Automatizovaná detekce vektorů útoku pomocí SDR (Software Defined Radio)

Bc. Ondrej Vavro

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Ondrej Vavro**
Osobní číslo:	**A21190**
Studijní program:	**N0613A140022 Informační technologie**
Specializace:	**Kybernetická bezpečnost**
Forma studia:	**Kombinovaná**
Téma práce:	**Automatizovaná detekce vektorů útoku pomocí SDR (Software Defined Radio)**
Téma práce anglicky:	**Automated Attack Vector Detection Using SDR (Software Defined Radio)**

Zásady pro vypracování

1. Specifikujte signály elektromagnetického spektra v rádiové oblasti, spadajících do signálů zpracováváných pomocí SDR (Software Defined Radio).
2. Popište nejčastejší útoky na bezdrátové technologie pomocí SDR.
3. Navrhněte přenosný systém pro detekci možných vektorů útoků s pomocí SDR.
4. Systém implementujte v testovacím prostředí.
5. Proveďte ověření funkcí navrženého systému a srovnejte jej s již dostupnými řešeními.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. COLLINS, Travis F., Robin GETZ, Di PU a Alexander M. WYGLINSKI. Software-defined radio for engineers: Artech House mobile communications series. Artech House, 2018. ISBN 978-1-63081-459-5.
2. EWING, Martin. ABCs of Software Defined Radio: Why Your Next Radio Will be SDR. Amer Radio Relay League, 2012. ISBN 978-0-87259-632-0.
3. POORE, Christopher. FISSURE: The RF Framework for Everyone. Proceedings of the GNU Radio Conference [online]. 2022, 7(1) [cit. 2022-11-30]. Dostupné z: [https://pubs.gnuradio.org/index.php/grcon/article/view/122/102](https://pubs.gnuradio.org/index.php/grcon/article/view/122/102 "https://pubs.gnuradio.org/index.php/grcon/article/view/122/102") .
4. PICOD, Jean-Michel, Arnaud LEBRUN a Jonathan-Christofer DEMAY. Bringing software defined radio to the penetration testing community. Black Hat USA Conference [online]. 2014 [cit. 2022-11-30]. Dostupné z: [https://www.blackhat.com/docs/us-14/materials/us-14-Picod-Bringing-Software-Defined-Radio-To-The-Penetration-Testing-Community-WP.pdf](https://www.blackhat.com/docs/us-14/materials/us-14-Picod-Bringing-Software-Defined-Radio-To-The-Penetration-Testing-Community-WP.pdf "https://www.blackhat.com/docs/us-14/materials/us-14-picod-bringing-software-defined-radio-to-the-penetration-testing-community-wp.pdf").
5. GRECO, Claudia, Giancarlo FORTINO, Bruno CRISPO a Kim-Kwang Raymond CHOO. AI-enabled IoT penetration testing: state-of-the-art and research challenges. ENTERPRISE INFORMATION SYSTEMS [online]. 2022 [cit. 2022-11-30]. ISSN 17517575. Dostupné z: doi:10.1080/17517575.2022.2130014 .
6. GUZMAN, Aaron a Aditya GUPTA. IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices. 1. Packt Publishing, 2017. ISBN 9781787285170.
7. VEENS, Thomas. Automated 2G traffic interception and penetration testing. Eindhoven, 2018. Diplomová práce. Eindhoven University of Technology.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **5. listopadu 2023**
Termín odevzdání diplomové práce: **13. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 5. ledna 2024

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomové práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne .....

podpis studenta

ABSTRAKT

Práca rozeberá problematiku bezpečnostných útokov na takmer celé spektrum elektromagnetických frekvencií používaných ku komunikácii a prenosu dát, a to pomocou SDR. Využíva faktu, že niektoré frekvencie sú považované za bezpečné pre prenos len vďaka svojej rozdielnej frekvencii od užívateľsky ľahko dostupných. Práca popisuje návrh a prevedenie prenositeľného zariadenia, ktoré je možné k tomuto účelu použiť.

Klíčová slova: bezpečnosť, frekvenčné spektrum, vektor útoku, SDR

ABSTRACT

Thesis analyzies security attacks on almost the entire range of electromagnetic frequencies used for communication and data transfer, with help of an SDR. It uses the fact that some frequencies are considered safe due to having different frequencies from the user frequencies, that are easily accessible. Thesis describes design, construction and implementation of a portable device useable to this end.

Keywords: security, frequency spectrum, attack vector, SDR

POĎAKOVANIE

Chcem sa poďakovať svojmu vedúcemu práce, pánu Ing. Davidu Malaníkovi, PhD., za jeho cenné poznatky v oblasti bezpečnosti, ktoré mi poskytol, určovanie smeru a formy práce, aby odpovedala vedeckému štandardu, a za jeho precíznosť pri kontrole obsahu práce a trpezlivosť pri jej korektúre.

Tiež chcem poďakovať celému obsadeniu fakulty, a predovšetkým jeho vedeniu, za to, že mi umožnilo venovať sa tomuto študijnému odboru a snáď tak prispieť k zvýšeniu bezpečnosti v modernom IT svete.

V neposlednej rade ďakujem svojim rodičom, súrodencom a blízkym za ich trpezlivosť, kolegom za ich ochotu deliť sa o študijné informácie a za diskusiu k študijným problémom.

OBSAH

ÚVOD

Prešlo viac ako 120 rokov od Herzovho objavu rádiových vĺn a ich využitia Marconim k prenosu kódovanej informácie. Za toto obdobie bolo ľudstvo schopné pokoročiť vo využívaní rádiovej komunikácie na takú úroveň, že dnes je len málo miest na Zemi, ktoré by neboli pokryté pozemnou rádiovou komunikáciou a takmer žiadne, ktoré by odolali dosahu satelitnej rádiovej komunikácie.

Táto skutočnosť viedla k tomu, že dnes je možné takmer z každého miesta na Zemi odpočúvať nejakú komunikáciu. Táto skutočnosť v minulosti nebola postatná, keďže pre zachytenie rádiovej komunikácie bolo potreba buď univerzálnu a komplexnú, ťažko prenositeľnú techniku alebo špeciálne zariadenie nastavené od výroby na jediný účel (a na relatívne úzke frekvenčné pásmo). V dôsledku toho nebola potreba ochrany komunikácie na prvom mieste, ak vôbec bola braná v potaz.

Vývoj však ženie kupredu i techniku v tejto oblasti, a to míľovými krokmi. To čo bolo kedysi možné len s objemným a drahým hardvérom je dnes dosiahnuteľné s ľahko prenositeľným zariadením, ktoré sa vojde doslova do dlane. Už nie je potreba veľmi citlivých prímačov a amplifikáciu a filtrovanie signálu, ktorý kvôli vysokému šumu ani nebolo možné dekódovať. Stačí sa dostaviť do rozumnej vzdialenosti, a ani konfigurovateľná filtrácia "za behu" nerobí modernej technike problémy.

