ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 621.396.669

ПОДХОД К РЕАЛИЗАЦИИ ОБНАРУЖЕНИЯ ВНЕШНИХ ПРОГРАММНО-АППАРАТНЫХ ВОЗДЕЙСТВИЙ НА СИСТЕМУ СПУТНИКОВОЙ НАВИГАЦИИ

Белянов Кирилл Сергеевич
лаборант кафедры безопасности и информационных технологий

Рыжиков Сергей Сергеевич
доцент кафедры безопасности и информационных технологий

Агуреев Иван Александрович
заведующий учебной лабораторией кафедры безопасности и информационных технологий

Национальный исследовательский университет "МЭИ"
111250, Россия, г. Москва, Красноказарменная улица, дом 14
e-mail: universe@mpei.ac.ru

Аннотация

Одним из наиболее распространенных типов высокоточных систем позиционирования являются спутниковые радионавигационные системы. При этом они имеют ряд уязвимостей, в частности - возможность навязывания приемной аппаратуре потребителя ложных навигационных сигналов. Предлагается подход к контролю целостности навигационных измерений на основе анализа изменения значений псевдодальностей с помощью радиопеленгатора, реализованного с применением программно определяемой радиосистемы HackRF One.

Ключевые слова: системы спутниковой навигации, навигационная аппаратура потребителей, имитационные помехи.

AN APPROACH TO THE IMPLEMENTATION OF THE DETECTION OF EXTERNAL SOFTWARE AND HARDWARE INFLUENCES ON THE SATELLITE NAVIGATION SYSTEM

Kirill S. Beloyanov
Scientific assistent, Department of Security and Information Technology

Sergey S. Ryzhikov
Postdoctoral researcher, Department of Security and Information Technology
Ivan A. Agureev
Head of Educational Laboratory, Department of Security and Information Technology

National Research University "Moscow Power Engineering Institute"
Krasnokazarmennaya st.,14, Moscow, Russia, 111250
email: AgureevIA@mpei.ru

ABSTRACT

One of the most common types of high-precision positioning systems is satellite radio navigation systems. But they have a number of vulnerabilities, for example, the possibility of imposing false navigation signals at the consumer's receiving equipment. An approach to monitoring the integrity of navigation measurements based on the analysis of changes in pseudo-distance values using a radio direction finder implemented using the software-defined HackRF One radio system is suggested.

Keywords: satellite navigation systems, consumer navigation equipment, simulation interference.

Введение

Современное общество сложно представить без использования систем спутниковой навигации (Global Navigation Satellite System - GNSS), предназначенных для определения местоположения в пространстве различных наземных, водных и воздушных объектов. Основной принцип функционирования GNSS – использование искусственных спутников Земли в качестве точек отсчета для вычисления географических координат на основе тригонометрических соотношений. Зная точные расстояния, по крайней мере, до трех спутников, можно определить текущее местоположение. В настоящее время в мире, помимо глобальных навигационных спутниковых систем ГЛОНАСС (Россия) и GPS (США), работы по развертыванию GNSS BDS и ГАЛИЛЕО проводят Китай и страны Европейского союза. Япония и Индия разворачивают региональные навигационные спутниковые системы QZSS и IRNSS соответственно [1].

Принцип работы спутниковых систем навигации основан на измерении расстояния от антенны на объекте (координаты которого необходимо получить) до спутников, положение которых известно с большой точностью. Таблица положений всех спутников называется альманахом, которым должен располагать любой спутниковый приёмник до начала измерений. Каждый спутник передаёт в своём сигнале весь альманах. Таким образом, зная расстояния до нескольких спутников системы, с помощью обычных геометрических построений, на основе альманаха, можно вычислить положение объекта в пространстве.

