COMPARATIVE ANALYSIS OF HACKRF ONE AND YARD STICK ONE IN THE STUDY OF SUB-GHZ WIRELESS COMMUNICATIONS*

DIMITAR N. GRESHKOV, ZDRAVKO Y. KUZMANOV

ABSTRACT: *This report presents a comparative analysis of the HackRF One and YARD Stick One in the context of an experimental study on sub-GHz wireless communications. It examines their architecture, operating principles, software, and capabilities regarding the interception, analysis, replay, and jamming of wireless systems operating in the 433 MHz band. The results highlight the differences between a flexible SDR platform providing access to I/Q data and a specialized RF device designed for digital sub-GHz communications.*

KEYWORDS: *HackRF One, YARD Stick One, Sub-GHz communications, Software Defined Radio (SDR), I/Q data, GNU Radio, RfCat, RF signal analysis*

DOI: https://doi.org/10.46687/MT26DNG

СРАВНИТЕЛЕН АНАЛИЗ НА HACKRF ONE И YARD STICK ONE ПРИ ИЗСЛЕДВАНЕ НА СУБГИГАХЕРЦОВИ БЕЗЖИЧНИ КОМУНИКАЦИИ

ДИМИТЪР Н. ГРЕШКОВ, ЗДРАВКО Ю. КУЗМАНОВ

АБСТРАКТ: *В настоящия доклад е представен сравнителен анализ на HackRF One и YARD Stick One при експериментално изследване на субгигахерцови безжични комуникации. Разгледани са техните архитектура, принцип на работа, използван софтуер и възможности за прихващане, анализ, възпроизвеждане и създаване на смущения при работа с безжична система в диапазона 433 MHz. Получените резултати показват различията между гъвкава SDR платформа, осигуряваща достъп до I/Q данни, и специализирано радиочестотно устройство, предназначено за работа с цифрови субгигахерцови комуникации.*

1 Въведение

Субгигахерцовите безжични комуникации намират широко приложение в системи за дистанционно управление, контрол на достъп, сигнализация, сензорни системи, автоматизация и различни устройства от типа Internet of Things. Използването на честоти под 1 GHz е свързано с редица практически предимства, включително сравнително добри условия за разпространение на радиосигнала и възможност за изграждане на компактни и нискоконсумиращи устройства.

Нарастващото използване на безжични технологии води и до необходимост от разработване на подходи за тяхното изследване и оценка на сигурността. При радиокомуникационните системи информацията се предава през общодостъпна физическа среда и може да бъде наблюдавана с подходящо радиочестотно оборудване. За разлика от кабелните комуникации, при които физическият достъп до линията може да бъде ограничен, радиосигналът се разпространява в пространството и неговото прихващане не изисква физическо свързване към комуникационния канал.

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

В последните години Software Defined Radio (SDR) платформите се превърнаха в широко използван инструмент за изследване на радиокомуникации. При SDR значителна част от обработката на сигнала се реализира чрез софтуер, което позволява една и съща хардуерна платформа да бъде използвана за различни честоти, модулации и комуникационни протоколи. HackRF One е пример за широколентова SDR платформа, която може да приема и предава сигнали в диапазона от 1 MHz до 6 GHz и предоставя достъп до I/Q семпли.

Паралелно с широколентовите SDR устройства съществуват и специализирани радиочестотни инструменти, предназначени за конкретни честотни диапазони и типове комуникации. YARD Stick One е такъв инструмент, разработен за работа с цифрови безжични системи под 1 GHz. Той използва радиотрансивър CC1111 и поддържа редица модулации, сред които ASK, OOK, GFSK, 2-FSK, 4-FSK и MSK.

Целта на настоящия доклад е да бъде извършен сравнителен анализ на HackRF One и YARD Stick One при изследване на субгигахерцови безжични комуникации. За целта са разгледани архитектурата и основните характеристики на двете устройства, използваният софтуер и нивото на достъп до приеманите радиосигнали. На практическо ниво са разгледани експерименти по прихващане и анализ на сигнали, определяне на параметри на комуникацията, възпроизвеждане на прихванати сигнали и изследване на влиянието на смущения.

Основната задача на сравнението е да се установи как различната архитектура на двете устройства влияе върху възможностите им за анализ и какъв тип задачи са подходящи за всяко от тях.

2 Субгигахерцови безжични комуникации и средства за тяхното изследване

2.1. Особености на субгигахерцовите комуникации

В областта на субгигахерцовите безжични комуникации попадат различни приложения, включително системи за дистанционно управление, безжични сензори, алармени системи, устройства за контрол на достъп и различни IoT устройства.

Сред широко използваните диапазони са тези около 433 MHz, 868 MHz и 915 MHz, като конкретното използване зависи от регионалните регулации и приложението. При системите за кратък обхват честотният диапазон около 433 MHz е особено разпространен при нискоскоростни устройства за дистанционно управление.

Една от особеностите на субгигахерцовите комуникации е сравнително голямата дължина на вълната в сравнение с микровълновите диапазони. Това позволява при определени условия радиосигналът да се разпространява на значителни разстояния и да бъде по-малко чувствителен към някои препятствия. Реалният обхват обаче зависи от множество фактори – предавателна мощност, чувствителност на приемника, антени, препятствия, смущения и конкретната среда.

От гледна точка на сигурността особеностите на физическия слой са важни, тъй като радиосигналът може да бъде прихванат без директна физическа връзка с устройството. Това създава възможност за пасивно наблюдение на комуникацията, записване на сигналите и последващото им анализиране.