A čo viac, komplexná a rýchla komunikácia, vyžadujúca logiku stavových automatov na čipe, je dnes do istej miery nahraditeľná rýchlymi procesormi a ich výpočetnou kapacitou či vhodnými, na mieste reprogramovateľnými, čipmi. Otvára sa tak možnosť dekódovať takmer akúkoľvek komunikáciu v reálnom čase s univerzálnym zariadením, a teda na ňu i útočiť. Toto otvára mnohé otázky ohľadom terajšieho zabezpečenia rádiovej komunikácie v našej spoločnosti.

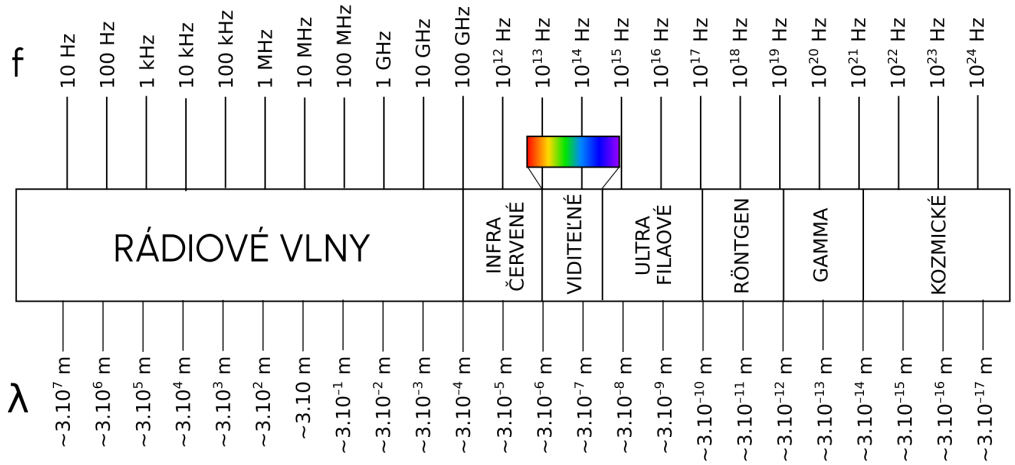
Táto práca sa zaoberá problematikou vyhľadávania slabých miest spôsobených nedostatočným zabezpečením alebo chybou v designovom návrhu komunikačných prvkov. V Sekcii 1 a 2 rozoberá fyzikálne princípy a základy rádiovej komunikácie, Sekcia 3 sa venuje univerzálnemu zariadeniu využívajúcemu softvér pre rádiovú komunikáciu – Software Defined Radio (SDR). Sekcia 4 ďalej skúma bezpečnosť v danej oblasti a Sekcia 5 prezentuje využiteľný softvér a nástroje pre analýzu a spracovanie zachytenej komunikácie. Nasledujúce sekcie prezentujú návrh a zostavenie zariadenia umožňujúceho skúmať bezpečnosť v teréne, a to na základe existujúcich komponentov (Sekcia 6), tak i novo vytvorených (Sekcia 6.5). Posledná Sekcia 7 skúma možnosti takéhoto zariadenia – v testovacom i reálnom prostredí.

I. TEORETICKÁ ČASŤ

1 ELEKTROMAGNETICKÉ SPEKTRUM

Elektromagnetická sila je jednou zo štyroch základných známych síl, pre ktorú existuje najpodrobnejší teoretický popis. Niet preto divu, že využitie tejto sily nás sprevádza každý deň, v každej oblasti ľudského života – v komunikácii, zdravotníctve, v senzoroch rôzneho typu, v osvetlovacej technike, gastronómii, a pod.

James Clerk Maxwell v klasickej teórii elektromagnetizmu, ktorá vznikla najmä z jeho práce, prepovedal vznik elektromagnetických vĺn, ktoré sa šíria priestorom [1]. V tej dobe predstava zahrňovala hlavne svetlo, ale matematicky dávali zmysel i iné frekvencie.



Obrázek 1.1 Rozdelenie elektromagnetického spektra, **f** predstavuje frekcencie a **λ** vlnové dĺžky [2].

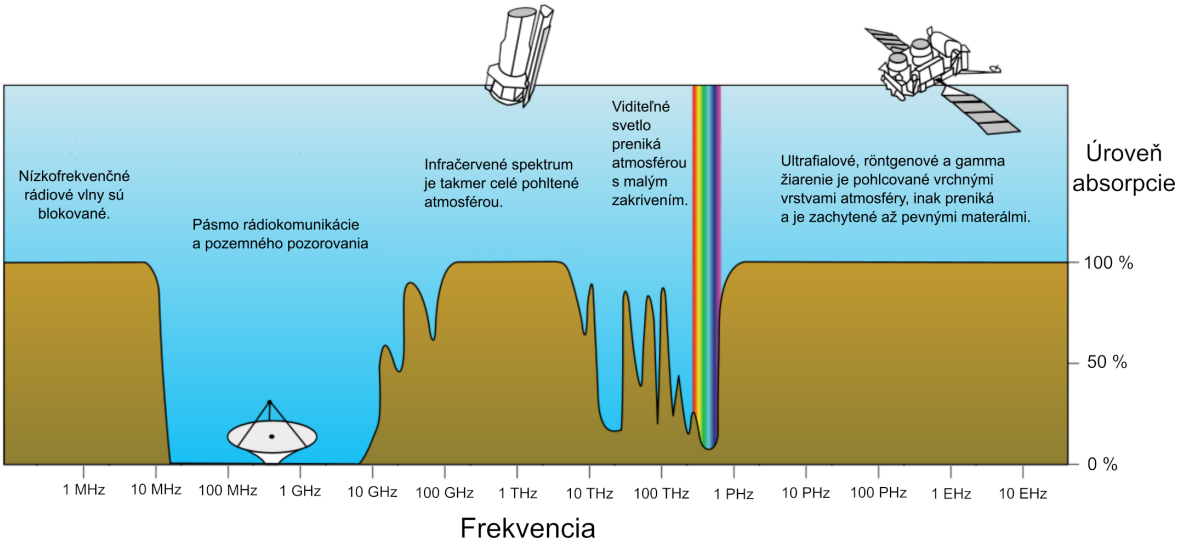
Z dnešného hľadiska môžeme elektromagnetické spektrum rozdeliť do nasledujúcich kategórií (viď Obr. 1.1):

- pásmo rádiových frekvencií – rádiokomunikácia, rádioidentifikácia, atp.
- infračervené pásmo – ohrev, termovizualizácia, nočné videnie, atp.
- viditeľné svetlo – ľudské videnie, fotografovanie, atp.
- ultrafialové pásmo – detekcia látok, dezinfekcia, overovanie bezpečnostných prvkov tlače, atp.
- rontgenové pásmo – medicínske využitie, detekcia materiálových chýb, bezpečnostné skenovanie, atp.
- pásmo gamma – sterilizácia, medicínske využitie, atp.

