МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н.Каразіна
Факультет математики і інформатики
Кафедра теоретичної та прикладної інформатики

Кваліфікаційна робота

бакалавр

на тему_____Розробка програмно-апаратних засобів радіоелектронного подавлення каналу зв'язку з дроном_____

Виконав: студент 4 курсу, групи МФ-42
спеціальність 122 «Комп'ютерні науки»
освітньо-професійна програма «Інформатика»

_Кононенко_А.О_____
(прізвище та ініціали)
Керівник
__Мєняйлов__Є.С_____
(прізвище та ініціали)
Рецензент
_____
(прізвище та ініціали)

Харків – 2023 року

Зміст

Вступ

1.1. Формулювання мети роботи, задач та обґрунтування актуальності теми

За останні роки дрони стали досить поширеним засобом військової та цивільної техніки. Вони використовуються для зйомки відео та фотографій, дослідження довкілля, доставки товарів, а також для виконання військових завдань. Проте, використання дронів може мати і негативні наслідки. Наприклад, дрони можуть використовуватися для здійснення терористичних актів, шпигунства, а також для впливу на безпеку польотів літаків та вертольотів. Таким чином, контроль над рухом дронів стає надзвичайно важливим завданням в сфері безпеки.

Одним із методів контролю над дронами є їх радіоелектронне подавлення. Тобто, розробка програмно-апаратних засобів, які здатні впливати на роботу радіоканалів дронів, є актуальною темою дослідження навіть у мирний час. З метою забезпечення безпеки мирного населення та військової інфраструктури, необхідно розробити простий, дешевий та портативний прилад протидії дронам.

Метою даної роботи є розробка програмно-апаратних засобів радіоелектронного подавлення каналу зв’язку з дроном у військовий та мирний час. Для досягнення цієї мети, поставлені наступні задачі:

– провести аналіз існуючих методів та засобів радіоелектронного подавлення каналу зв'язку з дроном;

– розробити алгоритми та програмне забезпечення для роботи з software defined radio;

– розробити програмну частину приладу та провести його випробування в реальних умовах.

1.2. Стислий огляд відомих результатів в області дослідження

Проблема захисту військових та цивільних об'єктів від дронів є актуальною для багатьох країн. З цієї причини, в останні роки, відбулося значне зростання досліджень в галузі боротьби з дронами.

Для виявлення дронів використовуються різноманітні технології, такі як радари, оптичні системи та радіоелектронні засоби.

Радари є однією з технологій, які використовуються для виявлення дронів. Радар працює на основі відбивання радіохвиль, які відправляються з радару до об'єкта та повертаються назад. Дрони можуть бути виявлені за допомогою радарів, які виявляють відбиті сигнали від металевих конструкцій дронів. Однак, радари мають деякі обмеження. Наприклад, вони не можуть працювати в місцях з великою кількістю перешкод, таких як ліси або міські зони, а також їх сигнал може бути спотвореним навколишніми об'єктами, що може призвести до помилкового виявлення.

Оптичні системи використовуються для виявлення дронів за допомогою відеокамер та інфрачервоного зондування. Вони можуть допомогти виявити дронів, які рухаються в повітрі або на землі, а також можуть виявляти теплові сигнатури, що випромінюються дронами. Однак, оптичні системи мають обмеження, такі як низька ефективність у поганих погодних умовах та недостатня чутливість до дронів, які використовують матеріали, що поглинають тепло.

Радіоелектронні засоби (РЕЗ) є ще однією ефективною технологією для виявлення та подавлення каналу зв'язку з дронами. РЕЗ використовуються для перехоплення радіосигналів, які передаються між дроном та пультом управління, і для налагодження перешкод на цьому каналі зв'язку. Важливою перевагою РЕЗ є можливість виявлення та подавлення каналу зв'язку з дронами на великих відстанях, незалежно від погодних умов.

Однак, РЕЗ також мають свої обмеження, які пов'язані з обробкою великої кількості даних, що необхідні для виявлення та ідентифікації дронів. Крім того, відомо, що деякі виробники дронів використовують шифрування для своїх каналів зв'язку, що може ускладнити роботу РЕЗ та знизити їх ефективність.

Основним недоліком усіх виробів з трьох категорій є їх ціна але недавній розвиток у сфері програмного радіо та технології SDR (Software Defined Radio) відкрили нові можливості для виявлення та подавлення каналу зв'язку з дронами.

Технологія SDR (Software-Defined Radio або програмно-визначене радіо) - це метод передачі та отримання радіосигналів, в якому аналогові сигнали конвертуються в цифрову форму і обробляються програмним забезпеченням. Це означає, що функції, які раніше були реалізовані за допомогою аналогових схем, тепер виконуються програмним забезпеченням.

У порівнянні з аналоговою технологією, SDR має кілька переваг. Одна з найбільших переваг полягає в тому, що можливість переналаштування діапазону частот відбувається програмно, що дає можливість працювати з різними типами радіосигналів. Крім того, SDR може забезпечити кращу якість прийому і передачі завдяки цифровому сигнальному обробленню та може бути оновлюваний шляхом зміни програмного забезпечення, що знижує вартість оновлення та підтримки обладнання.

З іншого боку, аналогові вироби використовують аналогові схеми для обробки радіосигналів, що може бути менш точним та залежним від певних параметрів технології виготовлення компонентів. Крім того, при зміні стандартів передачі радіосигналів необхідно замінювати обладнання, що може бути дуже витратно.

SDR може бути використаний для виявлення та ідентифікації радіосигналів дронів та їхнього подавлення, забезпечуючи нові можливості для боротьби з дронами та ціна виробів використовуючих цю технологію значно менша за вироби що використовують аналогову технологію.

У зв'язку з тим, що дрони стають все більш поширеними, захист від них стає все більш важливим завданням для військових та правоохоронних органів. Технології, що використовуються для виявлення та подавлення каналу зв'язку з дронами, розвиваються все швидше, проте на сьогоднішній день немає універсального засобу для протидії всім типам дронів. Кожен засіб має свої переваги та обмеження, і ефективність його використання залежить від конкретних умов.

Основною метою є створення прототипу засобу, який зможе ефективно виявляти та подавляти канал зв'язку з різними типами дронів використовуючи дешеве обладнання для ентузіастів.

Крім того, ми плануємо провести порівняльний аналіз розробленого приладу з іншими технологіями та засобами, які використовуються для протидії дронам. Такий аналіз дозволить визначити переваги та обмеження нашого приладу в порівнянні з іншими засобами, що використовуються на сьогоднішній день.

Основна частина

2 Протоколи зв’язку з дроном

Для розуміння проблеми радіоелектронного подавлення каналу зв'язку з дронами, важливо ознайомитися з різними видами зв'язку, які використовуються дронами. Вони можуть використовувати різноманітні технології зв'язку, включаючи Wi-Fi, аналоговий сигнал, цифровий сигнал та інші. Розглянемо деякі з них:

Wi-Fi:

Багато дронів використовують Wi-Fi для передачі даних між дроном та пультом управління. Wi-Fi є популярним протоколом бездротового зв'язку, який працює на основі стандарту IEEE 802.11. Цей протокол забезпечує швидку передачу даних і може використовуватися для контролю дрона та передачі відео з камери на пульт управління. Розпізнавання та перешкоджання Wi-Fi сигналу може бути важливим аспектом при розробці системи радіоелектронного подавлення для боротьби з дронами.

Плюси:

– Висока швидкість передачі даних: Wi-Fi може забезпечити високу швидкість передачі даних, що дозволяє в реальному часі контролювати дрона та отримувати відео з камери.

– Популярність та сумісність: Wi-Fi є широко поширеним стандартом бездротового зв'язку, що сприяє сумісності з багатьма пристроями та мережами.

– Низька вартість обладнання: Wi-Fi часто вже вбудований у багато пристроїв, що зменшує витрати на додаткове обладнання.

Мінуси:

– Обмежена дальність передачі даних: Wi-Fi має обмежену дальність передачі даних, зазвичай до кількох сотень метрів, що обмежує радіус дії дрона.