Метод измерения расстояния от спутника до антенны приёмника основан на определённости скорости распространения радиоволн. Для осуществления возможности измерения времени распространения радиосигнала, каждый спутник навигационной системы излучает сигналы точного времени в составе своего сигнала, используя точно синхронизированные с системным временем атомные часы. При работе спутникового приёмника его часы синхронизируются с системным временем, и при дальнейшем приёме сигналов вычисляется задержка между временем излучения, содержащимся в самом сигнале, и временем приёма сигнала. Располагая этой информацией, навигационный

приёмник вычисляет координаты антенны. Дополнительно накапливая и обрабатывая эти данные за определённый промежуток времени, становится возможным вычислить такие параметры движения, как скорость (текущую, максимальную, среднюю), пройденный путь и т. д.

Между космическими (группировка космических аппаратов) и наземными (подсистема контроля и управления, а так же навигационная аппаратура потребителей) сегментами GNSS идет постоянный обмен данными. Управляющий наземный сегмент отслеживает изменение положения спутников, анализирует данные орбит, синхронизирует атомные часы. Пользовательский наземный сегмент принимает сообщения от спутников, в которых содержится информация (рис. 1) об орбитальных данных, таблица положений всех спутников (альманах), коррекцию системного времени и другие данные [1].

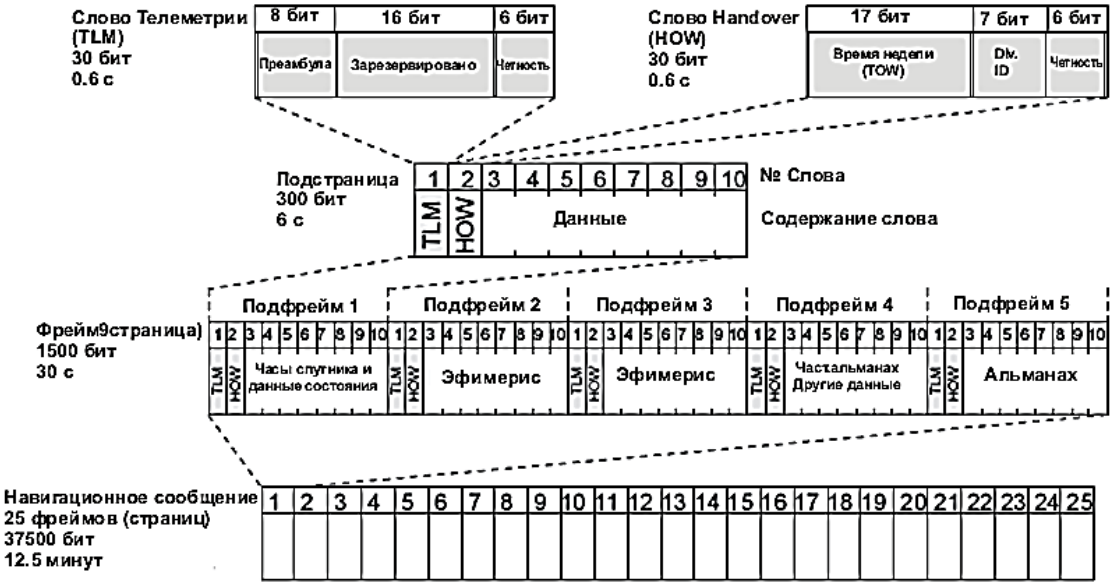

Рисунок 1. *Структура полного навигационного сообщения*

Приемники потребителей спутниковой информации путем математических вычислений полученных данных определяют свое точное местонахождение. Подмена или изменение передаваемой информации на приемники может привести к большой погрешности в вычислении реального местоположения.

Воздействия на навигационное оборудование

Перечень воздействий на системы навигационного оборудования очень велик, но можно выделить два наиболее часто используемых вида атак - блокирование сигнала и его подмену [2].

- «Энергетические» помехи (jamming) – радиопомехи, предназначенные для нарушения функционирования наземной аппаратуры потребителей информации GNSS путем подавления полезного информационного сигнала. К этому типу помех также следует отнести любые действия, направленные на нарушение функционирования самой GNSS, включая атаку на спутники и наземную инфраструктуру управления.