- pásmo kozmického žiarenia – astofyzika, sledovanie objektov ďalekého vesmíru, atp.

Frekcencie nad ultrafialovým žiarením (vrátene jeho časti) radíme do kategórie *ionizujúceho* žiarenia, pretože ich vplyvom dochádza k zmene genetickej informácie a rozpadu bunečného života. Tieto frekvencie na Zemi filtrujú vrstvy atmosféry a umožňujú tak život na našej planéte.

Nižšie frekvencie okolo seba vidíme každý deň. Ich vplyv na život je minimálny, prevážne sa premieňajú na teplo. Špeciálne rádiové frekvencie, ktoré majú schopnosť prenikať do istej miery predmetmi, sú vhodné pre komunikáciu na väčšie vzdialenosti. Na 1.2 je možné vidieť mieru absorpcie rôznych frekvencií elektromagnetického spektra v atmosfére.



Obrázek 1.2 Absorpcia elektromagnetických vĺn v atmosfére [3].

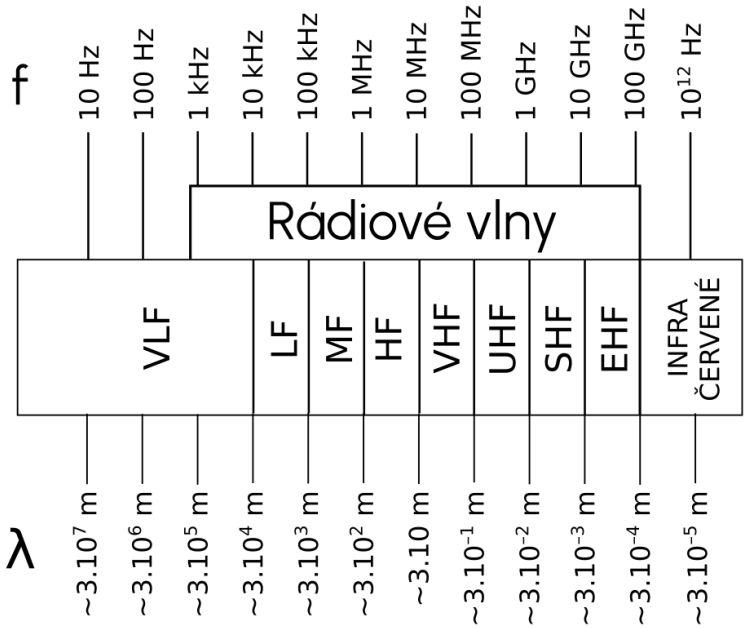
Je zreteľné, že z pohľadu absorpcie atmosférou je časť pásma rádiových frekvencií ideálna pre komunikáciu na dlhšie vzdialenosti. Ďalšie detaily v tomto smere poskytne nasledujúca kapitola.

2 RÁDIOVÝ PRENOS DÁT

Praktické vytvorenie elektromagnetických vĺn v kontrolovanom prostredí sa podarilo až Heinrichovi Herzovi. Krátko na to došlo i k ich praktickému využitiu pre potreby diaľkovej komunikácie, a k spopularizovaniu tohoto systému Guglielmom Marconim. Komunikáciu bola zo začiatku jednoduchá, šlo o dlhé a krátke signály kódované v morseovej abecede. Jednoduché zapínania a vypínania vysielania však veľmi skoro prestalo dostačovať a z toho dôvodu bolo potrebné hlbšie porozumieť problematike vysielania.

2.1 Využívané frekvencie

Vzhľadom na relatívne široké spektrum frekvencií spadajúcich do rádiového pásma a rôzne vlastnosti vysielania na rôznych frekvenciách bolo toto pásmo rozdelené na subpásma, kde je každé využíné na rôzne účely (typicky však podobného charakteru v danom pásme). Rozdelenie na subpásma na 2.1 je len jedno z možných, avšak najčastejšie používaných.



Obrázek 2.1 Rozdelenie rádového spektra podľa ITU, **f** predstavuje frekcencie a **λ** vlnové dĺžky [2].

Rádiové spektrum tvoria vlny so širokým rozpätím frekvencií približne do 100 GHz a môžeme ich rozdeliť do nasledujúcich kategórií [4] [5]:

- pásmo veľmi nízkych frekvencií (VLF) – využitie v komunikácii s ponorkami, v komunikácii v podzemních baniach

- pásmo nízkych frekvencií (LF) – využitie v navigácii, synchronizácii časových signálov, pre amatérske rádio a identifikáciu na rádiovej frekvencii (RFID)
- pásmo stredných frekvencií (MF) – využitie pre vysielanie rádia v oblasti amplitúdovej modulácie (AM), bezkontaktně prístupové systémy, lavínové záchranné vysielače, pre amatérske rádio
- pásmo vysokých frekvencií (HF) – využitie pre bezkontaktné platby a komunikáciu blízkeho poľa (NFC), leteckú komunikáciu "za horizont", komunikáciu na mori, bezdrôtové domáce telefóny
- pásmo veľmi vysokých frekvencií (VHF) – využitie pre vysielanie rádia v oblasti frekvenčnej modulácie (FM), televízne prenosy, amatérske rádio, bezpečnostné zložky (polícia, hasiči, a pod.), komunikáciu informácií o počasí z meteorologických staníc
- pásma ultra (UHF) a super (SHF) vysokých frekvencií – mikrovlnná komunikácia – bezdrôtovú lokálnu sieť (WiFi), BlueTooth, ZigBee, LoRa, a pod., mikrovlnný ohrev jedla, satelitnú navigáciu (GPS, Galileo, Glonass, Beidou), satelitná telefónna komunikácia, satelitné vysielanie, a pod.
- pásmo extra vysokých frekvencií (EHF) – rádio astronómia, mikrovlnné zbrane, a pod.

Z uvedených pásiem sa táto práca bude prevažne orientovať na rozmedzie od veľmi vysokých frekvencií (VHF) až po super vysoké frekvencie (SHF), keďže tieto tvoria jadro bežnej bezdrôtovej komunikácie v spoločnosti. Zároveň väčšina softvérovo definovaných rádií(SDR, definované v kapitole 3) pracuje s v pásme HF až SHF frekvencií, pričom pre použitie v HF spektre vyžaduje špeciálny formát antén, a preto sa nimi táto práca nezaoberá.