– Вразливість до перешкод: Wi-Fi сигнал може бути вразливим до перешкод та інтерференції, що може призвести до втрати зв'язку .

Аналоговий сигнал:

Деякі старіші моделі дронів використовують аналогові системи передачі сигналу. Аналоговий сигнал може передаватися на різних частотах, наприклад, на частотах FM або AM. Цей тип зв'язку використовує модуляцію аналогового сигналу для передачі інформації. Однак, аналоговий сигнал може бути вразливим до перешкод та інтерференції, що створює можливість для його радіоелектронного подавлення.

Плюси:

– Простота використання та низька вартість обладнання: аналогові передавачі та приймачі широко доступні і не вимагають складної настройки.

– Доступність різних частотних діапазонів: аналоговий зв'язок дозволяє використовувати різні частоти для передачі сигналу.

Мінуси:

– Низька якість передачі даних: аналоговий сигнал більш вразливий до шуму, перешкод та втрати сигналу, що може призвести до спотворення сигналу та втрати даних.

– Обмежена швидкість передачі даних: передача великого обсягу даних, зокрема відео високої якості, може бути складною через обмежену пропускну здатність аналогового зв'язку.

Цифровий сигнал:

Сучасні дрони все частіше використовують цифрові системи передачі даних. Цифровий сигнал може бути переданий у вигляді пакетів даних, які кодуються та декодуються за допомогою різних протоколів. Наприклад, деякі дрони використовують протоколи зв'язку, такі як MAVLink або DJI Ocusync. Цифрові системи можуть забезпечувати високу якість передачі даних та більшу стійкість до перешкод, що може ускладнити завади в їх каналі зв'язку.

Плюси:

– Висока якість передачі даних: цифровий сигнал забезпечує високу якість передачі даних та більшу стійкість до шуму, перешкод та втрати сигналу.

– Швидка передача даних: цифрові системи можуть забезпечувати швидку передачу великого обсягу даних, включаючи відео високої якості.

– Більша захищеність від перешкод: цифрові протоколи можуть бути більш стійкими до перешкод та інтерференції, забезпечуючи більш надійний зв'язок з дроном.

Мінуси:

– Вища складність налаштування: цифровий зв'язок може вимагати більшої настройки та складнішої системи передавачів та приймачів.

– Вища вартість обладнання: обладнання для цифрового зв'язку може бути дорожчим порівняно з аналоговими рішеннями.

Інші технології: Окрім Wi-Fi, аналогового та цифрового зв'язку, деякі дрони можуть використовувати інші комунікаційні технології, такі як Bluetooth, LTE або навіть власні високочастотні радіо-протоколи. Кожна з

цих технологій має свої особливості, які варто враховувати при розробці засобів радіоелектронного подавлення.

2.1 GPS

Це лише кілька прикладів видів зв'язку з дронами та їх переваги та недоліки. Враховуючи специфіку завдання радіоелектронного подавлення, важливо вивчити конкретний протокол, який використовується дроном, щоб розробити ефективний прилад для його протидії.

Також більшість дронів на ринку використовують протокол GPS. Протокол GPS (Global Positioning System) є системою навігації та позиціонування, яка використовує супутникові сигнали для визначення географічного положення дрона. GPS працює на основі мережі супутників,

розташованих на орбіті навколо Землі, і приймача GPS, встановленого на дроні.

Технічні деталі протоколу GPS включають наступні елементи:

– Супутники GPS: GPS мережа складається з 24 супутників, які обертаються на зазначеній орбіті. Кожен супутник випромінює сигнал, який містить інформацію про своє положення та точний час відправлення сигналу.

– Приймач GPS: Дрон використовує приймач GPS, що приймає сигнали від супутників і обробляє їх для визначення своєї географічної координати. Приймач аналізує час прийняття сигналу від різних супутників і використовує метод трилатерації для визначення точного місцезнаходження дрона.

– Сигнали GPS: Сигнали GPS передаються на двох носіях - L1 та L2. L1-сигнал використовується для цивільних застосувань, тоді як L2-сигнал зазвичай використовується для військових та професійних застосувань. Сигнали містять інформацію про час, позицію та корекції для покращення точності позиціонування.

Спуфінг GPS є методом атаки, при якому зловмисник передає підроблені сигнали GPS, що призводить до спотворення місцезнаходження дрона або вводу його в помилку. Ця атака може бути виконана за допомогою спеціалізованого обладнання, такого як спуфінг-генератори сигналу GPS. Зловмисники можуть замінювати справжні сигнали GPS підробленими сигналами, які мають неправильну інформацію про час, координати або швидкість.

Спуфінг GPS є атакою, при якій зловмисники передають підроблені сигнали GPS, що можуть змінити напрямок навігації дрона або навіть посадити його якщо підробити координати безпольотної зони. Давайте розглянемо більш докладно, як працює цей процес .

– Перехоплення сигналу GPS: Зловмисники використовують SDR для перехоплення сигналу GPS, який надсилається супутниками. Вони використовують високочутливі антени та SDR-пристрої для отримання слабкого сигналу GPS.

– Аналіз структури сигналу GPS: Отриманий сигнал розкладається на різні компоненти, такі як преамбула, навігаційні дані (ephemeris), коригуючі дані (almanac) та кодові фази де :

– Преамбула: Це початкова частина сигналу, що містить синхронізаційні сигнали та інші допоміжні дані для визначення часу та фази сигналу.

– Навігаційні дані (ephemeris): Ці дані містять інформацію про орбіти супутників, їх точні положення та часові параметри. Вони необхідні для визначення місцезнаходження приймача.

– Коригуючі дані (almanac): Ці дані містять загальну інформацію про всі супутники GPS, таку як їх номери та стан. Вони використовуються для пришвидшення визначення доступних супутників.

– Кодові фази: Сигнал GPS має кодові фази, які використовуються для вимірювання відстані між приймачем та супутниками.

– Модифікація сигналу: Зловмисники вносять зміни в декодований сигнал GPS, щоб підробити інформацію про місцезнаходження. Наприклад, вони можуть змінити часові дані, координати супутників або параметри сигналу.

– Генерація підробленого сигналу: Після модифікації сигналу зловмисники використовують SDR для генерації підробленого сигналу GPS з новими параметрами. Вони можуть відтворювати цей підроблений сигнал і передавати його повітрям.

– Вплив на приймач: Після передачі підробленого сигналу GPS приймач сприймає його як інформацію про місцезнаходження. Залежно

від змін, внесених у підроблений сигнал, приймач може отримати неправдиві дані про своє місцезнаходження.

Існує багато досліджень, що досліджують можливості спуфінгу GPS за допомогою SDR. Наприклад, дослідження "GPS Spoofing Detection Using a Software-Defined Radio" (2017) авторства A. M. Salem та A. H. Zaher, досліджує методи виявлення спуфінгу GPS з використанням SDR.

Також існує відкрите програмне забезпечення з відкритим вихідним кодом, як gps-sdr-sim, яке дозволяє користувачам створювати підроблені сигнали GPS та використовувати їх для тестування систем GPS або дослідження захисту від спуфінгу.