При по-простите системи могат да се използват ASK и OOK, при които цифровата информация е представена чрез промени в амплитудата или наличието на носещия сигнал.

Други системи използват FSK и сродни схеми, които представят информацията чрез промяна на честотата.

Изборът на модулация оказва влияние върху начина, по който сигналът може да бъде наблюдаван и обработван. За изследователя обаче е необходимо да се разграничат характеристиките на физическия сигнал от структурата на протокола. Модулацията определя начина на предаване на информацията по радиоканала, но не представлява сама по себе си механизъм за сигурност.

2.2. Software Defined Radio (SDR)

Софтуерно-дефинираното радио представлява подход, при който част от традиционните хардуерни функции на радиосистемата се реализират чрез софтуер. Вместо всяка функция да бъде фиксирана в специализиран хардуер, цифровият сигнал може да бъде подаван към програмна среда, в която да бъде филтриран, демодулиран, визуализиран и анализиран.

В приемен режим SDR устройството приема радиосигнала и го преобразува в цифрови семпли. При системи, работещи с I/Q представяне, всеки комплексен семпъл се състои от две компоненти – In-phase (I) и Quadrature (Q). Тези компоненти позволяват да се запази информация за амплитудата и фазата на сигнала и са основа за последваща цифрова обработка. GNU Radio например използва комплексни I/Q семпли при работа с SDR системи.

Едно от основните предимства на SDR е гъвкавостта. При промяна на изследваната комуникационна система често не е необходимо да бъде сменен хардуерът. Вместо това могат да бъдат променени честотата, честотната лента, филтрите, усилването или алгоритмите за обработка.

Тази гъвкавост прави SDR особено подходящ за изследване на неизвестни или частично известни радиосистеми. Например при първоначален анализ може да бъде извършено спектрално наблюдение, след което да се определят приблизителната честота и широчината на сигнала. След това могат да бъдат изследвани времевата структура и модулацията.

Най-големият недостатък при тези устройства е тяхната цена. Те са много по-скъпи от стандартни RF трансивъри. Друг недостатък на този подход е по-голямата сложност. Изследователят трябва да разбира както основните принципи на радиокомуникациите, така и начина на работа на използвания софтуер. При някои задачи е необходимо създаването на сигнални схеми и настройване на множество параметри.

2.3. Специализирани радиочестотни устройства

За разлика от широколентовите SDR системи, специализираните радиочестотни устройства са разработени за конкретен набор от честоти и комуникационни характеристики. Те обикновено предоставят по-високо ниво на абстракция и позволяват директно задаване на параметри като честота, модулация и скорост на данните.

YARD Stick One е пример за подобна специализирана платформа. Той е проектиран за цифрови безжични системи под 1 GHz и използва CC1111 радиотрансивър. Официалните работни диапазони са 300-348 MHz, 391-464 MHz и 782-928 MHz. Поддържат се ASK, OOK, GFSK, 2-FSK, 4-FSK и MSK, а максималната посочена скорост на данните е до 500 Kbps.

Тази специализация има както предимства, така и ограничения. От една страна, устройството е удобно за работа с нискоскоростни цифрови радиосистеми и не изисква изграждане на сложна SDR обработка за всяка основна операция. От друга страна, достъпът

до суровата форма на радиосигнала е по-ограничен в сравнение с широколентов SDR. Това също прави пресъздаването на прихванатия сигнал значително по-трудно.

Следователно изборът между SDR платформа и специализиран радиочестотен инструмент зависи от конкретната задача. При спектрален анализ и изследване на неизвестен сигнал SDR предоставя по-голяма гъвкавост. При работа с вече известен тип цифрова комуникация специализираният инструмент може да осигури по-бърз и удобен начин за експериментиране.

3 HackRF One

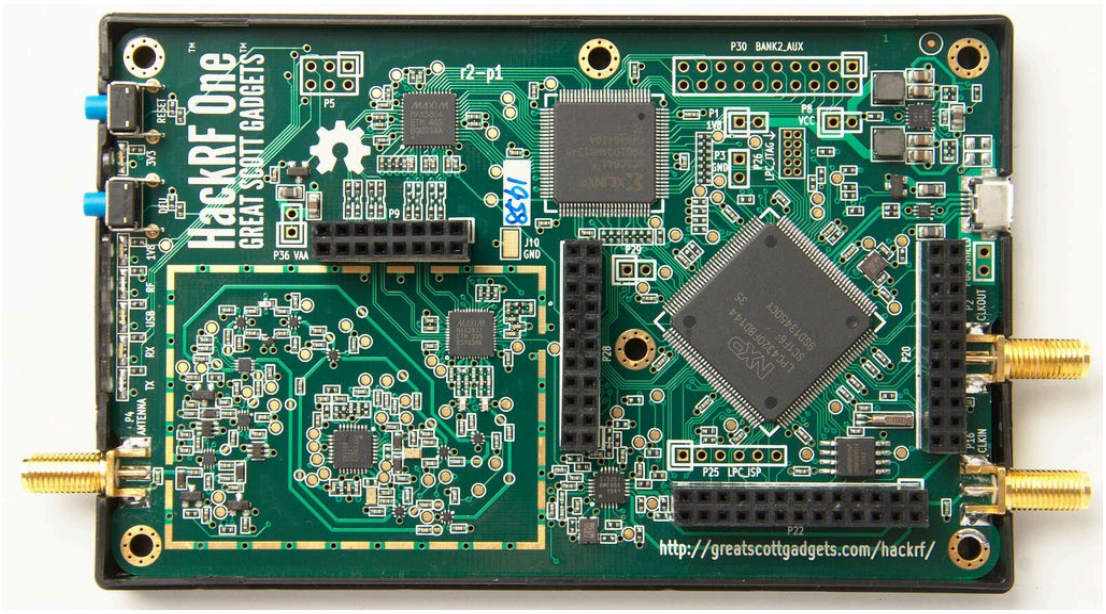
3.1. Архитектура и основни характеристики

