх пам'ятей.

3. **Цифрові та аналогові периферії:**

   ADC (аналогово-цифровий перетворювач): Підтримка до 16 каналів, роздільна здатність 12 біт. Це дозволяє з високою точністю перетворювати аналогові сигнали у цифрові.

DAC (цифрово-аналоговий перетворювач): Підтримка до 2 каналів 12 біт.

Таймери: Вбудовані багатофункціональні таймери для генерації PWM сигналів, вимірювання часу, створення затримок та керування.

USART, SPI, I2C: Інтерфейси для підключення периферійних пристроїв, таких як сенсори, дисплеї, датчики та інші.

Op-amp (Операційні підсилювачі): Вбудовані операційні підсилювачі для обробки аналогових сигналів.

4. **Перешкодозахищеність та високий рівень точності:**

STM32F3 підтримує вбудовані засоби захисту від електричних шумів та перешкод, що важливо для застосувань, де точність сигналів і надійність роботи є критичними.

Підтримка високоточного **таймера реального часу (RTC)** для управління часом і датою.

5. **Інтерфейси для з'єднання:**

USB 2.0: Підтримка USB, включаючи можливість роботи як хост і пристрій, що дозволяє легко підключати зовнішні пристрої.

CAN 2.0B: Підтримка контролера мережі CAN для промислових та автомобільних застосувань.

SDIO: Інтерфейс для підключення карт пам'яті SD, що може бути корисно для зберігання даних.

6. **Енергоспоживання:**

STM32F3 має кілька режимів енергозбереження для зниження споживаної потужності, що дозволяє використовувати мікроконтролери в портативних і енергозалежних системах.

Енергоефективні режими дозволяють досягати низького споживання енергії без значних втрат у продуктивності, що особливо важливо для акумуляторних пристроїв.

Особливості використання STM32F3

1. **Обробка аналогових сигналів:** Однією з особливостей STM32F3 є розширені можливості для роботи з аналоговими сигналами. Вбудовані ADC і DAC дозволяють безпосередньо працювати з аналоговими входами та виходами, а також використовувати операційні підсилювачі для фільтрації і посилення сигналів. Це робить STM32F3 ідеальним вибором для вимірювальних пристроїв, а також для систем, де необхідна точність і швидкість обробки аналогових сигналів.
2. **Обробка цифрових сигналів:** Завдяки вбудованим інструментам для цифрової обробки сигналів (DSP), включаючи математичні операції з плаваючою точкою, STM32F3 може використовуватися для виконання складних обчислень в реальному часі. Ці можливості дозволяють застосовувати мікроконтролери для обробки звукових, відео та інших типів сигналів.
3. **Контроль за збереженням даних:** Вбудовані інтерфейси, такі як SDIO для карт пам'яті і USB, дозволяють розширити можливості STM32F3 для зберігання та передачі великих обсягів даних. Це є важливим аспектом у системах моніторингу та збору даних, де потрібна велика пам'ять для зберігання інформації.

4. **Інтерфейси для зв'язку:** Завдяки підтримці стандартів UART, SPI, I2C, STM32F3 може підключатися до різних периферійних пристроїв, таких як датчики, дисплеї, модулі зв'язку, а також до інших мікроконтролерів або комп'ютерів.
5. **Мережеві можливості:** Завдяки підтримці CAN і USB, STM32F3 може використовуватися в промислових мережах для обміну даними або для підключення до інших пристроїв для забезпечення більш складних обчислень або інтеграцій в більші системи.

2.9 Застосування STM32F3 в проекті

У цьому проекті STM32F3 може використовуватися як головний мікроконтролер для збору даних, обробки сигналів та взаємодії з ESP8266 для моніторингу Wi-Fi мереж. Завдяки потужній обробці цифрових сигналів і високій точності роботи з аналоговими сигналами, STM32F3 може ефективно взаємодіяти з різними сенсорами та модулями, збираючи інформацію про навколишнє середовище.

1. **Обробка та зберігання даних:** STM32F3 буде відповідати за отримання даних від GPS-модуля, а також за обробку Beacon Frames, отриманих від ESP8266. Дані можуть бути збережені на карті пам'яті або передаватися на інші пристрої для подальшої обробки.
2. **Інтерфейси для зв'язку:** STM32F3 може використовувати інтерфейси UART або SPI для комунікації з ESP8266, а також з іншими модулями, такими як датчики або зовнішні пристрої.
3. **Енергозбереження:** Використання режимів енергозбереження STM32F3 дозволить значно знизити споживану потужність пристрою, що є важливим для мобільних або портативних застосувань.