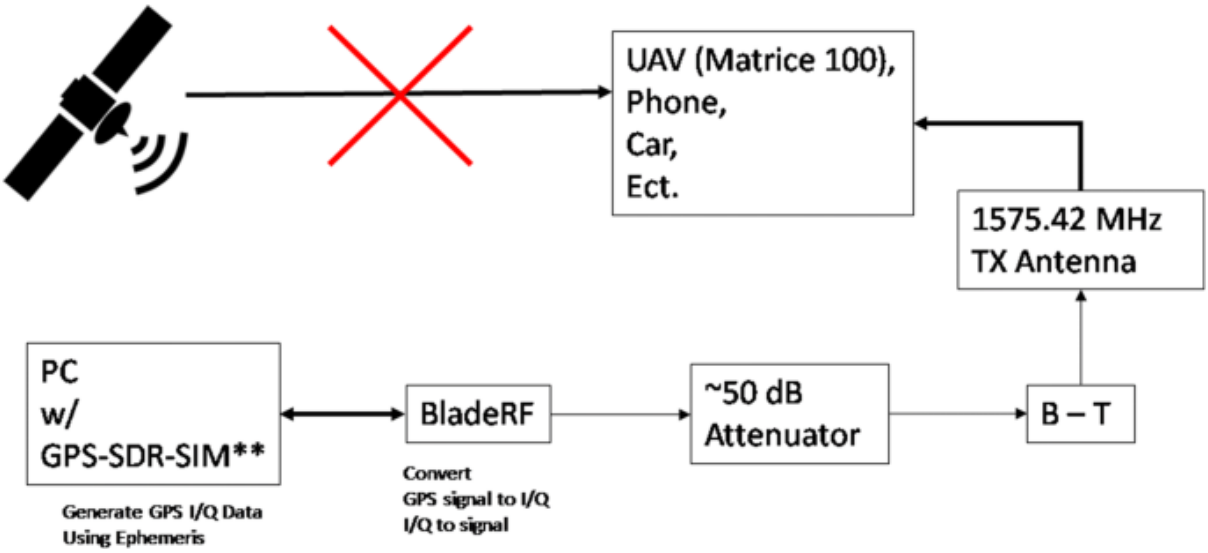


Рисунок 1 - Процес спуфінгу GPS

Однак важливо зазначити, що спуфінг GPS є незаконною діяльністю та може мати серйозні наслідки для навігаційної безпеки та приватності. Ці технічні деталі наведені тут з метою надати інформацію про можливість такої атаки.

2.2 Аналоговий сигнал

Протокол аналогового зв'язку в дронах може варіюватися в залежності від виробника та моделі дрона. Типово, дрони використовують різні частоти для передачі і прийому аналогових сигналів між дроном і керуючим пристроєм.

Структура аналогового сигналу може бути представлена як неперервна хвиля змінної амплітуди. Цей сигнал може мати різні параметри, такі як частота несучої хвилі, модуляція сигналу та формат передачі даних.

Найпоширеніші частоти, які використовуються в аналоговому зв'язку з дронами, знаходяться в діапазоні 2,4 ГГц (наприклад, частота Wi-Fi), 5,8 ГГц та 900 МГц. Ці частоти є популярними через свою доступність та можливість використання без ліцензій.

Проте, через аналогову природу цих протоколів, вони піддаються різного роду атакам. Деякі з них включають:

– Jamming: Атака за допомогою шуму або інтерференції на частоті передачі, що призводить до зниження якості зв'язку або повної втрати зв'язку між дроном і керуючим пристроєм.

– Signal Spoofing: Ця атака полягає в створенні підробленого сигналу, який підміняє легітимний сигнал, що передається між дроном і керуючим пристроєм. Це може призвести до впливу на поведінку дрона або перехоплення його контролю.

– Replay Attacks: Під час цієї атаки зловмисник перехоплює аналоговий сигнал, що передається між дроном і керуючим пристроєм, і повторно відтворює його. Це може призвести до виконання попередньо записаних команд або зміни стану дрона.

– Frequency Hopping: Деякі аналогові протоколи використовують техніку перехоплення частоти, коли частота передачі періодично змінюється. Атака на такі протоколи може полягати в прогнозуванні частоти зміни та перехопленні сигналу під час переходу на нову частоту.

Дослідження в галузі атак на аналогові протоколи зв'язку з дронами продовжуються. Наприклад, "A Comprehensive Analysis of UAV Wireless Communications: Physical Layer Vulnerabilities and Security Solutions" (2020) виконувало огляд фізичних вразливостей аналогових протоколів зв'язку з дронами та пропонувало методи захисту.

Важливо зазначити, що будь-які атаки на протоколи зв'язку з дронами без належної дозволу і згоди є незаконними. Ця інформація повинна розглядатися виключно в освітніх цілях, а дотримання законів та правил, пов'язаних з використанням дронів та безпекою, є обов'язковим.

Аналогові протоколи зв'язку з дронами поступово замінюються цифровими протоколами з кожним роком. Цифрові протоколи забезпечують більшу швидкість передачі даних та точність інформації, що є важливим для дронів, особливо в комерційних та професійних сферах. Вони використовуються для передачі команд керування, потокового відео та телеметричних даних між пультом керування та дроном.

Одна з основних переваг цифрових протоколів полягає в їх стійкості до шуму та інтерференції. Цифрові сигнали можуть бути ефективно захищені від спотворень та збоїв завдяки вбудованим механізмом корекції помилок. Крім того, цифрові протоколи можуть забезпечити більшу пропускну здатність, дозволяючи передавати більше даних за одиницю часу.

Проте варто зазначити, що у деяких випадках аналогові протоколи все ще можуть бути використані в деяких моделях дронів, особливо в простіших моделях або там, де вимагається низька латентність та швидкість зв'язку. Наприклад, аналогові протоколи можуть бути

використані для передачі відеосигналу з вбудованої камери дрона на пульт керування, щоб пілот міг спостерігати зображення в реальному часі.
Загалом, розвиток технологій та дослідження в галузі цифрових протоколів зв'язку з дронами продовжуються, що сприяє поступовому відмовленню від аналогових протоколів, через це атака на ций протокол не буде розглядатись у цій роботі.

2.3 WiFi

Протокол Wi-Fi (бездротова локальна мережа) є одним з найпоширеніших протоколів бездротового зв'язку, який дозволяє підключати пристрої до мережі Інтернет через бездротовий зв'язок. Він працює на різних частотах, таких як 2,4 ГГц і 5 ГГц, і використовується у багатьох пристроях, включаючи дрони.
На низькому рівні, протокол Wi-Fi базується на стандарті IEEE 802.11, який визначає основні принципи передачі даних у бездротовій мережі.
Wi-Fi (або IEEE 802.11) фрейм - це структурована одиниця даних, яка використовується для передачі інформації через бездротову мережу Wi-Fi. Фрейм Wi-Fi має наступну побітову структуру:

– Преамбула (Preamble) - 56 біт. Використовується для синхронізації передачі даних і встановлення зв'язку між передавачем і приймачем.

– Заголовок керування (Frame Control) - 16 біт. Містить у собі інформацію про тип фрейма, адреси призначення та джерела, а також деякі контрольні біти.

– Довжина (Length) - 16 біт. Вказує загальну довжину фрейма, включаючи заголовок та дані.

– Адреса одержувача (Receiver Address) - 48 біт. Вказує MAC-адресу приймача, до якого призначений фрейм.

– Адреса передавача (Transmitter Address) - 48 біт. Вказує MAC-адресу відправника фрейма.

– Додаткова адреса 1 (Address 1) - 48 біт. Використовується для передачі додаткових адресних даних (залежно від типу фрейма).

– Додаткова адреса 2 (Address 2) - 48 біт. Використовується для передачі додаткових адресних даних (залежно від типу фрейма).

– Додаткова адреса 3 (Address 3) - 48 біт. Використовується для передачі додаткових адресних даних (залежно від типу фрейма).

– Послідовності (Sequence Control) - 16 біт. Використовується для нумерації і управління послідовністю фреймів.

– Заголовок даних (Data) - змінна довжина (0-2312 біт). Містить корисні дані, які передаються через Wi-Fi мережу (наприклад, IP-пакети).

– FCS (Frame Check Sequence) - 32 біти. Контрольна сума, яка використовується для перевірки цілісності даних у фреймі.

Структура пакета Wi-Fi може змінюватися в залежності від типу фрейму. Найбільш поширеними типами фреймів є:

– Менеджер фрейм (Management Frame): Використовується для керування мережею, включаючи реєстрацію, аутентифікацію та управління точками доступу.

– Керуючий фрейм (Control Frame): Використовується для керування передачею даних, включаючи затримку передачі, підтвердження отримання та інші параметри.
– Фрейм даних (Data Frame): Використовується для передачі фактичних даних між пристроями у мережі.