2.2 Správa a legislatíva

Po úvodnom objave existencie a možnostiach využitia elektromagnetických vĺn, nastal veľký boom v ich využívaní. Už v roku 1865 preto vznikla Medzinárodná telegrafická únia, ktorá mala na starosti prepájanie národných telegrafických sietí. Neskôr, s príchodom hlasovej komunikácie, bola táto organizácia v 1949 začlenená do štruktúry Organizácie spojených národov (UN) ako jej agentúra a premenovaná na *Medzinárodnú telekomunikačnú úniu (ITU)*.

ITU je zodpovedná za koordináciu užívania rádiofrekvenčného pásma na medzinárodnej úrovni, za vznik a koordináciu štandardov pre telekomunikáciu a informačné

komunikačné technológie, a za vytváranie vhodných podmienok pre rozširovanie komunikačných technológií v rozvojových krajinách. ITU je v jednotlivých zemiach sveta podporovaná národným úradom, v Česku je to *Český telekomunikační úřad (ČTÚ)*.

ČTÚ má na starosti množstvo úloh prideleným rôznymi zákonmi ČR. Okrem iného sa jedná o prideľovanie a správu rádiových frekvencií v ČR, reguláciu trhu a stanovovanie podmienok podnikania, predkladá legislatívne návrhy vláde a spolupracuje na príprave zákonov, udeľuje a vyberá poplatky za využívanie istých frekvenčných pásiem, stará sa o právoplatné využívanie frekvenčného spektra a uděľuje sankcie za porušenie, a pod.

Prideľovanie frekvencií sa riadi Medzinárodným telekomunikačným rádom, ktorého sekcie upravuje vyhláška ČR 105/2010 Sb., upravená vyhláškou ČR 467/2021 Sb (k aktuálnemu dátumu). ČTÚ prideľuje frekvencie na základe plánu v *Národní kmitočtové tabulce* schválenej v spomenutej vyhláške a tiež vydáva všeobecné opatrenia, ktoré oprávňujú využívanie niektorých frekvencií za špecifických podmienok. Každý užívateľ určitého frekvenčného pásma má na starosti dodržiavanie predpisov a to vrátane zamedzenia rušenia iných pásiem neprimeraným vysielacím výkonom.

Vo frekvenčnom spektre sú vymedzené frekvenčné pásma používané v priemysle, vo vede a lekárstve (ISM pásma), ktoré sú takzvanými voľnými frekvenciami, čo znamená, že využívanie je obmedzené iba vysielacím výkonom, za jeho využívanie nie je potrebné platiť poplatky a na daných frekvenciách sa predpokladá, že rušenie z okolia bude značné a je potrebné s ním počítať. Tieto frekvencie sú najviac používané v priemysle práve vďaka možnosti ich celosvetového využitia. V Českej republike je zoznam takýchto frekvencií upravený všeobecným opetrením č. VO-R/10/07.2021-8, ktoré doplňuje ďalšie frekvencie k medzinárodne vymedzeným. Vybrané frekvencie je možné vidieť v tabuľke 2.1.

Okrem týchto frekvencií existujú ešte ISM pásma špecifické pre niektoré regióny, či krajiny. Táto práca sa bude venovať predovšetkým spomenutým ISM pásmam, a v prípade odbočenia od nich bude použitie takýchto pásiem explicitne popisovať.

2.3 Signálová teória

Ako bolo uvedené, frekvenčné pásma sa skladajú z rôznych pridelených rozsahov. Rozsahy môžu byť podľa potreby delené na rádiové kanály. Na to, aby sme porozumeli limitom rádiovej komunikácie, je potreba matematicky namodelovať prenášanú informáciu.

Rozsah frekvencií	**Stredová frekvencia**	**Šírka pásma**	**Typické využitie**
13,553 - 13,567 MHz	13,56 MHz	14 kHz	RFID a NFC platby
26,957 - 27,283 MHz	27,12 MHz	326 kHz	priemyselné ohrievanie a sušenie, medicínska elektroterapia, diaľkové ovládanie hračiek
40,66 - 40,7 MHz	40.68 MHz	40 kHz	diaľkové ovládanie a telemetria
138,2 - 138.45 MHz	138.33 MHz	25 kHz	ground-penetrating radary (GPR)
433,05 - 434.75 MHz	434.4 MHz	1,7 MHz	diaľkové ovládania, zvončeky, bezdrôtové merače veličín
915 - 921 MHz	918 MHz	6 MHz	mobilné siete
2,4 - 2,5 GHz	2,45 GHz	100 MHz	WiFi a Bluetooth
5,725 - 5,875 GHz	5,8 GHz	150 MHz	WiFi a automatické dverné systémy
24,0 - 24.25 GHz	24,125 GHz	250 MHz	mobilné signálové senzory

Tabulka 2.1 ISM frekvenčné pásma

2.3.1 Deterministický a náhodný signál

Prenášaná informácia môže nadobúdať rôzne neznáme hodnoty v čase, a preto je vhodné ju modelovať ako náhodný signál. Na rozdiel od *deterministického signálu*, u náhodného (stochastického) signálu nie je možné predom určiť jeho hodnotu v akomkoľvek čase a je možné ho popísať iba určitými štatistickými vlastnosťami, či pravdepodobnostnými charakteristikami [5].

Signály teda môžeme rozdeliť z pohľadu možnosti predikcie informácie na:

- deterministické – je možné určiť všetky budúce hodnoty signálu
  - periodické – hodnoty sa pravidelne opakujú s určitou periódou
  - neperiodické – neexistuje žiadna perióda opakovania
- náhodné (stochastické) – budúce hodnoty signálu nedokážeme presne určiť, ale iba s určitou pravdepodobnosťou
  - stacionárne – štatistické charakteristiky signálu nezávisia od voľby počiatku časovej osi
    - ergodické – štatistické charakteristky jedného úseku signálu sa zhodujú so štatistikami celého signálu

    - neergodické – štatistické charakteristiky signálu sa líšia medzi jeho úsekmi i voči celistvému signálu
  - cyklostacionárne – štatistické charakteristiky signálu obsahujú určitú pravidelnú periódu opakovania
  - nestacionárne – voľba počiatku časovej osi mení charakteristiky signálu

Prenášaný signál je *spojitý* v čase, keďže je prenášaný skrze spojité médium. Jeho reprezentácia vo výpočetných systémoch je však *diskrétna*, pretože digitálne systémy nedokážu pracovať priamo so spojitou reprezentáciou. Pre *spojitý signál* zaveďme označenie $x(t)$ a pre *diskrétny signál* označenie $x(n)$. Rozdielom $x(n)$ oproti $x(t)$ je, že $x(n)$ je definovaný len v diskrétnych častoch nT_s, kde n nadobúda hodnoty $\pm 1, \pm 2, \pm 3, \ldots$ a T_s je odstup jednotlivých časových okamihov.