- «Имитационные» помехи (spoofing) – радиопомехи, предназначенные для передачи потребителю ложной информации путем формирования специальными источниками сигналов, аутентичных сигналам GNSS.

На практике проще и надежнее реализуются энергетические помехи. Однако любое воздействие такого рода на радиоаппаратуру легко распознается и позволяет, соответственно, учитывать наличие помехового воздействия при работе аппаратуры.

«Spoofing»-помехи представляются сегодня более опасными, так как их воздействие приводит к формированию ложной навигационной информации при отсутствии понимания о наличии помехового воздействия. Далее будут рассматриваться только данный вид помех.

Для проведения атаки, злоумышленник транслирует поддельный навигационный сигнал со схожими характеристиками, но с более высоким уровнем, чем истинный. Приемник автоматически отдает приоритет сигналам с лучшим качеством приема, и таким образом злоумышленник перехватывает управление над приемником навигационного сигнала и устройством, в котором он установлен.

На основе передаваемого ложного сигнала приемник вычисляет ошибочные координаты своего местоположения. Изменение местоположения происходит постепенно, чтобы устройство не включило режим блокировки. Получив контроль над устройством, злоумышленник может использовать его в своих интересах.

Контроль целостности навигационных измерений по уровню принимаемого сигнала может быть произведен следующими способами:

1. В заданном географическом районе производятся статистические измерения качества принимаемого сигнала. В случае если уровень сигнала превышает допустимый порог, система сигнализирует об ошибке.
2. Навигационным оборудованием отслеживается скорость изменения уровня сигнала на входе приемника. Если мощность сигнала увеличилась слишком сильно за короткий промежуток времени, система сигнализирует об ошибке.

Предлагается бюджетная аппаратная реализация устройства контроля целостности навигационных измерений, позволяющая получателю данной информации обнаружить подмену сигнала за счет анализа изменения значений псевдодальностей.

Порог определяется исходя из минимальной и максимальной скоростей изменения псевдодальности каждого видимого спутника в штатной ситуации (сигнал не подвергается подмене). Считается, что на сигнал происходит воздействие, если изменения в значениях псевдодальностей принимаемых сигналов не соответствуют следующему условию [2]:

$\min(\Delta p_i)\ p_i(n) < \max(\Delta p_i)$

где Δp_i - вектор изменений псевдодальностей i-го спутника без спуфинга,

$p_i(n)$ – значение псевдодальности i-го спутника в эпоху n.

Реализация подхода по обнаружению воздействия на навигационные системы

Наиболее вероятна ситуация, в которой излучение ложного сигнала GNSS атакующим будет происходить из одной точки в пространстве, при этом не важно, находится передатчик атакующего в прямой видимости от принимающей антенны или нет. Напротив, сигналы от настоящих космических аппаратов GNSS приходят на принимающую антенну с разных направлений. Опираясь на это допущение, можно сделать вывод, что внешнее преднамеренное воздействие на сигналы GNSS может быть эффективно зафиксировано, когда сразу несколько навигационных сигналов имеют одинаковое или очень близкое друг к другу направление прихода электромагнитной волны.

Приняв допущение, что излучение ложного сигнала GNSS злоумышленником наиболее вероятно будет происходить из одной точки в пространстве, в основу комплекса для обнаружения внешнего программно-аппаратного воздействия на сигналы спутниковой навигации может быть взята схема радиопеленгатора (рис. 2).

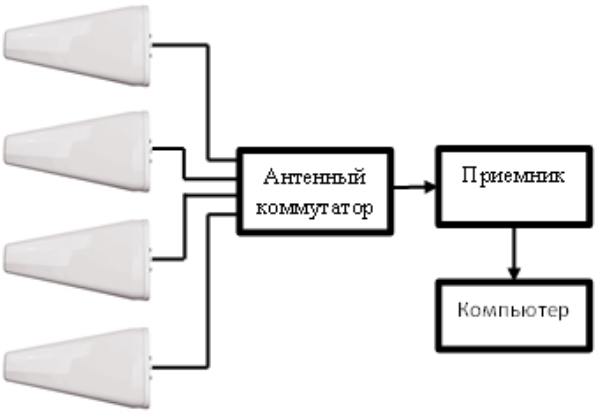

Рисунок 2. Структурная схема комплекса

В качестве приемного устройства выступает открытая аппаратная платформа, программно определяемая радиосистема (SDR) HackRF One, которая под управлением компьютера через антенный переключатель производит коммутацию входа приемника и отдельных элементов антенной системы.