Management frames в протоколі Wi-Fi використовуються для керування мережею, обміну інформацією між точками доступу і клієнтськими пристроями, а також для встановлення та збереження з'єднання. Кожен тип фрейма має свою функцію та специфічний код. Ось детальний опис кожного типу фрейма:

– Beacon Frame:
  – Призначення: Використовується точками доступу для розсилання інформації про мережу та її параметри.
  – Код у двійковому форматі: 1000 0000 0000 0000 (0x8000)
– Probe Request Frame:
  – Призначення: Відправляється клієнтськими пристроями для пошуку доступних мереж.
  – Код у двійковому форматі: 0100 0000 0000 0000 (0x4000)
– Probe Response Frame:
  – Призначення: Відправляється точками доступу відповідно на Probe Request і містить інформацію про мережу.
  – Код у двійковому форматі: 0101 0000 0000 0000 (0x5000)
– Authentication Frame:
  – Призначення: Використовується для аутентифікації клієнта перед підключенням до мережі.
  – Код у двійковому форматі: 1011 0000 0000 0000 (0xB000)
– Association Request Frame:

– Призначення: Відправляється клієнтськими пристроями для запиту на асоціацію з точкою доступу.

– Код у двійковому форматі: 0000 0000 0000 0000 (0x0000)

– Association Response Frame:

– Призначення: Відправляється точками доступу відповідно на Association Request для підтвердження асоціації.

– Код у двійковому форматі: 0001 0000 0000 0000 (0x1000)

– Disassociation Frame:

– Призначення: Використовується для відключення клієнта від мережі.

– Код у двійковому форматі: 1010 0000 0000 0000 (0xA000)

– Deauthentication Frame:

– Призначення: Використовується для деаутентифікації клієнта з мережі.

– Код у двійковому форматі: 1100 0000 0000 0000 (0xC000)

– Action Frame:

– Призначення: Використовується для передачі спеціальних дій або повідомлень між точками доступу і клієнтськими пристроями.

– Код у двійковому форматі: 1101 0000 0000 0000 (0xD000)

Кожен фрейм має заголовок, що містить поле "Frame Control", яке визначає тип фрейма та його параметри. Коди фреймів у двійковому форматі показуються з використанням 16-бітного поля "Frame Control".

Ці фрейми грають важливу роль у керуванні і підтримці бездротових мереж Wi-Fi, забезпечуючи роботу точок доступу та клієнтських пристроїв. Коректна інтерпретація та обробка цих фреймів є важливою для забезпечення стабільної та безпечної роботи мережі Wi-Fi.

Детальніше розглянемо Deauthentication frame.

Deauthentication frame є одним з типів management frames в протоколі Wi-Fi. Його призначення полягає в деаутентифікації (відключенні) клієнта від

бездротової мережі. Цей фрейм надсилається від точки доступу (AP) до клієнтського пристрою, щоб повідомити його про відключення з мережі. Reason Code визначає причину відключення і може бути одним зі значень:

– Unspecified reason (причина не вказана)

– Previous authentication no longer valid (попередня аутентифікація більше не дійсна)

– Deauthenticated because sending STA is leaving (деаутентифікація через виїзд відправляючого STA)

– Disassociated due to inactivity (роз'єднання через неактивність)

– Disassociated because AP is unable to handle all currently associated STAs (роз'єднання через неможливість точки доступу обробити всі асоційовані STAs)

– Class 2 frame received from nonauthenticated STA (отримано клас 2 фрейм від невхідної STA)

– Class 3 frame received from nonassociated STA (отримано клас 3 фрейм від нероз'єднаної STA)

– Disassociated because sending STA is leaving (роз'єднання через виїзд відправляючого STA)

Deauthentication frame може бути використаний для різних цілей, таких як заборона доступу до мережі для певного клієнта, змушення переаутентифікуватися або роз'єднання через неактивність. Деаутентифікація може бути використана як захисний механізм для забезпечення безпеки мережі та управління ресурсами. Але ця функціональність може також бути використана для атак

Атака Deauthentication (деаутентифікації) є одним з видів атак на бездротові мережі Wi-Fi. Під час цієї атаки зловмисник намагається відключити підключених клієнтів від точки доступу, надсилаючи спеціальні Deauthentication frames.

Атака Deauthentication використовує недолік в безпеці протоколу Wi-Fi, що дозволяє надсилати Deauthentication frames з будь-якою MAC-адресою в якості відправника. Цю проблему було вирішено у стандарту 802.11w, але доволі мало приладів які використовують цей стандарт. Зловмисник може відправляти фальшиві Deauthentication frames до точки доступу або клієнтів, використовуючи різні техніки, такі як "перехоплення" трафіку, "маніпулювання" сигналом використовуючи Wi-Fi адаптери які мають функціональність Packet Injection .

Атака Deauthentication може мати наступні наслідки:

– Відключення клієнта від точки доступу: Зловмисник може відключити підключеного клієнта від мережі, змушуючи його повторно аутентифікуватися та встановлювати нове з'єднання.

– Відключення точки доступу від клієнтів: Зловмисник може відключити всіх або певних клієнтів від точки доступу, перешкоджаючи їх сполученню з мережею.

– Зміна з'єднання клієнта: Зловмисник може використовувати атаку Deauthentication, щоб викликати втрату зв'язку у певних клієнтів і спробувати перехопити їх з'єднання або змусити їх підключатися до підробленої мережі, підконтрольної зловмиснику.

– Створення спаму в мережі: Зловмисник може відправляти багато фальшивих Deauthentication frames, створюючи перевантаження мережі та перешкоджаючи нормальному зв'язку.

Для здійснення атаки Deauthentication зловмиснику необхідно знати MAC-адресу цілі (пристрою, який він хоче відключити) та MAC-адресу точки доступу, до якої пристрій підключений. Зловмисник відправляє фрейми Deauthentication зі своїм власним MAC-адресою в якості відправника, але зі зміненою MAC-адресою цілі, щоб виглядати як автентичний сигнал від точки доступу. Щоб їх отримати атакуючий перехоплює фрейми між

ціллю та точкою доступу, отримавши них він формує підроблений фрейм за цією формою:

– Тип та підтип фрейма (2 байти): Ідентифікує фрейм як фрейм управління та тип Deauthentication.

– Керуючий флаг (2 байти): Вказує на тип керування, в даному випадку - Deauthentication.

– Довжина фрейма (2 байти): Вказує на загальну довжину фрейма, включаючи заголовок та поле даних.

– MAC-адрес приймача (6 байт): Вказує MAC-адресу пристрою, який буде відключений.

– MAC-адрес відправника (6 байт): Вказує MAC-адресу точки доступу або зловмисника, який відправляє фрейм.

– MAC-адреса BSSID (6 байт): Вказує MAC-адресу точки доступу.

– Послідовний номер (2 байти): Ідентифікує послідовний номер фрейма для керування порядком фреймів.

– Причина (2 байти): Вказує причину відключення.

Зловмисник може надсилати фрейми Deauthentication в повторюваному режимі, щоб переконатися, що пристрій не зможе встановити з'єднання з точкою доступу. Це може призвести до втрати зв'язку та перебоїв в роботі підключених пристроїв.