HackRF One е широколентова SDR платформа, предназначена за приемане и предаване на радиосигнали. Устройството работи в диапазона от 1 MHz до 6 GHz, използва half-duplex режим и поддържа до 20 милиона семпъла в секунда. I/Q семплите са с 8-битова резолюция.

Хардуерът разполага със SMA конектор за антена, USB интерфейс за връзка с компютър и възможност за софтуерно управление на усилването и базовия филтър. Устройството може да бъде използвано както за приемане, така и за предаване, което го прави подходящо за контролирани експерименти с радиосигнали.

Широкият честотен диапазон е едно от основните предимства на HackRF One. Едно устройство може да бъде използвано за изследване на комуникации в различни части на радиочестотния спектър, без необходимост от специализиран хардуер за всяка отделна честота.

При изследване на субгигахерцови комуникации това позволява например наблюдение на системи около 433 MHz, 868 MHz и други подходящи честоти. Важно е при предаване да се спазват приложимите регулаторни ограничения, тъй като HackRF One е тестово оборудване и самото устройство не гарантира съответствие с изискванията за радиопредаване.



Фиг. 1. HackRF One

3.2. Работа с I/Q данни

Основна характеристика, която отличава HackRF One от YARD Stick One, е възможността за работа със сурови I/Q семпли.

При цифровото представяне на комплексния сигнал I компонентата представя една от ортогоналните компоненти на сигнала, а Q компонентата – другата. Комбинирани заедно, те предоставят информация, която може да бъде използвана за анализ на честотата, амплитудата, фазата и времевата структура на радиосигнала.

В GNU Radio комплексните семпли могат да бъдат обработвани от различни блокове. Те могат да бъдат визуализирани, филтрирани, записвани във файл или подавани към последваща обработка. GNU Radio описва комплексните семпли като последователности от I и Q компоненти, които могат да бъдат съхранявани и обработвани като цифрови данни. Това позволява един и същ сигнал да бъде анализиран многократно, без повторно задействане на оригиналния предавател.

Тази възможност е особено полезна при анализ на неизвестни сигнали. Изследователят може първоначално да наблюдава спектъра, след това да разгледа времевата форма и накрая да извърши по-подробен анализ на модулацията.

Тази особеност има голямо значение при експерименталното изследване, защото позволява отделяне на етапите на прихващане и анализ. Един сигнал може първо да бъде записан, след което да бъде разглеждан при различни настройки на филтри, визуализация и обработка.

3.3. Използван софтуер

За работа с HackRF One в лабораторната постановка е използван софтуерът GNU Radio. GNU Radio е програмна среда за цифрова обработка на сигнали, която позволява изграждането на сигнални вериги чрез свързване на отделни функционални блокове.

При експериментите входният сигнал от HackRF One се подава към блок за визуализация на спектъра. По този начин може да се наблюдава активността около зададената централна честота.

За изследването около 433 MHz е използвана честота на семплиране от 1 MHz. При задаване на централна честота около 433 MHz натискането на бутон на дистанционното управление води до появата на отчетлив сигнален пакет.

Към сигналната схема може да бъде добавен и File Sink, чрез който приеманите данни се записват за последващ анализ. За възпроизвеждане на записан сигнал се използва обратна структура, при която записаните данни се подават към предавателната част на HackRF One.

Този подход демонстрира основната концепция на SDR: хардуерът осигурява достъп до радиосигнала, а конкретната обработка се определя чрез софтуера.

4 YARD Stick One

4.1. Архитектура и основни характеристики

YARD Stick One (фиг. 2) е специализиран инструмент за работа с цифрови безжични сигнали под 1 GHz. За разлика от HackRF One, той не е широколентова SDR платформа, а използва специализиран радиотрансивър CC1111. Официалните работни честоти включват диапазоните 300-348 MHz, 391-464 MHz и 782-928 MHz.

Устройството работи в half-duplex режим и може както да приема, така и да предава цифрови радиосигнали. Поддържаните модулации включват ASK, OOK, GFSK, 2-FSK, 4-FSK и MSK.



Фиг. 2. YARD Stick One

YARD Stick One разполага със SMA конектор за антена и се свързва към компютър чрез USB. За разлика от HackRF One, устройството е тясно свързано с възможностите на CC1111. Това означава, че работата му е по-ограничена по отношение на честоти и обработка, но същевременно предоставя директен достъп до функции, предназначени за цифрови радиосистеми под 1 GHz.

4.2. CC1111 и начин на работа

CC1111 е интегриран радиотрансивър с микроконтролер, предназначен за нископотребителски субгигахерцови безжични приложения. Именно използването на този радиочип определя основните възможности на YARD Stick One.