Антенный коммутатор для программно-определяемой радиосистемы HackRF One был реализован на плате расширения Opera Cake, которая управляется программно по интерфейсу I2C и предоставляет возможность коммутировать вход трансивера с одним из 8 выходов антенного переключателя.

В качестве программного инструментария были выбраны визуальная среда GNU Radio Companion и библиотеки на языках программирования Python или C++ [3]. Цифровая обработка сигналов осуществляется одноплатным компьютером Orange Pi Prime, который поддерживает операционную систему GNU/Linux.

Цифровая обработка сигнала осуществляется в программной среде GNU Radio в соответствие с блок-схемой, представленной на рисунке 3.

При обработке сигнала последовательно реализуются следующие операции:

- извлечение измерений с каждого отдельного элемента антенной системы из общего потока данных;
- BPSK демодуляция;
- многофазная синхронизация;
- фазовая автоподстройка частоты;
- слепое уравнивание (CMA);
- визуализация расхождения фаз сигнала.

Для приема сигнала используется четыре элемента - слабонаправленных керамических ГЛОНАСС/GPS патч-антенны (рис.4).

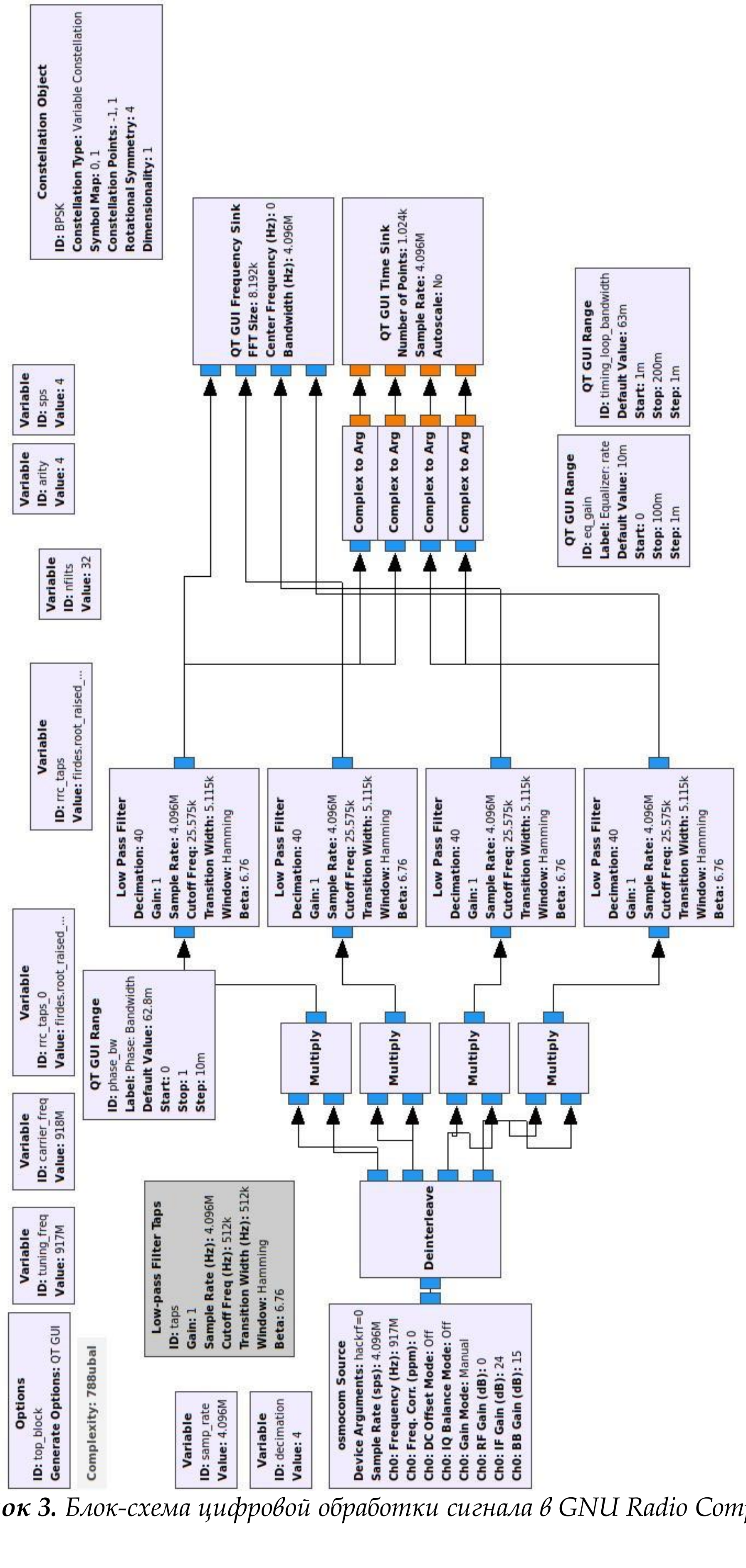

Рисунок 3. *Блок-схема цифровой обработки сигнала в GNU Radio Companion*

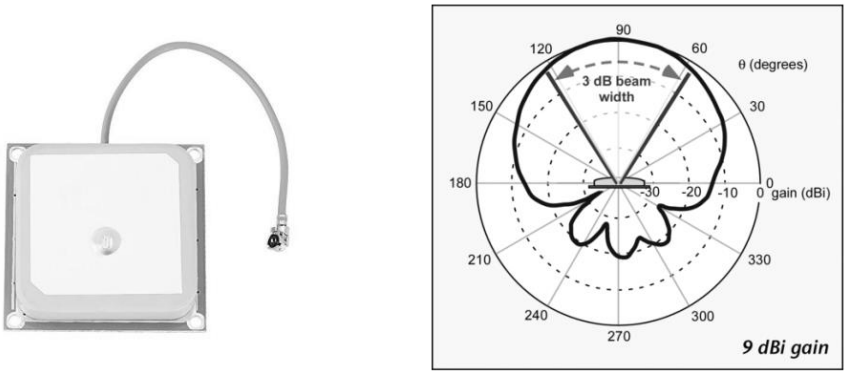

Рисунок 4. *Керамическая патч-антенна и ее диаграмма направленности в горизонтальной плоскости*

Прототип технического решения размещен в компактном пластиковом корпусе с габаритами 180х150х50мм (рис. 5).