STM32F3 — це високопродуктивні мікроконтролери з багатими можливостями для обробки аналогових і цифрових сигналів, а також для підключення до інших пристроїв. Завдяки своїй гнучкості та багатофункціональності вони є чудовим вибором для проектів, де важлива точність обробки сигналів і швидкість роботи з даними, що робить їх ідеальними для застосувань у бездротових системах, вимірювальних пристроях та вбудованих системах.

2.10 ST HAL та CMSIS: Порівняння та Причини Використання CMSIS у Проекті

ST HAL (Hardware Abstraction Layer) є бібліотекою, розробленою STMicroelectronics для мікроконтролерів STM32. Вона надає абстракцію апаратного забезпечення, що дозволяє розробникам працювати з різними апаратними модулями, такими як GPIO, UART, SPI, I2C, таймери та інші, без необхідності вручну налаштовувати низькорівневі реєстри. Використовуючи HAL, програміст може легко взаємодіяти з апаратними компонентами, не замислюючись про деталі їх реалізації. Завдяки цій бібліотеці розробка програм для STM32 стає значно простішою, оскільки багато з операцій, таких як налаштування периферії або обробка переривань, вже є реалізованими. Однак, таке абстрагування додає певний рівень накладних витрат, що може вплинути на продуктивність системи, особливо коли потрібно працювати з високопродуктивними або низькорівневими операціями.

CMSIS (Cortex Microcontroller Software Interface Standard), розроблений ARM, надає інші можливості для програмування мікроконтролерів, зокрема тих, що базуються на архітектурі ARM Cortex. CMSIS є стандартом для програмного забезпечення, яке оптимізовано для роботи з мікроконтролерами на базі ARM, і пропонує набір інструментів для

взаємодії з ядром мікроконтролера. Це включає базові функції, необхідні для налаштування системних таймерів, обробки переривань, керування енергоспоживанням, а також оптимізовану обробку цифрових сигналів і керування периферією. CMSIS дозволяє максимально ефективно працювати з апаратними ресурсами, даючи програмісту доступ до детальних налаштувань і можливість оптимізувати код під конкретні задачі.

У цьому проекті вибір на користь CMSIS виправданий низкою факторів. Перш за все, CMSIS дає розробнику максимальний контроль над апаратним забезпеченням, що є важливим, коли необхідно виконувати завдання з високими вимогами до продуктивності та точності. Для завдань, пов'язаних з обробкою сигналів або збором даних з мережі, такий рівень контролю дозволяє знизити накладні витрати, які виникають при використанні HAL. CMSIS дає змогу працювати безпосередньо з реєстрами, що дозволяє створювати більш швидкі й ефективні програми, оптимізовані для конкретних завдань. Це дуже важливо для проектів, де кожен біт пам'яті та кожен такт процесора можуть мати значення.

Використання CMSIS також дає можливість значно знизити накладні витрати на пам'ять. У порівнянні з HAL, який включає додатковий код для абстракції апаратного рівня, CMSIS дозволяє зберігати лише необхідну частину коду, що важливо, коли ресурси мікроконтролера обмежені. Це дозволяє максимально ефективно використовувати пам'ять, що є критичним для більш складних проектів.

Крім того, CMSIS дозволяє більш детально керувати енергоспоживанням. У системах, що працюють на батареях або в умовах обмеженого енергоспоживання, програміст може використовувати можливості CMSIS

для точнішого налаштування режимів енергозбереження, що важливо для забезпечення довговічності роботи пристроїв.

Оскільки CMSIS є стандартом для всіх мікроконтролерів ARM, його можна використовувати в будь-яких проектах, де потрібно працювати з мікроконтролерами на базі ARM Cortex. Це робить його універсальним рішенням, яке може бути легко інтегроване з іншими бібліотеками чи інструментами. Це також дає перевагу в плані переносимості та сумісності з іншими розробками.