При работа с устройството не се получава същият тип сурови I/Q данни, характерен за SDR платформите. Вместо това радиотрансивърът трябва да бъде конфигуриран с параметри като честота, модулация и други настройки на радиокомуникацията. Вместо да се получи самият радиосигнал, това устройство записва самата информация, която се изпраща през радиосредата (стига параметрите да са зададени правилно).

Този модел на работа е по-близък до начина, по който функционира готов радиомодул. Изследователят задава параметрите на радиочипа и получава цифров резултат от неговата обработка.

Това е съществено различие спрямо HackRF One. При HackRF анализът може да започне от самия физически сигнал и постепенно да премине към по-високо ниво. При YARD Stick One значителна част от обработката вече се извършва от радиочипа.

Тази архитектура е подходяща, когато типът на радиокомуникацията е приблизително известен. Например ако се предполага, че дадено устройство използва OOK около 433 MHz, YARD Stick One може да бъде конфигуриран директно за тази честота и модулация.

4.3. Използван софтуер

YARD Stick One се използва с RfCat – софтуерна среда, която позволява управление на CC1111 чрез Python интерфейс. Официалната информация за устройството посочва, че YARD Stick One се доставя с RfCat firmware, а самият RfCat позволява управление на радиотрансивъра от интерактивна Python среда или от собствена програма.

В лабораторната постановка RfCat се използва за настройване на работната честота и режима на модулация. След стартиране на интерактивната среда могат да бъдат зададени параметри за приемане и предаване.

При експериментите са изследвани различни комбинации от честота и модулация, включително 169 MHz ASK/OOK, 315 MHz ASK/OOK, 868 MHz ASK/OOK, 915 MHz ASK/OOK, 433 MHz GFSK и 433 MHz ASK/OOK.

Особено внимание е отделено на 433 MHz ASK/OOK, тъй като именно в този режим е наблюдавана комуникацията на изследваното дистанционно управление.

При използване на RfCat могат да бъдат изпълнявани функции за слушане и предаване. Това предоставя сравнително лесен начин за експериментиране с поддържаните радиорежими, без да е необходимо изграждането на сложна GNU Radio схема.

5 Експериментално изследване с HackRF One и YARD Stick One

5.1. Прихващане и анализ на сигнали

Първоначалното експериментално изследване е проведено с HackRF One. Целта е да бъде установена работната честота на изследваното дистанционно управление и да бъде анализирана структурата на предаваните сигнали.

При наблюдение около 433 MHz се установява, че при натискане на бутон се появява кратък сигнален пакет. При липса на натискане на бутон се наблюдава основно фонов радиошум.

Използването на GNU Radio позволява сигналът да бъде разгледан в честотната област. При няколко последователни предавания се наблюдава повторяемост на сигналната структура.

След това са направени записи на I/Q данните. Тези записи могат да бъдат използвани за последващ анализ и сравнение.

Предимството на HackRF в този етап е, че изследването може да започне без предварително точно познаване на структурата на комуникацията. Спектърът предоставя информация за това къде се намира сигналът и кога се активира.

След определяне на приблизителната честота е проведено изследване с YARD Stick One. Чрез RfCat са зададени 433 MHz и OOK като предполагаем режим на модулация. При приемане се наблюдава активност при натискане на бутон.

При YARD Stick One обаче получената информация е на по-високо ниво и не предоставя същия достъп до суровия физически сигнал, който е наличен при HackRF.

При допълнителни тестове са разгледани и други честоти и режими. Това показва практическата възможност на YARD Stick One да бъде използван за бързо тестване на различни конфигурации, но също така демонстрира зависимостта му от възможностите на CC1111.

5.2. Определяне на параметрите на комуникацията

При използване на HackRF One работната честота се определя чрез спектрално наблюдение. При изследваната система се установява честота около 433.92 MHz.

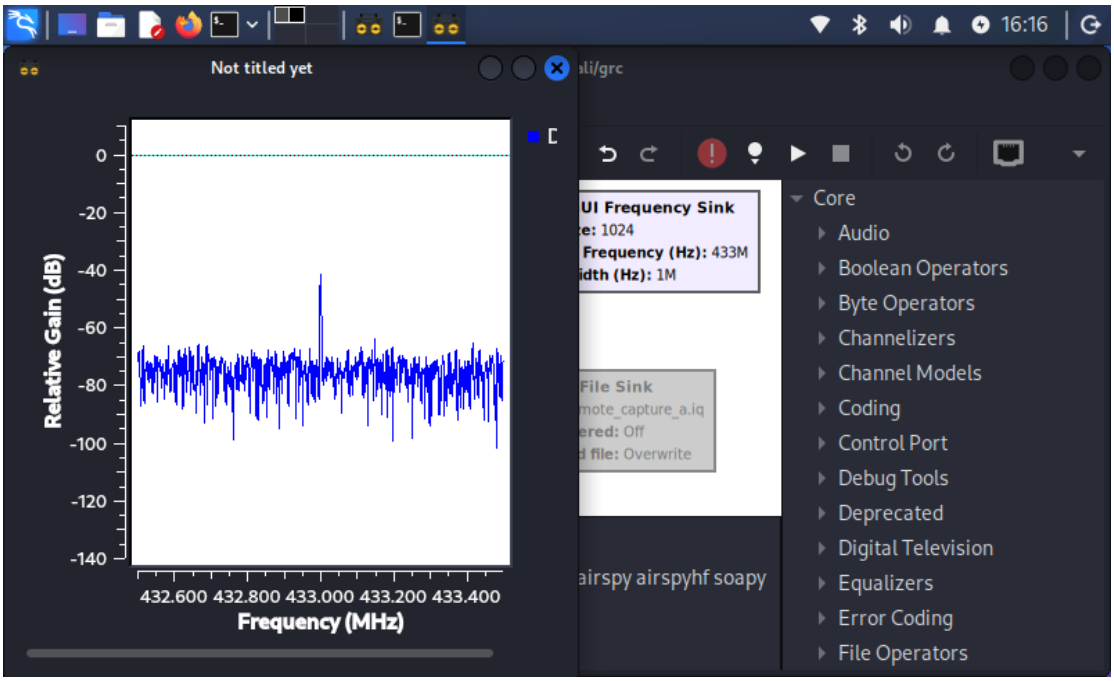
Чрез времевия анализ на сигнала се установява, че предаването се състои от кратки импулси и се активира при подаване на команда. Структурата е съвместима с OOK, при която наличието и отсъствието на носещ сигнал се използват за представяне на цифрова информация.