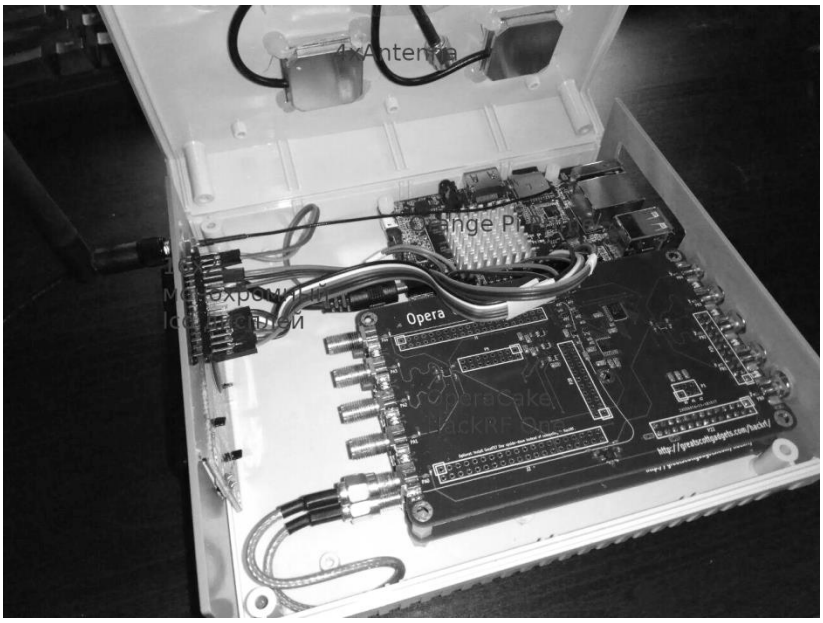

Рисунок 5. Прототип устройства по обнаружению воздействия на навигационные системы

В ходе испытаний устройства было отмечено негативное влияние на функциональные характеристики устройства следующих факторов:

- недостаточное электромагнитное экранирование радиочастотной части;
- низкий уровень сигнала на входе приемника;
- недостаточная чувствительность приемника.

Заключение

Для оценки потенциальных угроз искажения выбранных критических данных была спроектирована структурная схема макета. Осуществлен выбор компонентной базы для макетирования аппаратно-программного комплекса.

Была выбрана следующая связка технологических решений: HackRF One - приемник сигнала и Orange Pi Prime - система управления. Для приема сигнала использовались промышленно выпускаемые керамические патч-антенны.

Проведенная апробация показала приемлемую эффективность работы разработанного макета в лабораторных условиях.

В дальнейшем в качестве мер по улучшению производительности предполагается рассмотреть:

- возможность использования специальных защитных экранов от электромагнитного излучения на радиочастотной части приемника;
- использование малошумящих усилителей между антенной и приемником;
- использование активных GPS антенн;
- использование приемника с большим разрешением АЦП.

Список литературы

1. Структура навигационного сообщения ГЛОНАСС. Режим доступа: http://seaman-sea.ru/glonass/511-struktura-soobschenija.html (дата обращения: 25.10.2020).
2. Шепель В. И., Ергалиев Д. С., Тулегулов А. Д. Сравнительный анализ глобальных навигационных спутниковых систем // Труды Международного симпозиума «Надежность и качество», Том. 1, 2012, pp. 469-470. Режим доступа: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-globalnyh-navigatsionnyh-sputnikovyh-sistem (дата обращения: 24.09.2021).
3. Дао Х. К, Ступин Д. Д., Шевченко Р. А. Принципы обнаружения преднамеренных помех, воздействующих на аппаратуру потребителей спутниковых радионавигационных систем. Журнал радиоэлектроники [электронный журнал]. 2019. № 5. Режим доступа: http://jre.cplire.ru/jre/may19/14/text.pdf (дата обращения: 25.10.2020).
4. Opera Cake: надстройка RF-переключения для HackRF One. Режим доступа: https://github.com/mossmann/hackrf/tree/master/hardware/operacake (дата обращения: 05.04.2021).

References

1. The structure of the GLONASS navigation message. Access mode: http://seaman-sea.ru/glonass/511-struktura-soobschenija.html (date of access: 10/25/2020).
2. Shepel V. I., Ergaliev D. S., Tulegulov A. D. Comparative analysis of global navigation satellite systems // Proceedings of the International Symposium "Reliability and Quality", Vol. 1, 2012, pp. 469-470. Access mode: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-globalnyh-navigatsionnyh-sputnikovyh-sistem (date of access: 24.09.2021).
3. Dao H. K, Stupin D. D., Shevchenko R. A. Principles of detecting deliberate interference affecting the equipment of consumers of satellite radio navigation systems. Radio electronics journal [electronic journal]. 2019. No. 5. Access mode: http://jre.cplire.ru/jre/may19/14/text.pdf (date of access: 10/25/2020).
4. Opera Cake: RF Switching add-on for HackRF One. Access mode: https://github.com/mossmann/hackrf/tree/master/hardware/operacake (date accessed: 04/05/2021).