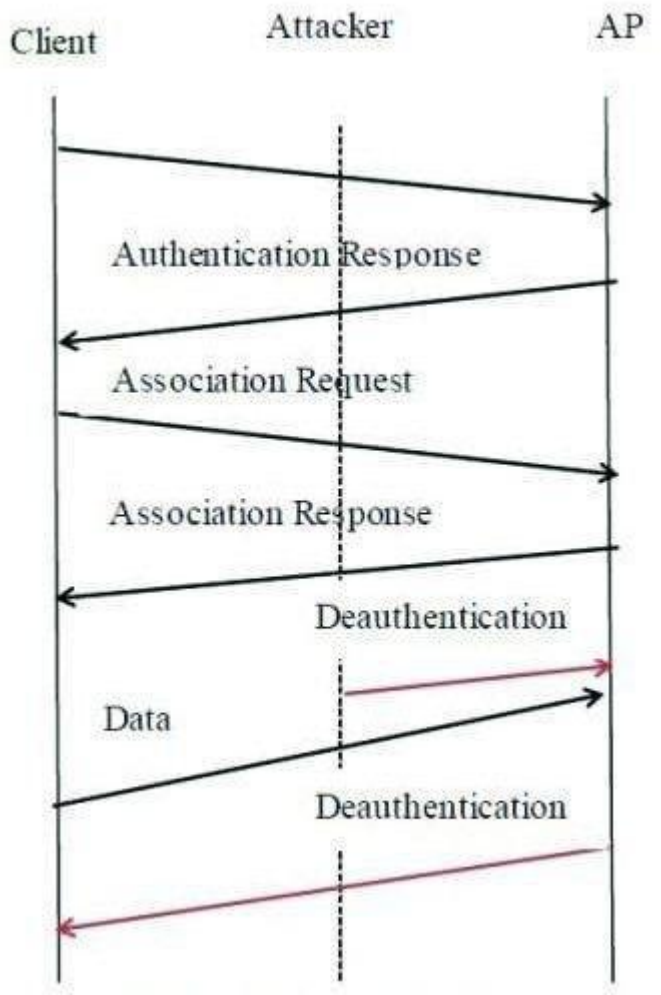


Рисунок 2 - Атака Deauthentication

Атака Deauthentication може бути використана для різних цілей, таких як злам доступу до бездротових мереж, перехоплення трафіку, спам-атаки та інші зловживання. Ця атака є одним з векторів атак на безпеку мереж Wi-Fi і вимагає від операторів мереж та користувачів вжиття заходів безпеки для запобігання її наслідкам. Вона також може бути використана для розладу комунікацій с дроном, та показує себе дуже ефективно проти дронів що використовують цей протокол. Це наприклад було продемонстровано на Defcon 23 у виступі під назвою “Robinson and Mitchell - Knocking my neighbors kids cruddy drone offline“. Під дією атаки розривається зв’язок між дроном та пультом, що переводить дрон у Failsafe Mode, який може відрізнятись у різних виробників дронів, наприклад у представленному виступі дрон моментально сідав після

виконання атаки. Додатково до ефективності даної атаки вона дуже легка у виконанні. Існує багато open source додатків які імплементують цю атаку, наприклад пакет Aircrack-ng, який має додатки airodump-ng (для знаходження Mac адрес) і aireplay-ng (для надсилання підроблених пакетів, які включають Deauth), які ми використовуємо для цієї демонстрації. На жаль дрон який ми маємо не може працювати в Wi-Fi режимі, тому демонстрація буде проводитись на іншому приладі. Ця демонстрація має сенс тому що усі прилади що використовують один і теж стандарт – Wi-Fi, та однаково вразливі до цієї атаки.

Хоча на демонстрації атака проводилася вручну, її можна автоматизувати через формат MAC адреси:

Формат MAC-адреси: XX:XX:XX:XX:XX:XX або XX-XX-XX-XX-XX-XX, де кожен XX представляє собою одну шістнадцяткову цифру (від 0 до 9 або від A до F).

Наприклад, припустимий формат MAC-адреси може виглядати так: 00:1A:2B:3C:4D:5E або 00-1A-2B-3C-4D-5E.

Зверніть увагу, що перша половина MAC-адреси (три групи) називається OUI (Organizationally Unique Identifier) і ідентифікує виробника мережевого обладнання, а друга половина (три групи) є унікальним ідентифікатором, що присвоюється самим виробником.

Тому є можливість зберегти усі відомі OUI виробників дронів та автоматизувати відбір MAC адрес та підорбки пакетів для роботи без втручання людини.

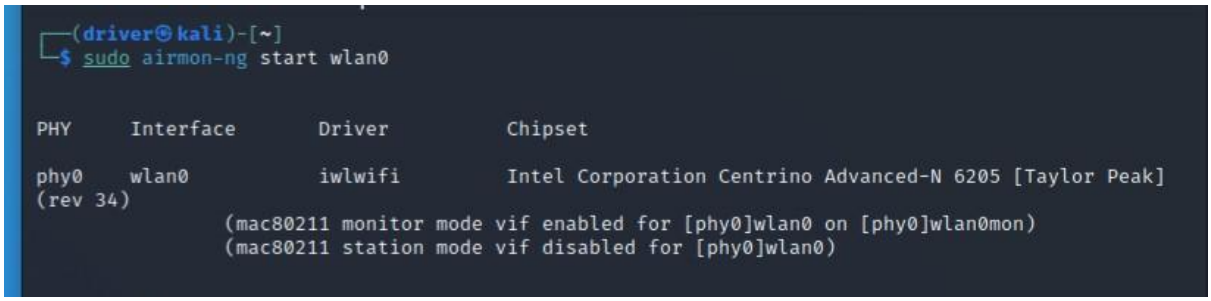
Для демонстрації цієї атаки нам потрібно:

1. Комп’ютер з операційною системою Linux або телефон з ОС Android з модифікованим ядром.
2. Wi-Fi адаптер з можливістю Packet Injection
3. Wi-Fi роутер та Wi-Fi клієнт (дрон та пульт чи подібне)

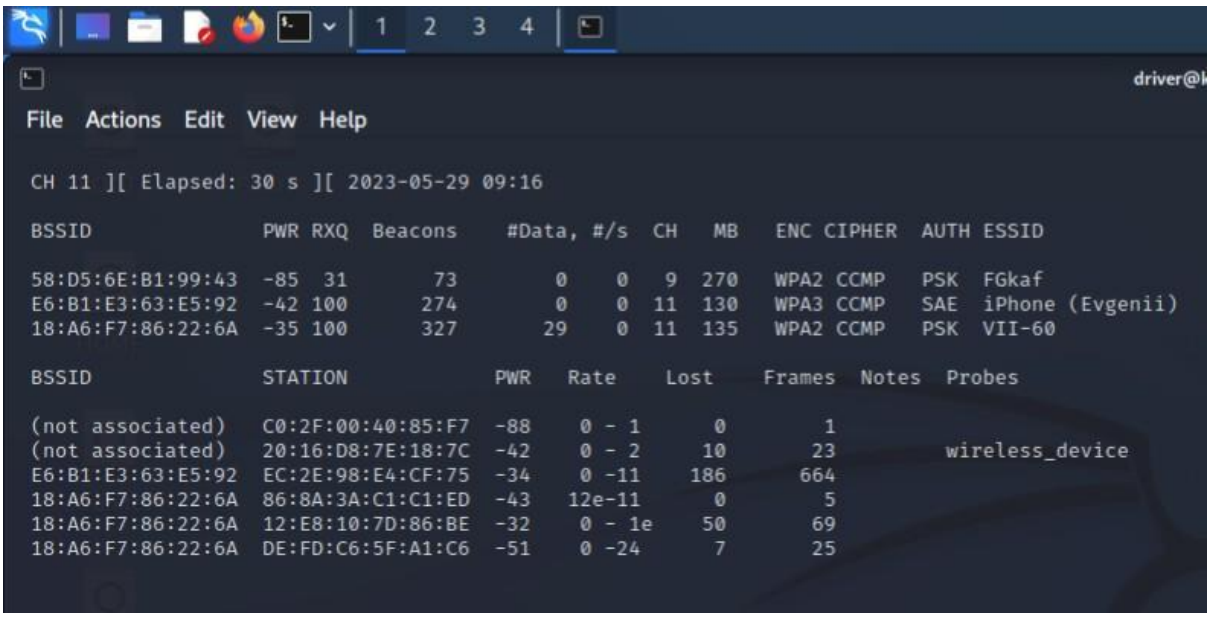
4. aircrack-ng чи аналоги (mdk3)