Ďalej si ukážeme definície niektorých žiadaných typov signálov a ich charakteristík.

Periodický signál je typický pre nosnú vlnu u modulovaného signálu. Pre periodické signály platí, že sa ich hodnota pravidelne opakuje v čase s určitým časovým odostupom:

$$f(t) = f(t + nT_0) \tag{2.1}$$

, kde T_0 je konštanta, doba periódy, s rozsahom $0 < T_0 < \infty$ a n je prirodzené kladné číslo.

Nosná vlna typicky býva harmonický signál, sínusoida. Vzhľadom ku komplexnej povahe elektromagnetických vĺn je najlepšie vyjadrená *komplexnou exponenciálou* ako:

$$x(t) = e^{j2\pi f_0 t} = \cos 2\pi f_0 t + j \sin 2\pi f_0 t \tag{2.2}$$

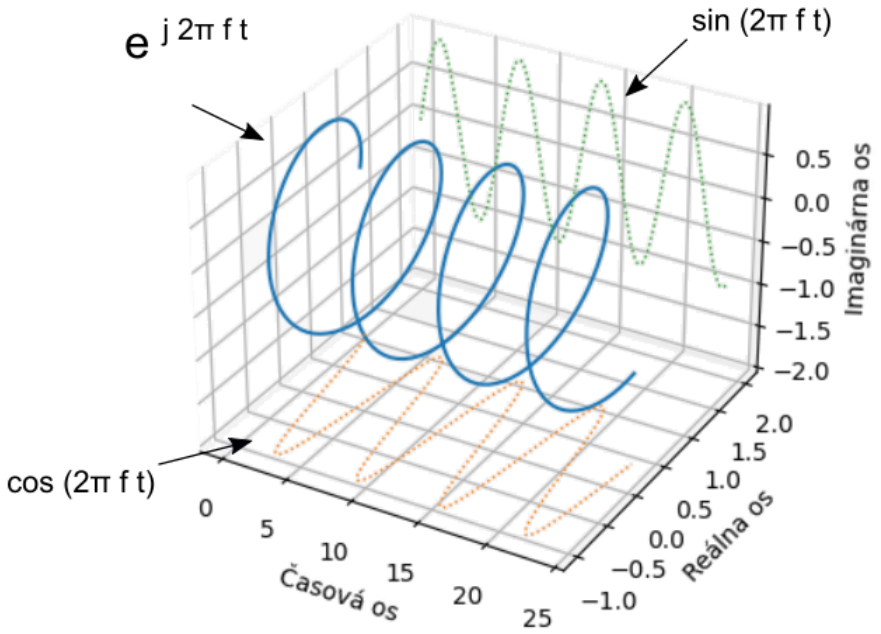
Kde reálna zložka vyjadrená kosínusom predstavuje zložku elektrického poľa a imaginárna zložka vyjadrená sínusom vyjadruje zložku magnetického poľa. Situáciu je možné ilustrovať obrázkom 2.2.

Diskrétna forma komplexnej exponencionály má podobu:

$$x(n) = e^{j2\pi f_0 n} = \cos 2\pi f_0 n + j \sin 2\pi f_0 n \tag{2.3}$$

Rozdiel medzi týmito dvoma signálmi spočíva v tom, že:

- frekvencia diskrétneho signálu nie je jednoznačná, pretože platí:



Obrázek 2.2 Komplexná exponenciála vyjadrujúcu elektromagnetickú vlnu.

$$e^{j2\pi(f_0+1)n} = e^{j2\pi f_0 n} \tag{2.4}$$

, a preto býva f_0 definovaná len v rozsahu $0 \leq f_0 \leq 1$

- ak má byť periodická s periódou N musí platiť:

$$e^{j2\pi f_0(n+N)} = e^{j2\pi f_0 n} \tag{2.5}$$

$$\begin{aligned} \text{pre } n = 0 \quad &\Rightarrow \quad e^{j2\pi f_0 N} = 1 \\ f_0 N = m \quad &\Rightarrow \quad f_0 = \frac{m}{N}, \quad m \in \mathbb{N} \end{aligned}$$

, z čoho vyplýva, že diskrétny signál vzorkovaný z periodického spojitého signálu je tiež periodický len v prípade, že vzorkovacia frekvencia je rovná celočíselnému násobku m počtu vzorku behom periódy $T_0 = f_0^{-1}$, a teda $\frac{1}{f_0} = mT_s \Rightarrow \frac{f_s}{f_0} = m$. Tento fakt je dôležitým aspektom pri spektrálnej analýze signálov [5].

2.4 Modulácia, multiplex a prenos dát

2.4.1 Modulácia

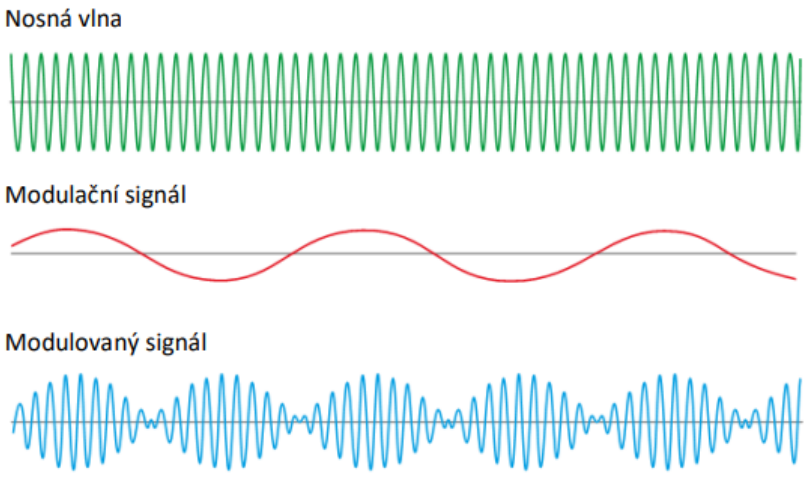
Na základe porozumenia vlastnostiam periodických signálov bolo možné namiesto cyklického zapínania a vypínania signálu prejsť na komplexnejšie úpravy – moduláciu nosnej elektromagnetickej vlny.