Незважаючи на те, що використання ST HAL може бути зручним і швидким для багатьох стандартних завдань, в нашому проекті, де потрібна висока продуктивність, точність і контроль над апаратним забезпеченням, CMSIS є більш доцільним вибором. Він дозволяє гнучко налаштувати систему, максимально оптимізувати використання апаратних ресурсів і забезпечити високу швидкість обробки даних, що є критичним для завдань, пов'язаних з обробкою Beacon Frames та іншими високопродуктивними операціями в бездротових мережах.

3 Підготовчий етап

На початковому етапі роботи було вивчено технічну документацію компонентів, що використовувались у проекті:

STM32 мікроконтролер: основний обчислювальний блок, що забезпечує управління всіма модулями.

ESP8266 модуль: пристрій для сканування бездротових мереж і передачі даних.

GPS-модуль GP01: необхідний для отримання точних географічних координат.

SD-картка: пристрій для збереження отриманих даних у зручному форматі.

Було проаналізовано можливі методи інтеграції цих компонентів у єдину систему, а також визначено архітектуру пристрою. Особлива увага приділялась забезпеченню стабільної роботи апаратної частини та мінімізації енергоспоживання, оскільки пристрій передбачав автономну роботу.

Крім того, було досліджено алгоритми роботи Wi-Fi модулів для отримання максимально точних даних про мережі, включаючи їхній SSID, MAC-адреси, рівень сигналу (RSSI) та інші параметри.

3.1 Розробка апаратної частини

На цьому етапі було побудовано схему підключення основних компонентів пристрою:

1. **Підключення ESP8266 до STM32:** забезпечення передачі даних через UART інтерфейс. Було протестовано взаємодію мікроконтролера з модулем для отримання списку доступних Wi-Fi мереж.
2. **Інтеграція GPS-модуля:** використання NMEA-протоколу для отримання координат. Було протестовано точність роботи модуля у відкритих місцевостях.
3. **Підключення SD-карти:** використання SPI протоколу для збереження даних. Проведено тестування запису та зчитування даних у файлах.

Особливістю роботи стало забезпечення коректної роботи всіх компонентів у єдиній системі. Було враховано можливі конфлікти при одночасній передачі даних між модулями та STM32.

3.2 Розробка програмного забезпечення

Програмне забезпечення було розроблено мовою C з використанням бібліотек для роботи з STM32. Було реалізовано такі модулі:

1. **Модуль сканування Wi-Fi:**
- Здійснював періодичний пошук доступних мереж за допомогою ESP8266.
- Збирав інформацію про SSID, MAC-адреси, рівень сигналу (RSSI).
2. **Модуль отримання GPS-даних:**
- Запитував географічні координати з GPS-модуля.
- Обробляв дані, що надходять у форматі NMEA, та витягував широту й довготу.
3. **Модуль збереження даних:**
- Формував записи у форматі CSV (дата, час, координати, SSID, MAC-адреса, RSSI).
- Записував інформацію на SD-карту.
4. **Модуль енергозбереження:**
- Реалізував функції переходу пристрою в режим очікування між скануваннями.

Для забезпечення стабільності роботи було проведено ретельне тестування коду, особливо в умовах одночасного зчитування даних із GPS та запису їх на SD-карту.

3.2 Тестування пристрою

Для перевірки працездатності пристрою було організовано серію польових випробувань. У ході тестів пристрій використовувався для збору даних у різних частинах міста.
Результати тестів включали:

- списки доступних Wi-Fi мереж із точними координатами їхнього розташування;
- стабільну роботу пристрою впродовж кількох годин без необхідності перезавантаження;
- точне визначення координат навіть у складних умовах (поблизу будівель).

Було виявлено та виправлено незначні недоліки в роботі GPS-модуля та збереженні даних.

3.4 Аналіз отриманих результатів

У результаті виконаної роботи було створено функціональний прототип пристрою для картографування Wi-Fi мереж. Зібрані дані можуть бути використані для:

- аналізу покриття Wi-Fi мереж;
- визначення зон із слабким сигналом;
- створення карт доступних точок доступу.

Підсумки роботи

У процесі розробки пристрою для картографування Wi-Fi мереж на базі мікроконтролера STM32 було виконано ряд важливих етапів, починаючи від проектування апаратної частини та закінчуючи реалізацією програмного забезпечення для збору і обробки даних. Розробка такого пристрою має велике значення для аналізу бездротових мереж, оскільки дозволяє виявляти зони з високим або низьким рівнем сигналу, що є важливим для оптимізації покриття і планування мереж.