HackRF предоставя възможност за допълнителен анализ на честотната широчина и времевата структура. Това е особено полезно при неизвестни комуникации, защото параметрите могат да бъдат изведени експериментално.

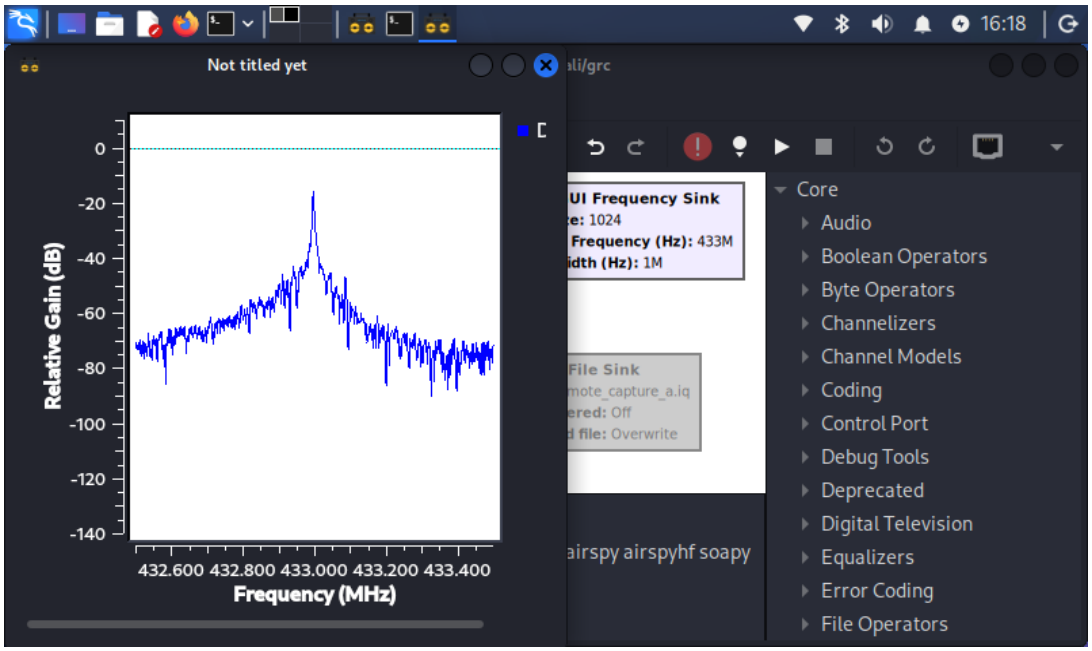
При YARD Stick One определянето на параметрите се извършва по различен начин. Вместо директно наблюдение на спектъра се задават предполагаемите параметри и се проверява дали устройството може да приема активността.

При експериментите е установено, че при 433 MHz ASK/OOK се получава структурирана информация, съответстваща на наблюдаваната комуникация. При други настройки, например 433 MHz GFSK, резултатът е различен.

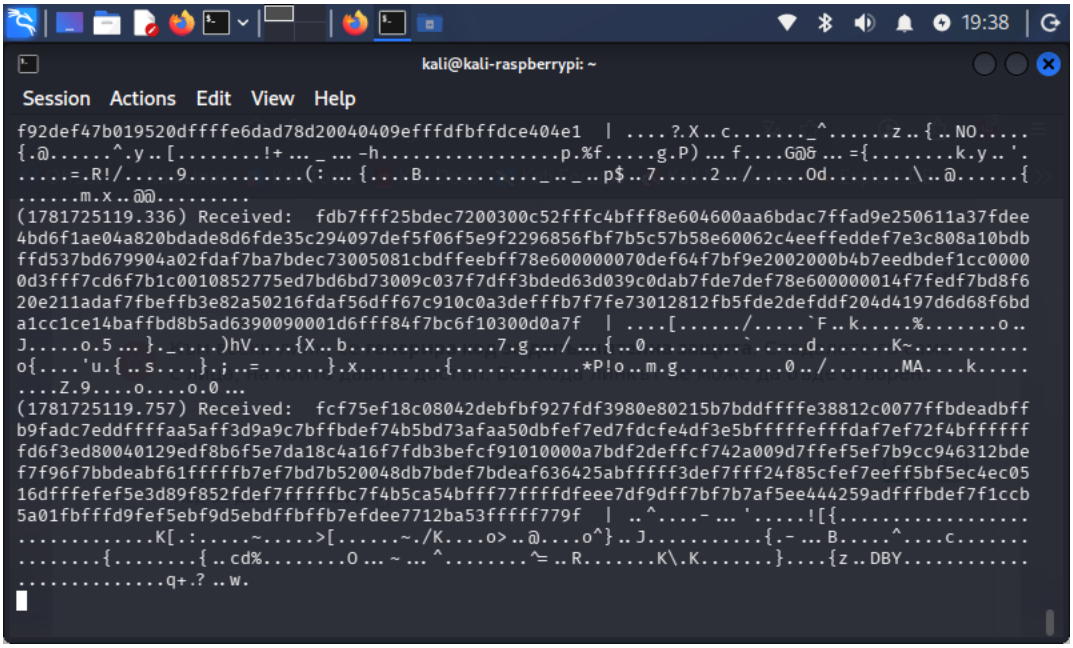
Това показва различния подход на двете устройства. HackRF е по-подходящ за откриване и характеризиране на неизвестен сигнал, докато YARD Stick One е по-подходящ за работа с вече определени параметри.