Проведемо демонстрацію

1. Підключимо клієнта до роутеру
2. Переведемо адаптер до режиму монітору

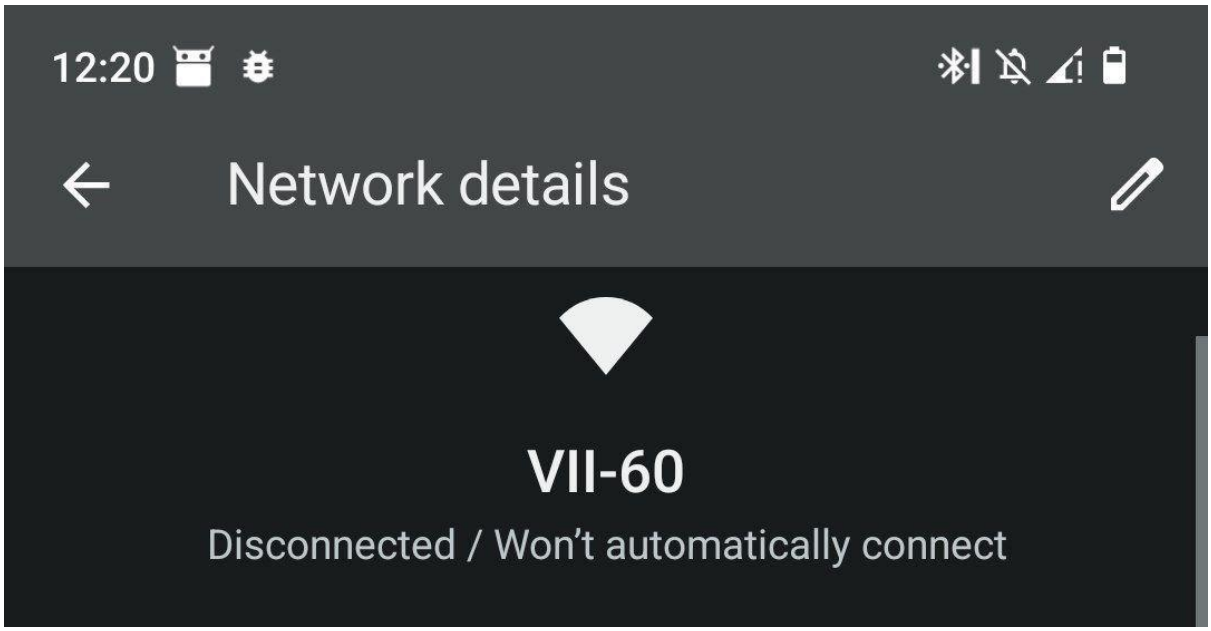


3. Використаємо airodump-ng для пошуку атакуємого роутера.Бачимо що цільовий роутер працює на 11 каналі, тому ми фіксуємо адаптер на 11 каналі, також ми бачимо BSSID цільового роутера (18:A6:F7:86:22:6A), та MAC адресу (Station) цілі (12:E8:10:7D:86:BE).



4. Знаючи BSSID та MAC ми можемо провести атаку за допомогою aireplay

5. Бачимо результат



Тому можна зробити висновок що подібна атака все ще актуальна і буде актуальна доки стандарт аутентифікації WPA3 повністю не замінить застарілий WPA2.

2.4 Цифровий сигнал

Оглянемо останній та найпоширеніший вид зв'язку – цифровий сигнал. У цьому контексті протоколи, такі як MavLink та OcuSync, відіграють значну роль. Давайте детальніше розглянемо їх та інші аспекти цифрових протоколів.Кожна компанія, що розробляє дрони, може використовувати власні імплементації протоколів зв'язку. Це означає, що імплементація може відрізнятися в залежності від вимог компанії та можливостей пристрою. Різні пристрої можуть мати відмінності в швидкості передачі, потужності сигналу, дальності зв'язку та підтримуваних функцій. Кожна компанія старається покращити ефективність та надійність свого протоколу для кращого взаємодії з дроном.

Звичайно, основним завданням модуляції цифрового сигналу є передача цифрових даних через аналоговий канал зв'язку. Це досягається шляхом перетворення цифрових бітів на аналоговий сигнал, який може бути переданий через канал зв'язку. Існує кілька різних видів модуляції, які використовуються для цих цілей. Давайте розглянемо найпоширеніші з них:

Amplitude Shift Keying (ASK):

ASK є одним з простих методів модуляції, де амплітуда аналогового сигналу змінюється для кодування бітів даних. Якщо біт 1, то амплітуда сигналу висока, якщо біт 0, то амплітуда сигналу низька. Цей метод простий у реалізації, але вразливий до шуму та спотворень.

Frequency Shift Keying (FSK):

FSK використовує зміну частоти аналогового сигналу для кодування бітів даних. Кожен біт кодується на певну частоту. Наприклад, біт 1 може бути кодований як сигнал з високою частотою, а біт 0 - як сигнал з низькою частотою. Цей метод є стійким до шуму, але вимагає більшої пропускної здатності каналу.

Phase Shift Keying (PSK):

PSK використовує зміну фази аналогового сигналу для кодування бітів даних. Є кілька варіантів PSK, включаючи Binary Phase Shift Keying (BPSK), де фаза сигналу змінюється на 180 градусів для кодування бітів. Наприклад, біт 1 може мати фазу 0 градусів, а біт 0 - фазу 180 градусів. Існують також більш складні варіації, такі як Quadrature Phase Shift Keying (QPSK), де фаза сигналу змінюється на 90 або 180 градусів для кодування двох бітів одночасно.

Quadrature Amplitude Modulation (QAM):

QAM поєднує зміни фази та амплітуди сигналу для кодування даних. Він дозволяє передавати більше бітів на символ, що дозволяє підвищити швидкість передачі даних. QAM може мати різні варіації, такі як 16-QAM або 64-QAM, які використовують різні комбінації фази і амплітуди для кодування бітів.

Також важливо пам’ятати про OFDM.

OFDM (Orthogonal Frequency Division Multiplexing) - це метод модуляції, в якому широкосмуговий сигнал розбивається на багато вузькосмугових

субносій, що передаються паралельно. Кожна субносія має ортогональну взаємну ортогональність, що дозволяє їм існувати поруч без спотворення один одного. OFDM забезпечує ефективне використання спектру, високу стійкість до інтерференції та високу швидкість передачі даних. Він широко використовується в бездротових стандартах, таких як Wi-Fi, LTE та 5G, для ефективної передачі даних у бездротових мережах. Цей метод також використовується у багатьох пропрієтарних технологіях зв’язку з дронами таких як Ocusync, та багатьма ентузіастами разом з протоколом MavLink.

Ці цифрові методи модуляції є лише декількома з багатьох наявних варіантів. Кожен з них має свої переваги та обмеження, і їх вибір залежить від конкретного застосування та умов каналу зв'язку.

MavLink:

MavLink є відкритим протоколом зв'язку для безпілотних повітряних апаратів (БПЛА) і дронів. Він забезпечує передачу даних між дроном і земними станціями, такими як контролери пульта дистанційного керування або комп'ютери. MavLink побудований на базі серіалізованого протоколу, що дозволяє передавати повідомлення у вигляді пакетів даних. Він підтримує різноманітні типи повідомлень, такі як керування польотом, статус дрона, датчики тощо. Цей протокол є популярним у спільноті розробників дронів та має велику кількість імплементацій.

OcuSync:

OcuSync є пропрієтарним цифровим протоколом зв'язку, розробленим компанією DJI для своїх дронів. Цей протокол забезпечує стабільне та надійне передавання відео та даних між дроном і контролером пульта дистанційного керування. Основною особливістю OcuSync є його здатність до автоматичного перемикання між різними частотними діапазонами та зменшення

втрат сигналу у високоінтерференційних середовищах. В результаті це забезпечує високу якість зображення та стабільну передачу даних навіть на великій відстані.

Зараз найбільш популярними дронами є дрони компанії DJI, тому має сенс розглянути протокол Ocusync детальніше. А конкретніше версію 2.0.