Modulácia rádiových vĺn je metóda používaná v rádiovom prenose pre prenos informácií skrze zmenu vlastností nosnej vlny, ako je frekvencia, amplitúda, či fáza. Táto technika bola zásadnou pre umožnenie praktickej bezdrôtovej komunikácie v reálnom čase na dlhé vzdialenosti [6].

Modulácia využíva *nosnú vlnu* (carrier wave), ktorá je periodickou harmonickou vlnou o frekvencii väčšej (typicky ďaleko väčšej) ako je frekvencia informácie. Určité parametre tejto vlny sú upravované v čase na základe vstupného signálu (baseband). Ako príklad si môžeme vziať amplitúdovú moduláciu. Amplitudová modulácia je vlastne len súčinom nosnej vlny a vstupného signálu [5]:

$$w(t) = c(t) \cdot s(t) \tag{2.6}$$

, kde $c(t) = \sin(\omega_c t + \phi_c)$ predstavuje nosnú vlnu (carrier), $s(t)$ je modulačný signál (obecne signál rôznorodého charakteru) a $w(t)$ predstavuje výslednú modulovanú vlnu, príklad ktorej je možné vidieť na obrázku 2.3.



Obrázek 2.3 Amplitúdová modulácia nosnej vlny [3].

Nosná vlna má vzhľadom na komplexnú povahu elektromagnetickej vlny častejšie formu $c(t) = \exp(j\omega_c t + \phi_c)$ a teda výsledný modulovaný signál má povahu:

$$w(t) = s(t) \cdot e^{j\omega_c t + \phi_c} \tag{2.7}$$

Bez modulácie by bolo potrebné prenášať informáciu, ako napríklad zvukové vlny hlasu, na ich vlastnej frekvencii(20 Hz – 20 kHz), čo by malo množstvo negatívnych následkov, ako napr.:

- úzka šírka pásma – dochádza k rýchlemu zahlteniu prenosového kanálu (existuje vlastne len jeden možný)
- nemožnosť prenosu – pri nízkych frekvenciách by dochádzalo k príliš veľkému útlmu
- príliš komplikovaný vysielací a príjmací hardvér – ladenie frekvencií podľa aktuálneho typu prenášanej informácie a jej frekvencie by spôsobovalo množstvo problémov ako na vysielacej, tak i príjmacej strane (rôzne typy antén, oscilačných obvodov, atp.)

Naopak, modulácia umožňuje využívanie ďaleko väčších frekvencií než je frekvencia prenášanej informácie, čo umožňuje vytvorenie viacerých komunikačných kanálov, znižuje riziko medzikanálového rušenia a tiež umožňuje použiť menší vysielací výkon.

Medzi základné typy modulácie patria [6]:

- amplitúdová modulácia (AM) – spomenutá vyššie, moduluje výkon (amplitúdu) vlny. Kedysi používaná k prenosu terestriálneho vysielania, dnes skôr používaná k obojsmernej komunikácii.
- frekvenčná modulácia (FM) – moduluje frekvenciu nosnej vlny podľa signálu, t.j. $w(t) = exp(j\omega_c t + j2\pi \int_0^t s(t))$ (pre zjednodušenie predpokladáme, že fáza je v čase $t = 0$ nulová, t.j. $\phi = 0$). Oproti amplitúdovej modulácii ponúka lepšiu ochranu signálu voči šumu a preto sa stále bežne používa v terestriálnom vysielaní (rádio) a VHF komunikácii.
- fázová modulácia (PM) – zahŕňa zmenu fáze nosnej vlny na základe signálu, t.j. $w(t) = \exp(j\omega_c t + s(t))$ (pre zjednodušenie opäť predpokladáme, že fáza je v čase $t = 0$ nulová).

Podobne ako výpočetná technika postupne prešla vývojom z analógovej formy k digitálnej, rovnako i modulácia má analógovú i digitálnu podobu. Varianty modulácie digitálnych signálov sú:

- kľúčovanie amplitúdovým posuvom (ASK) – obdobne ako AM mení amplitúdu signálu, avšak využíva len určité špecifické hodnoty amplitúdy (napr. nízku a vysokú) pre kódovanie digitálneho signálu.

- kľúčovanie frekvenčným posuvom (FSK) – obdobne ako FM mení frekvenciu signálu, na základe signálu ju nastavuje na špecifické hodnoty.
- kľúčovanie fázovým posuvom (PSK) – obdobne ako u PM mení fázu signálu, nastavuje fázu na preddefinované hodnoty.

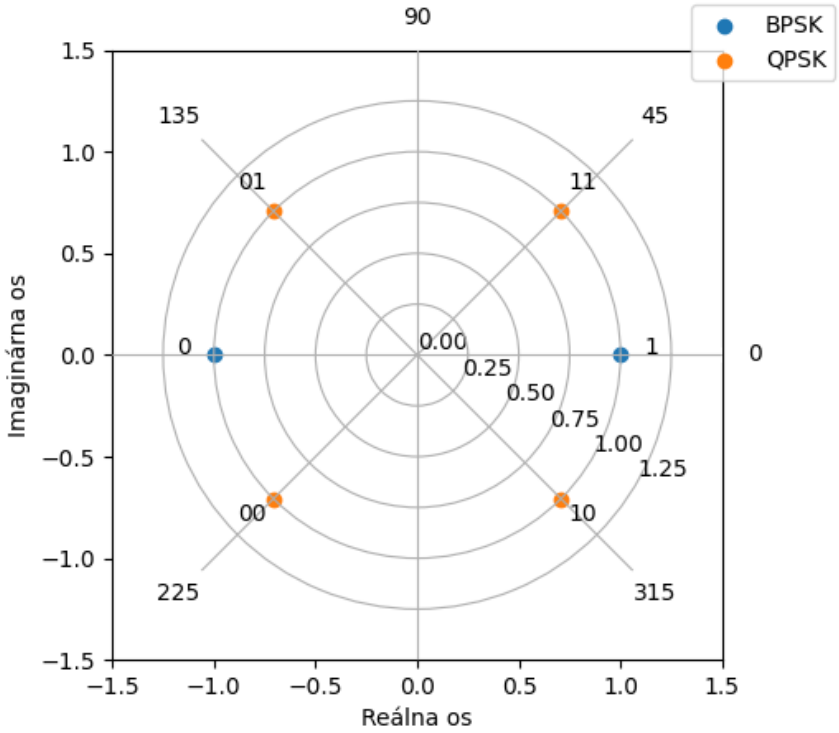
Tieto digitálne modulácie nadobúdajú v praxi rôznych variant, ktoré majú vlastné pomenovania. Niektoré vybrané varianty sú popísané nižšie:

- binárne kľúčovanie fázovým posuvom (BPSK) – funguje ako fázová modulácia, pričom nastavuje fázu podľa binárneho signálu na hodnoty vzdialené od seba čo najďalej na fázovej kružnici, aby bolo možné ich jednoducho rozlíšiť. To znamená, že napr. pre hodnotu signálu 0 nastavuje fázu na 0° a pre hodnotu signálu 1 na 180°.
- kvadratúrne kľúčovanie fázovým posuvom (QPSK) – obdobne ako BPSK nastavuje hodnotu fáze na jednoducho rozlíšiteľné hodnoty, v tomto prípade sa jedná o stredy kvadrantov jednotkovej kružnice, t.j. hodnoty fáze 45°, 135°, 225° a 315°. Tieto hodnoty fáze kódujú dátové symboly 11, 01, 00, a 10. Takýto prípad, kedy sú hodnoty rozlíšené o hodnotu fáze 90° nazývame *kvadratúrou* alebo *ortogonalitou*.
- kvadratúrna amplitúdová modulácia (QAM) – obdobná situácia ako u QPSK, avšak využívame 2 amplitúdovo modulované vlny, posunuté vo fáze o 90°. Vlny sú sčítané pre prenos avšak na príjmači je možné ich znovu separovať vďaka ich ortogonalite. Je tak možné preniesť dvojnásobný objem dát na rozdiel od AM. Táto schéma sa často využíva u pokročilejších modulácií.

Pre lepšiu ilustráciu a porovnanie môžeme zobraziť symboly prenášané BPSK a QPSK moduláciami na fázovej kružnici, či *IQ diagrame* [5]. IQ diagram obsahuje reálnu osu, ktorá predstavuje tzv. in-phase zložku a imaginárnu osu, ktorá predstavuje tzv. kvadratúrnu zložku (posunutú o 90°), ako je vidieť na obrázku 2.4. Body na obrázku reprezentujú hodnoty fáze komplexnej exponenciály kódujúce symboly modulácie, pre porovnanie viď obrázok 2.2. To znamená, že fáza signálu je v pravidelných intervaloch, ktoré odpovedajú tempu prenosu symbolov, upravovaná tak, aby odpovedala aktuálne prenášanému symbolu.

Modulácie BPSK, QPSK a QAM sú využívané v bežne používaných sieťach ako WiFi, Bluetooth a v terestriálnom vysielaní DVB-T/T2.

Ďalšie pokročilé typy modulácie sú neustále vo vývoji s cieľom preniesť spoľahlivo čo najväčší možný objem informácie.



Obrázek 2.4 Fázový diagram pre vybrané variácie digitálnej modulácie PSK, spolu s kódovými značkami.

2.4.2 Multiplex a mnohonásobný prístup

Na základe poznatkov o ISM frekvenčných pásmach uvedených v sekcii 2 a z informácií z predošlého odstavca je možné vyvodiť, že dostupné frekvenčné pásma by sa mohli rýchlo stať zahltenými, ak by nedochádzalo k istej forme zdieľania, či organizácie komunikácie.

Multiplex je metóda kombinácie viacerých analógových alebo digitálnych signálov do jedného signálu pre potreby prenosu skrze zdieľané médium, v tomto prípade úzky kanál vo využiteľnej časti elektromagnetického frekvenčného spektra.

Takáto organizácia či zdieľanie môže prebiehať na rôznych úrovniach a tak môžeme rozlišovať [5]:

- multiplex časovým delením (TDM) – každý z nezávislých signálov má v časovom okne pridelenú určitú jeho časť, tzv. *slot*, ktorý môže plne využívať, pričom časové okná sa pravidelne opakujú. Signály sa teda rovnocenne striedajú v čase pri využívaní kanálu.
- multiplex s frekvenčným delením (FDM) – každý z nezávislých signálov má pridelené vlastné frekvenčné pásmo v rámci kanálu, ktoré plne využíva.
- multiplex s kódovým delením (CDM) – každý z nezávislých signálov má pridelené

jedinečné kódovacie signály. Je tak možné zároveň v čase i frekvencii vysielať viacero signálov v rámci kanálu, ktoré je na príjmači možné vďaka kódovaniu rozlíšiť.

- multiplex s prestorovým delením (SDM) – každý z nezávislých signálov je prenášaný oddelenou anténou, pričom tieto antény sú dostatočne smerové na to, aby sa pri vysielaní signály nerušili alebo je využitá technológia fázovo synchronizovaných antén (phase array), ktoré umožnujú pomocou konštruktívnej a deštruktívnej interferencie vytváranie vysoko smerových lúčov (beam forming) vo variabilnom smere.

častejšie sa v bezdrôtových sieťach rieši prepojenie viacerých účastníkov, často pri nezávislých kominikáciách, v rámci zdieľaného kanála. Takáto komunikácia je založená na multiplexe, ale často vyžaduje komplikovanejšiu a mierne odlišnú technológiu, aby bolo umožnené oddelenie jednotlivých nezávislých komunikácií.

Táto forma zdieľania sa nazýva *protokol mnohonásobného prístupu* a zahŕňa pravidlá a vzájomné dohody, ktoré zabezpečujú bezproblémový prístup a využívanie bezdrôtového kanálu všetkými účastníkmi. Obdobne k formám multiplexu rozlišujeme:

- mnohonásobný prístup s časovým delením kanálov (TDMA)
- mnohonásobný prístup s frekvenčným delením kanálov (FDMA)
- mnohonásobný prístup s kódovým delením kanálov (CDMA)
- mnohonásobný prístup s prestorovým delením kanálov (SDMA)

Tieto protokoly hrajú výraznú rolu v prístupe k vysoko vyťaženým službám ako sú mobilné siete (CDMA a TDMA).

2.4.3 I/Q signál

I/Q signál (in-phase / quadrature) je dvojzložkový signál používaný v moderných rádiových komunikačných prostriedkoch. Jedná sa o dve nezávislé vlny, kosínusovú (in-phase) a sínusovú (quadrature), kde ako názov napovedá je jedna vlna posunutá o 90° vo fáze oproti druhej [7]. Snímanie a vytváranie takéhoto zdanlivo zdvojeného signálu má viaceré užitočné vlastnosti.

Súčtom vĺn, ktoré majú fázu 0° a 90° dostávame vlnu s fázou 45°. Podmienkou je však, aby obe vlny mali rovnakú amplitúdu. V prípade rozdielnej amplitúdy získavame signál s rôznym fázovým posuvom a to od 0°, v prípade úplného potlačenia Q zložky,

až po 90°, v prípade úplného potlačenia I zložky. Takýmito úpravami dokážeme pokryť I. kvadrant fázovej kružnice.