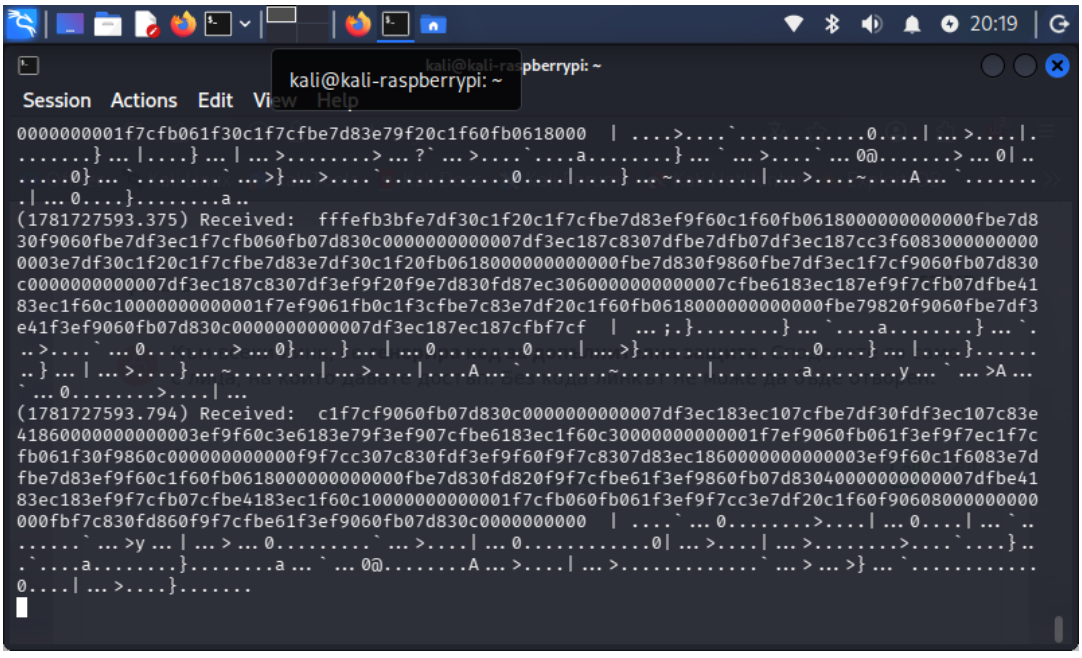
Фиг. 3. HackRF One / GNU Radio / нормално състояние



Фиг. 4. HackRF One / GNU Radio / получаване на сигнал



Фиг. 5. YARD Stick One / RfCat / нормално състояние



Фиг. 6. YARD Stick One / RfCat / получаване на сигнал

5.3. Възпроизвеждане на прихванати сигнали

След записването на сигналите с HackRF One е проведен експеримент за тяхното повторно предаване.

Записаните I/Q данни са използвани като вход на предавателната схема в GNU Radio. При повторното предаване успешно е извършена replay атака на устройство, използващо фиксиран код.

Този резултат показва, че HackRF може да бъде използван за възпроизвеждане на конкретен прихванат физически сигнал. Причината за това е възможността да се съхрани самата форма на радиосигнала, а не само извлечена от него цифрова последователност.

При YARD Stick One е направен различен подход. Чрез RfCat получените данни са представени като цифрова последователност, която може да бъде подадена към функция за предаване.

При директно предаване на прихванатата последователност устройството не реагира по същия начин, както при HackRF.

Това е един от най-съществените практически резултати от сравнението. При YARD Stick One получената информация не представлява непременно пълно описание на физическата форма на оригиналния RF сигнал. При OOK комуникациите времевата структура на импулсите е важна и простото представяне на резултата като поредица от байтове не винаги е достатъчно за точно възпроизвеждане на оригиналното предаване.

HackRF, от друга страна, запазва физическата форма на сигнала чрез I/Q семплите. Това позволява записаният сигнал да бъде възпроизведен с много по-малка промяна спрямо оригинала.

5.4. Създаване на смущения

Допълнителният експеримент има за цел да покаже възможностите на двете устройства при създаване и наблюдение на радиосмущения в контролирана лабораторна среда.

При HackRF One е използван шумов източник в GNU Radio, който се подава към предавателната част. При настройване около работната честота се създава допълнителна радиочестотна активност.