У ході роботи були вирішені основні технічні завдання:

1. **Інтеграція компонентів:** Успішно здійснено інтеграцію різних компонентів, таких як Wi-Fi модуль ESP8266, GPS приймач, мікроконтролер STM32 і SD-картка для зберігання даних. Завдяки цьому пристрій може збирати дані про Wi-Fi мережі і супутникові координати в реальному часі, забезпечуючи високий рівень точності і надійності.
2. **Розробка програмного забезпечення:** Реалізовано програму для обробки даних, що надходять від Wi-Fi модуля та GPS приймача. Алгоритм збору даних і їх збереження на SD-картці забезпечує ефективну роботу пристрою навіть за умов обмежених ресурсів.
3. **Оптимізація енергоспоживання:** Для забезпечення автономної роботи пристрою було реалізовано ефективні методи управління енергоспоживанням. Важливим кроком стала оптимізація режимів сну мікроконтролера і Wi-Fi модуля, що дозволяє пристрою працювати тривалий час без підзарядки.
4. **Візуалізація та аналіз даних:** Дані, що збираються пристроєм, можуть бути використані для побудови карт покриття Wi-Fi мереж, що дозволяє оцінити якість сигналу в різних точках території. Ці

дані можуть бути використані для подальшого аналізу і оптимізації мереж.

5. **Вирішення технічних проблем:** Протягом роботи було вирішено низку технічних проблем, зокрема забезпечення коректної роботи в умовах нестабільного сигналу GPS і сканування Wi-Fi мереж з різними параметрами.

Висновок

У даному проекті ми здійснили розробку системи для збору та аналізу даних з Wi-Fi мереж, зокрема для прийому Beacon Frames та аналізу мережевих характеристик. Основною метою було створення ефективного пристрою, який би дозволяв відслідковувати бездротові мережі, що передають Beacon Frames, для подальшого аналізу та збереження цих даних. Для цього було обрано ряд сучасних компонентів, таких як мікроконтролери STM32 та ESP8266, GPS-модуль GP01, а також використання CMSIS для забезпечення високої продуктивності при програмуванні.

Вибір STM32 як основного мікроконтролера для управління пристроєм обумовлений його потужністю, багатофункціональністю та здатністю працювати в реальному часі з великими обсягами даних. Використання чистого CMSIS в даному проекті дозволяє досягти максимальної ефективності при роботі з апаратними ресурсами, даючи точний контроль над реєстрами мікроконтролера та забезпечуючи швидкість виконання операцій, необхідну для аналізу Wi-Fi Beacon Frames.

Використання ESP8266 в режимі монітора для прийому Beacon Frames дозволяє ефективно здійснювати моніторинг бездротових мереж у режимі реального часу. Завдяки гнучким можливостям цього модуля, вдалося

забезпечити стабільну передачу зібраних даних на основний мікроконтролер для подальшого аналізу та збереження.

Таким чином, реалізація проекту продемонструвала ефективність вибраних апаратних компонентів та програмного забезпечення для досягнення поставлених цілей. Завдяки гнучкості CMSIS та можливості налаштовувати апаратні ресурси на низькому рівні, вдалося забезпечити високу швидкість обробки даних, що є критичним для аналізу бездротових мереж.

Проект продемонстрував, що використання високопродуктивних мікроконтролерів, сучасних бездротових модулів та оптимізованих програмних бібліотек дозволяє створювати ефективні та надійні рішення для збору та аналізу даних у бездротових мережах, що може бути корисним у багатьох застосунках, таких як моніторинг безпеки мереж, аналіз покриття Wi-Fi, тощо

Список використаної літератури

1. **STM32 Documentation (STMicroelectronics)**
   https://www.st.com/en/microcontrollers-microprocessors/stm32f3-series/documentation.html
2. **CMSIS (Cortex Microcontroller Software Interface Standard)**
   https://arm-software.github.io/CMSIS_6/latest/General/index.html
3. **ESP8266 Documentation**
   https://github.com/esp8266/esp8266-wiki
4. **Wi-Fi 802.11 Protocol Specification**
   https://www.ieee802.org/11/
5. **GP01 GPS Module Datasheet**
   https://docs.ai-thinker.com/_media/gp-01_specification.pdf
6. **STM32CubeMX (STMicroelectronics)**
   https://www.st.com/resource/en/data_brief/stm32cubemx.pdf