DJI OcuSync 2.0 використовує спеціальну комунікаційну схему на основі OFDM. DJI описує її як "SDR" (програмно-конфігуровані радіо), ймовірно, через те, що вона реалізована у програмному забезпеченні, що працює на власному ASIC (Sparrow або S1, також відомий як Pigeon).

Ця схема не базується на Wi-Fi або інших готових системах зв'язку, але вона має деякі спільні риси з LTE. Ймовірно, хтось ознайомився з фізичною специфікацією LTE і використав її як "добрі практики". Проте, подібність закінчується тут, тому немає сенсу намагатися використовувати конкретні особливості LTE у контексті DJI OcuSync 2.0.

Пакети можуть становити 20 МГц, 10 МГц, 3 МГц, 1,4 МГц , а там 1,4 МГц-CA (ймовірно, для зміни каналів передачі при високій завантаженості каналів)

Модуляція OFDM використовується для всіх пакетів; Окупований пропускна здатність слабко нижчий, ніж виділена пропускна здатність, наприклад, 20 МГц використовує 1201 підносії з 15 кГц кожен, так ~ 18 МГц окупованої пропускної здатності.

Тривалість символів - 15 кГц, плюс циклічний префікс (CP). Під час передискретизації переходить до довжини степеня двох на зразок, тому, наприклад, 20 МГц може бути переплаченим до 30,72 МГц (= 2048 * 15000 кГц). Через CP чистий символ швидкості нижча за 15 кГц. З розміром FFT 2048 використовуються лише середні 1201 підносії (для 20 МГц).

Довжина CP для 20 МГц становить 144 (для 20 МГц), 72 (для 10 МГц) тощо. Деякі символи, зокрема перший, останній та середній для звичайних пакетів DL (структура символу залежить від типу даних), мають довший CP (144+16 для 20 МГц, 72+8 для 10 МГц).

Пакети можуть бути спрямовані вниз (від дрона до RC), вгору (від RC до дрона) та транслюватися (Drone-ID). Вони всі використовують OFDM, але з різною пропускною здатністю, а сигнал догори використовує технологію зміну каналів.[1]

Також в ході роботи було помічено що цей протокол транслює сигнал по багатьом каналам одночасно, було помічено 3 різних сигнала на різних частотах. Також була отримана інформація про те що цей протокол може працювати як на 2.4 ГГц так і на 5.8, але не може змінювати діапазон коли дрон здійснює політ.

Атаки на протоколи цифрового зв'язку з дронами можуть включати наступні способи:

– Деніал сервісу (Denial of Service, DoS): Ця атака полягає в перевантаженні мережі або системи дрона шкідливим трафіком, що призводить до відмови в обслуговуванні. Це може призвести до втрати зв'язку та недоступності дрона.

– Вторгнення в мережу (Network Intrusion): Ця атака спрямована на незаконне отримання доступу до мережі дрона для перехоплення або зміни передачі даних. Наприклад, зловмисник може отримати несанкціонований доступ до живого відеопотоку з камери дрона або перехопити його команди управління.

– Підробка пакетів (Packet Spoofing): Ця атака полягає відправці підроблених пакетів даних з метою зловживання або зміни даних, що

[1] https://github.com/tmbinc/random/tree/master/dji/ocusync2

передаються між дроном і контролером. Це може призвести до некоректної реакції дрона на команди або недостовірної інформації про стан дрона.

– Розкриття інформації (Information Disclosure): Ця атака спрямована на отримання конфіденційної інформації, такої як паролі, сертифікати або інші важливі дані, які використовуються для зв'язку з дроном. Зловмисники можуть використовувати отриману інформацію для несанкціонованого доступу до системи дрона.

– Перехоплення і відтворення (Interception and Replay): Ця атака полягає в перехопленні команд або даних, переданих між дроном і контролером, і їх повторенні зловмисником. Це може призвести до несанкціонованого управління дроном або виконання небажаних дій.

Для імплементації кожної з цих атак потрібне попереднє володіння інформацію про виробника дрона, його інтерфейсу зв'язку, формат повідомлень що використовує його протокол та канали роботи.

Атаки які не потребують попередньої інформації,такі як створення інтерференції, є дуже неефективними проти цифрового сигналу сучасних дронів. Для реалізації подібної атаки потрібно дуже дороге та потужне обладнання, яке здатне забезпечити 60 МГц або більше пропускної здатності на трансляцію. Також така атака може створювати проблеми в роботі засобів працюючих на діапазоні 2.4 ГГц, тому використання таких атак сильно обмежене.

Для ідентифікації дрона та отримання інформації для атаки можно використати декілька способів. Наприклад Drone ID.

Drone ID, або ідентифікатор дрона, це унікальний код, який присвоюється безпілотному літальному апарату. Він дозволяє розрізняти один дрон від іншого і є важливою складовою систем управління дронами та безпеки повітряного простору.

Кожен Drone ID може містити різні види інформації, залежно від вимог та правил регулювання. Зазвичай він включає унікальний ідентифікатор, що може бути числовим або алфавітно-числовим кодом. Цей ідентифікатор може бути призначений окремо для кожного дрона або виділений з певного діапазону.

Також, Drone ID може містити інформацію про власника дрона, таку як ім'я та контактні дані. Це дозволяє ідентифікувати та зв'язатися з власником у разі потреби.

Дослідження показали що трансляція цієї інформації немає шифрування[2], тому ця інформація може бути використана для отримання інформації що необхідна для атаки.

Також можна використати feature detection. Це може включати виявлення амплітудних піків, частотних компонент, часових шаблонів, змін у формі сигналу, зв'язків між різними компонентами сигналу та інші розпізнавальні особливості.

Feature detection у сигналах може мати різноманітні застосування, включаючи обробку сигналів, розпізнавання шаблонів, виявлення сигналів в шумі, аналіз спектра та інше. За допомогою алгоритмів feature detection можна виділити інформаційно значущі складові сигналу та використовувати їх для подальшого аналізу, класифікації або прийняття рішень.

Одним з відомих методів feature detection у сигналах є використання фільтрів, алгоритмів кореляції, спектрального аналізу, машинного навчання та інших технік. Ці методи дозволяють виявляти та виділяти специфічні особливості в сигналі, які можуть бути корисними для подальшого аналізу та обробки.

---

[2] https://github.com/proto17/dji_droneid

Дослідження у галузі feature detection у сигналах включають розробку нових алгоритмів, покращення ефективності виявлення, використання глибокого навчання та інших інноваційних підходів. Ці дослідження допомагають розширити можливості аналізу сигналів, розпізнавання та використання інформації, що міститься в сигналах для різноманітних застосувань.

Використання цих технік допоможе отримати інформацію необхідну для ідентифікації дрона та необхідного способу атаки.

3 Реалізація

Під час аналізу предметної області ми зіткнулися з проблемами для реалізації даного проекту. По-перше ціна та наявність обладнання, потужності якого вистачило би для його реалізації цього проекту у повній мірі. По-друге малий об’єм інформації за цією або суміжних темах. По-третє повна відсутність документації до протоколу Ocusync 2.0, що є основною ціллю даного проекту.

Тому був реалізований базовий алгоритм детекції сигналу та атаки на нього.

Для виконання цієї задачі, існує кілька мов програмування та технологій, які можна використовувати. Основний вибір залежить від конкретних потреб, доступності інструментів та знань програміста. Ось декілька популярних варіантів:

– Python: Python є однією з найпоширеніших мов програмування для наукових обчислень та обробки сигналів. Він має багатий екосистему бібліотек, таких як NumPy, SciPy, Pandas та Matplotlib, які забезпечують потужні функції обробки сигналів та аналізу даних.

– MATLAB: MATLAB є популярним середовищем для чисельних обчислень та сигнального аналізу. Він має багатий набір інструментів та функцій, спеціально розроблених для обробки сигналів. MATLAB дозволяє легко виконувати операції з сигналами, використовувати алгоритми обробки сигналів та візуалізувати результати.

– C/C++: Якщо швидкодія є критичним фактором, мови програмування C або C++ можуть бути вибором. Вони надають близьке до металу програмування та дозволяють ефективно виконувати обчислення на вбудованих системах або вимогливих за ресурсами середовищах.