При нормални условия на експеримента изследваната система демонстрира надеждна работа на разстояние приблизително 25-30 m. При наличие на контролирано смущение около работната честота надеждният обхват е намален до приблизително 8-10 m.

Този експеримент демонстрира предимството на HackRF при задачи, при които е необходимо генериране на специфичен радиосигнал. Чрез GNU Radio може да бъде определен типът на сигнала и начинът, по който той се подава към предавателната част.

YARD Stick One също разполага с предавателни възможности, но възможностите му за генериране на произволен широколентов шум са по-ограничени. Устройството има значително по-малка мощност от HackRF One. Предназначено е преди всичко за работа с поддържаните цифрови модулации на CC1111, а не за свободно формиране на произволна I/Q форма.

При проведените експерименти не е установено сравнимо ефективно въздействие върху обхвата чрез YARD Stick One. Това показва практическата разлика между широколентовия SDR подход и специализирания радиотрансивър.

Експериментите със смущения са проведени в контролирана лабораторна среда. При реално предаване на радиосигнали трябва да бъдат спазвани приложимите национални и европейски изисквания за използване на радиочестотния спектър.

6 Сравнителен анализ на резултатите

6.1. Предимства и ограничения на HackRF One

Основното предимство на HackRF One е неговата гъвкавост. Широкият честотен диапазон от 1 MHz до 6 GHz позволява използването на едно устройство за изследване на множество различни радиосистеми. Поддържането на I/Q семпли позволява достъп до физическата форма на сигнала и последващата му цифрова обработка.

Това прави HackRF особено подходящ за първоначално изследване на неизвестни радиосигнали. Чрез спектрално наблюдение може да бъде установена честотата, след което да бъдат анализирани широчината, времевата структура и модулацията.

Друго важно предимство е възможността за запис на I/Q данни. Записаният сигнал може да бъде анализиран многократно и при подходяща конфигурация да бъде възпроизведен.

HackRF е подходящ и за експерименти, при които е необходимо генериране на различни видове сигнали. GNU Radio позволява изграждането на сложни сигнални вериги и промяна на параметрите без промяна на основния хардуер.

Основното ограничение, изключвайки високата цена, е сложността на работа. За пълното използване на възможностите на HackRF е необходимо разбиране на SDR концепциите, I/Q представянето, семплирането, филтрацията и цифровата обработка на сигнали. Създаването на подходяща GNU Radio схема също може да изисква повече време.

Допълнително ограничение е 8-битовата резолюция на I/Q семплите, която поставя ограничения върху динамичния диапазон в сравнение с някои по-нови и по-висок клас SDR системи. Това не пречи на използването му за голям брой практически експерименти, но е характеристика, която трябва да бъде отчетена при по-прецизни измервания.

6.2. Предимства и ограничения на YARD Stick One

Основното предимство на YARD Stick One е специализацията му. Устройството е разработено именно за цифрови безжични системи под 1 GHz и поддържа типични за тази област модулации.

Работата с RfCat позволява бързо задаване на честота и режим на модулация и извършване на приемане или предаване. Това намалява необходимостта от изграждане на сложна цифрова сигнална обработка.

YARD Stick One е особено удобен при експерименти, при които вече са известни основните параметри на комуникацията. Например при известна честота 433.92 MHz и предполагаема OOK модулация устройството може да бъде конфигурирано директно за съответната задача.

Друг плюс е компактността на устройството и сравнително простият начин на работа. RfCat предоставя програмируем интерфейс, чрез който радиотрансивърът може да бъде използван от Python. Официалният проект описва YARD Stick One именно като платформа, предназначена за RfCat.

Основното ограничение е по-ниското ниво на достъп до сигнала. За разлика от HackRF One, YARD Stick One не предоставя общ SDR интерфейс със сурови I/Q семпли. Анализът е ограничен от възможностите на CC1111 и поддържаните от него режими.

Това се проявява особено ясно при възпроизвеждането на прихванати OOK сигнали. Прихванатата цифрова информация не винаги съдържа достатъчно информация за точно възстановяване на оригиналната времева форма на RF сигнала. В резултат директното предаване на получените данни може да не доведе до успешна replay атака.

6.3. Сравнение на приложимостта им при различни задачи

Резултатите от експериментите показват, че HackRF One и YARD Stick One не трябва да се разглеждат като напълно взаимозаменяеми устройства.

При първоначално изследване на неизвестна комуникация HackRF One предоставя значително по-широки възможности. Чрез спектралното наблюдение може да бъде открита активността, а I/Q записът позволява сигналът да бъде запазен в оригиналната му цифрова форма.

При анализ на вече идентифицирана цифрова комуникация YARD Stick One може да бъде по-удобен. Ако са известни честотата, модулацията и приблизителните параметри, те могат директно да бъдат зададени чрез RfCat.

При подробен физически анализ HackRF има предимство поради достъпа до I/Q данни. Това позволява изследване на характеристиките на сигнала, които могат да бъдат загубени при по-високо ниво на обработка.

При стандартни операции по приемане и предаване на поддържани цифрови модулации YARD Stick One предлага по-специализиран подход. Неговият хардуер и софтуер са оптимизирани за работа с възможностите на CC1111, което опростява някои задачи.

При генериране на произволни или нестандартни радиосигнали HackRF отново има по-голяма гъвкавост. GNU Radio позволява сигналът да бъде изграден програмно от различни блокове и да бъде променян според експерименталната задача.