– TensorFlow та PyTorch: Якщо ви плануєте використовувати глибоке навчання для задачі feature detection, фреймворки машинного навчання, такі як TensorFlow або PyTorch, можуть бути корисними. Вони надають

гнучкість та потужність для розробки та навчання моделей глибокого навчання для обробки сигналів.

Крім цього, існує також ряд спеціалізованих бібліотек та інструментів, які можуть бути використані для конкретних завдань детекції сигналів, таких як OpenCV, SciPy, GNU Radio тощо.

Вибір мови програмування для використання для виконання цього завдання у більшості спирався на бажання у подальшому розробити компактний та енергоефективний прилад що виключає Python, тож була використана мова C. Matlab також для цієї цілі не придатний, але також вимагає дорогої ліцензії. Але треба зазначити що проект dji-drone_id використовує Matlab. Також важливо що бібліотека libhackrf що використовується для розробки програмного забезпечення для SDR яке ми маємо використовує C.

Також у проекті використовується WiFi адаптер тому розглянемо бібліотеки які дають можливість з ним працювати.

У мові C є декілька бібліотек, які можна використовувати для керування Wi-Fi адаптером. Ось кілька популярних бібліотек для цього:

– libnl: Це бібліотека, яка надає API для керування мережевими інтерфейсами в Linux. Вона містить функції для налаштування Wi-Fi адаптера, створення та налаштування мережевих інтерфейсів, налаштування мережевих параметрів і багато іншого.

– wpa_supplicant: Це програма, яка забезпечує реалізацію клієнта Wi-Fi для систем Linux. Она також включає бібліотеку libwpa_supplicant, яку можна використовувати власне для керування Wi-Fi адаптером. Вона дозволяє підключатися до мереж Wi-Fi, налаштовувати параметри підключення і отримувати інформацію про стан мережі.

– libiw: Ця бібліотека надає API для роботи з Wi-Fi адаптерами в Linux. Вона дозволяє отримувати інформацію про наявні мережі Wi-Fi,

налаштовувати параметри підключення, здійснювати пошук нових мереж і багато іншого.

Було розглянуто лише бібліотеки на Linux, тому що ця операційна система краще підходить для реалізації портативного приладу, та тому що інші операційні системи не можуть запровадити той же контроль над адаптером. Для реалізації було вибрано libnl, через те що вона є частиною основної частини системи, та замінило собою libiw, тому використання libiw не є доцільним. Також не є доцільним використання wpa_supplicant, через те що на багатьох системах його не встановлено

Для виконання роботи було використано Hackrf SDR та Netgear A6210 WiFi адаптер

Однією з основних проблем детекції та підбору атаки дрона є загруженість каналів у діапазоні 2.4 ГГц, зокрема сигналами Wi-Fi. Це може призводити до перешкод у комунікації та погіршення продуктивності системи. І саме тому важливо мати ефективну систему відсіювання подібних сигналів.

Існує декілька підходів до вирішення цієї проблеми. Один з них полягає в використанні спеціального - Wi-Fi адаптера, який може майже миттєво надати інформацію про Wi-Fi сигнали поряд. Цей адаптер може бути підключений до комп'ютера і разом з розробленим програмним забезпеченням визначати наявність та інтенсивність подібних сигналів, а також канали на

Програмне забезпечення, що працює з Wi-Fi адаптером, проводить сканування навколишнього спектра для виявлення наявності сигналів Wi-Fi що можуть перешкоджати подальшому аналізу.За допомогою цих даних можна встановити, які канали є зайнятими сильними сигналами Wi-Fi, і виключити їх з подальшого опрацювання.

Такий підхід дозволяє ефективно відсіювати сигнали Wi-Fi та інші джерела перешкод, забезпечуючи швидшу детекцію та ідентифікацію сигналу дрона.

Цей підхід є ефективним та швидким у порівнянні з програмним відсіюванням сигналів, оскільки використовує спеціалізований апаратний засіб - Wi-Fi адаптер, який має вбудовані функції аналізу сигналів. Завдяки цьому система може швидко реагувати на зміни в спектрі сигналів та забезпечувати ефективну детекцію.

Також це уможливлює використання Deauthentication атаки проти дронів що використовують WiFi для зв’язку.

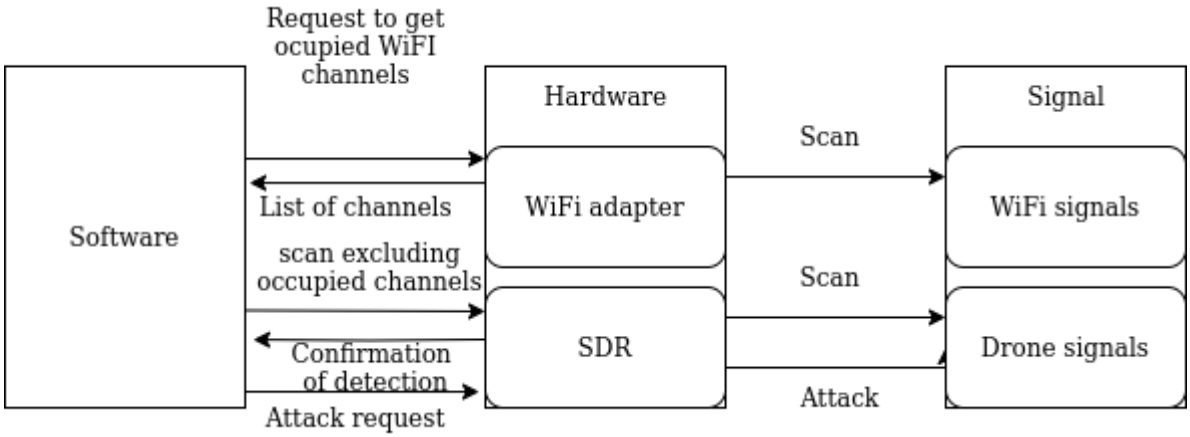


Рисунок 3 - діаграма роботи засобу

Виділення цього сигналу також уможливлює подальшого використання більш точних алгоритмів ідентифікації та reverse engineering для аналізу та розробки нових способів атак.

На жаль на даний момент реалізована лише атака без попередньої інформації, через нестачу даних про специфіку протоколу.

Висновки

Тема виявлення, ідентифікації та подавлення канала зв’язку є дуже актуальною сьогодні, через велику кількість фактів неправомірного використання дронів. Тому робота є доцільною у цьому напрямі.

В цій роботі було оглянено та проаналізовано декілька актуальних протоколів що використовують дрони зі споживацького ринку такі як

– GPS
– WiFi
– Аналоговий сигнал
– Цифровий сигнал

Було також проаналізовано та протестовано різні види атак та можливості виконання їх за допомогою SDR та інших апаратних засобів.

Результатом роботи став додаток що реалізує можливість ідентифікації сигналу як сигнал дрона та атаки його. В ході поточної роботи додаток був розроблений та протестований, також був реалізовані рекомендації з використання додатку та обладнання для виконання більш комплексних задач.

Щодо модифікації додатку, потрібно реалізувати більш точні алгоритми ідентифікації дрона, також треба більш детально дослідити протоколи цифрового зв’язку для реалізації точної ідентифікації самого дрона, його протоколу зв'язку та атаку необхідну для виведення його з експлуатації.

Список використаних джерел

[1]https://github.com/tmbinc/random/tree/master/dji/ocusync2
[2]https://github.com/proto17/dji_droneid

Згадані джерела

GPS Spoofing Detection Using a Software-Defined Radio" (2017) A. M. Salem A. H. Zaher

"A Comprehensive Analysis of UAV Wireless Communications: Physical Layer Vulnerabilities and Security Solutions" (2020) Xiaofang Sun Derrick Wing Kwan Ng Zhiguo Ding Yanqing Xu

Knocking my neighbors kids cruddy drone offline (Defcon 23) Robinson and Mitchell