При създаване на смущения също се наблюдава разлика. HackRF позволява генериране на шумови и други сигнали чрез SDR обработка, докато YARD Stick One е ограничен от функционалността на радиотрансивъра CC1111.

От гледна точка на обучението двете устройства също предоставят различни възможности. Използването на съвременни технологични платформи в практически ориентирано обучение подпомага развитието на технически компетентности, умения за експериментиране и способност за решаване на практически задачи [8]. HackRF позволява по-добро изучаване на физическия слой на радиокомуникацията – спектър, семплиране, I/Q представяне и модулация. YARD Stick One от своя страна предоставя по-пряк начин за експериментиране с цифрови субгигахерцови комуникации и програмиране на радиотрансивър.

Следователно сравнението показва не толкова, че едното устройство е универсално по-добро от другото, а че те са предназначени за различни нива на анализ. HackRF One е по-гъвкав инструмент за изследване на самия радиосигнал, докато YARD Stick One е по-специализиран инструмент за работа с определен клас цифрови радиосистеми.

7 Заключение

В настоящия доклад е извършен сравнителен анализ на HackRF One и YARD Stick One при изследване на субгигахерцови безжични комуникации. Разгледани са техните архитектурни особености, начинът им на работа, използваната софтуерна среда и приложимостта им при различни експериментални задачи.

HackRF One представлява широколентова SDR платформа с работен диапазон от 1 MHz до 6 GHz, възможност за приемане и предаване и достъп до I/Q семпли. Тези характеристики го правят подходящ за спектрален анализ, изследване на неизвестни сигнали, запис на радиосигнали и тяхното последващо цифрово обработване.

YARD Stick One е специализиран субгигахерцов радиочестотен инструмент, базиран на CC1111. Той поддържа редица цифрови модулации и е предназначен за работа с радиосистеми под 1 GHz. Управлението му чрез RfCat позволява сравнително лесно задаване на основните параметри и извършване на приемане и предаване.

Проведеното експериментално изследване показва съществена разлика между двата подхода. При HackRF One сигналът може да бъде наблюдаван на физическо ниво, записан като I/Q данни и впоследствие обработван или възпроизвеждан. Това предоставя голяма свобода при анализа на неизвестни комуникации.

При YARD Stick One работата се извършва на по-високо ниво. Радиотрансивърът обработва сигнала според зададените настройки, а RfCat предоставя интерфейс за управление на тази функционалност. Този подход е по-ограничен, но е удобен при работа с вече известни честоти и поддържани модулации.

Експериментите с изследваната 433 MHz система показват, че HackRF One е по-подходящ за първоначално характеризиране на сигнала и за запазване на неговата физическа структура. YARD Stick One може успешно да се използва за приемане на цифрова комуникация, когато нейните основни параметри са предварително определени, но директното възпроизвеждане на прихванатите данни не винаги е достатъчно за точно възстановяване на оригиналния RF сигнал.

При експериментите със смущения също се установява разлика. HackRF One позволява програмно генериране на шумови сигнали чрез GNU Radio и предоставя по-голяма свобода при формирането на предаването. YARD Stick One е ограничен от възможностите на CC1111 и не е предназначен за същото ниво на произволна I/Q обработка.

В крайна сметка двата инструмента допълват по-скоро, отколкото заменят един друг. HackRF One е подходящ за широк спектър от задачи, свързани с наблюдение, запис и анализ на физическия радиосигнал, докато YARD Stick One предоставя специализиран и по-опростен подход към цифрови субгигахерцови комуникации.

Използването на двата инструмента в една лабораторна постановка позволява радиокомуникацията да бъде разглеждана от различни нива – от физическата форма на сигнала до параметрите на цифровия радиотрансивър. Това прави комбинирания подход подходящ за експериментално изследване на различни безжични системи и за оценка на техните технически характеристики и сигурност.

ЛИТЕРАТУРА:

[1] OFCOM IR 2030 - Licence Exempt Short Range Devices. https://www.ofcom.org.uk/siteassets/resources/documents/spectrum/interface-requirements/ir-2030.pdf

[2] Qinuo Electronics Co.,Ltd. "What is the difference between rolling code and fixed code remote?" https://www.qinuo.net/news/64.html

[3] Great Scott Gadgets – HackRF One. https://greatscottgadgets.com/hackrf/one/

[4] Great Scott Gadgets – YARD Stick One. https://greatscottgadgets.com/yardstickone/

[5] Youngblood, G. "A Software-Defined Radio for the Masses, Part 1". https://www.arrl.org/files/file/Technology/tis/info/pdf/020708qex013.pdfhttps://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.2117-0-201809-I!!PDF-E.pdf

[6] International Telecommunication Union. "Data format definition for exchanging stored I/Q data for the purpose of spectrum monitoring". https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.2117-0-201809-I!!PDF-E.pdf

[7] atlas0fd00m/rfcat: RfCat - swiss-army knife of ISM band radio. https://github.com/atlas0fd00m/rfcat

[8] Tasinov, T. Y. (2023). A Step Up – From 3D to 6D Printing. Possible and Future Applications of New Materials and Technologies in the Technology Education of Students. In: Innovation Models for Implementing Qualifications and Forming Competencies in the Educational System. Shumen: Konstantin Preslavsky University Press, pp. 286–293. ISBN 978-619-201-732-3.