Zvyšné fázové kvadranty je možné získať použitím negatívnej amplitúdy, t.j. v prípade I zložky získame použitím negatívnej amplitúdy signál s fázou 180° a v prípade Q zložky signál s fázou 270°. Amplitúdová i frekvenčná modulácia je stále možná vďaka spoločnej amplitúdovej či frekvenčnej modulácii I a Q zložiek.

Tento spôsob generovania signálu podstatne zjednodušuje hardvérový návrh a umožňuje vysielať fázovo modulovaný signál pomocou jednoduchej amplitúdovej modulácie[8].

Ďalšou užitočnou vlastnosťou IQ signálu pri príjmaní je, že pri vzorkovaní signálu vznikajú I a Q zložky nezávisle na sebe. Táto vlastnosť umožňuje získavať vzorky rovnakého signálu v dvoch fázových rovinách a efektívne tak zdvojnásobiť vzorkovaciu frekvenciu, keďže časť signálu, ktorá by vplyvom aliasingu zanikla v I zložke sa prejaví v Q zložke a naopak.

IQ forma signálu tiež umožňuje jednoduchý hardvérový návrh fázových modulačných schém, ktoré sú na rozdiel od amplitúdovej modulácie jednoduchšie rozlíšiteľné pri nízkom odstupe signálu od šumu.

2.4.4 Šum

Pojem *šum* zahrňuje rôzne neužitočné signály, ktoré narušujú príjem žiadaných signálov. Zdrojom týchto signálov sú na jednej strane rôzne iné vysielače, tak i signály, ktoré nemajú pôvod v ľudskej komunikácii. Jedná sa o signály s pôvodom [5]:

- kozmickým – vznikajú mimo Zem a prenikajú atmosférou
- atmosferickým – prejavy počasia a kumulácie náboja v atmosfére, odrazy signálu od ionosféry, at.d
- lokálnym – rôzne zariadenia a elektronické súčiastky generujú vlastné nežiadúce signály, ktoré môžu spôsobovať rušenie
- tepelný – zmena teploty spôsobuje zmenu elektrických vlastností materiálov
- a pod.

Tieto formy šumu môžeme modelovať spoločne ako *aditívny Gaussovský šum*, či *biely šum*, keďže jeho spektrálna výkonová hustota je nulová [5], a modelujeme ho ako:

$$Y = S + N = S + \mathcal{N}(\mu, \sigma^2) \tag{2.8}$$

Následne môžeme definovať *odstup signálu od šumu (SNR)* ako pomer signálu S a šumu N:

$$SNR = \frac{S}{N} \quad [dB] \tag{2.9}$$

Táto veličina sa meria v decibeloch a je často používaná k odhadu kvality prijímaného signálu.

2.4.5 Ideálny komunikačný kanál

V náväznosti na obmedzené možnosti prenosových kanálov a existenciu šumu je vhodné si zadefinovať maximálnu kapacitu kanálu.

Prenosový kanál o šírke pásma B (Hz) dokáže pri priemernom výkone príjmaného signálu S (W) a priemernom výkone šumu N (W) preniesť:

$$C = B \cdot \log_2 1 + \frac{S}{N} \tag{2.10}$$

Veličina C označuje maximálnu kapacitu kanálu a je vyjadrená v bitoch za sekundu, označuje sa tiež ako *Shannonov limit* či *kapacita*.

Na základe tohoto vzťahu môžeme určiť, či je vôbec možné daným kanálom preniesť požadovaný objem dát alebo je potreba prenosový kanál zväčšiť.

2.4.6 Vzorkovací teorém

Prevod spojitého signálu na diskrétny v číslicových systémoch je zásadný pre jeho spracovanie. Avšak, ako bolo spomenuté v predošlom odstavci, pre jeho správne spracovanie je potrebné zachytiť v jednolivých vzorkách dostatok informácie na to, aby bolo ho možné verne zrekonštruovať. Táto potreba je zachytená v *Shannon-Nyquist-Kotelnikovom vzorkovacom teoréme*, ktorý požaduje vzorkovať analógový signál s frekvenciou (vzorkovacou, f_s), ktorá je väčšia alebo rovná dvojnásobku navyššej frekvencie ($f_{i\max}$) obsiahnutej vo vzorkovanom signále, t.j.:

$$f_s \geq 2 \cdot f_{i\max} \tag{2.11}$$

2.4.7 Diskrétna Fourierova transformácia

Akýkoľvek signál je možné rozložiť na súbor harmonických signálov. Signály je často vhodné analyzovať z pohľadu frekvenčných harmonických zložiek, ktoré ich utvárajú. K

prevodu z časových vzoriek na frekvenčné úrovne (biny) sa požíva *diskrétna Fourierova transformácia (DFT)* [5] [9]:

$$\mathcal{F}(kF_s) = T_s \sum_{n=0}^{N-1} x(nT_s) e^{-j2\pi \frac{k}{N} n} \tag{2.12}$$

, kde:

- $x(t)$ je vstupný spojitý signál a $x(nT_s)$ sú jeho vzorky v časových okamihoch vzdialených o T_s, t.j. $f_s = \frac{1}{T_s}$ je vzorkovacia frekvencia,
- N je celkový počet časových vzoriek a tiež celkový počet diskrétnych frekvencií (frekvenčných úrovní, binov),
- $F_s = \frac{1}{NT_s}$ je základná frekvencia a kF_s jej násobky pre $k \in \langle 0, N)$,
- a $\frac{k}{N}$ je uhlová frekvencia komplexnej exponenciály.

Takáto reprezentácia signálu sa nazýva *spektrum* a plnohodnotne vyjadruje pôvodný signál, za predpokladu, že je dodržaný vzorkovací teorém. Funkcia je potom reverzibilná na pôvodný signál pomocou *inverznej Fourierovej transformácie*:

$$x(nT_s) = \frac{1}{NT_s} \sum_{k=0}^{N-1} \mathcal{F}(kF_s) e^{+j2\pi \frac{n}{N} k} \tag{2.13}$$

Pre výpočet DFT existuje množstvo vysoko optimalizovaných algoritmov, ktoré sú používajú pod označením *rýchla Fourierova transformácia (FFT).*

2.4.8 Cyklostacionárne signály

Signály vytvárané ľuďmi májú často cyklostacionárny charakter, a to práve vďaka použitiu modulácie pri prenose. Modulovaný signál sa v spektre na prvý pohľad nemusí líšiť od šumu (až na vysielaný výkon), avšak bližšie určenie o aký signál sa jedná je pre laika náročné. Cyklostacionárne vlastnosti takýchto signálov umožňujú z ich charakteristík určiť bližšie charakter takýchto signálov.

Signály môžeme rozdeliť na signály vykazujúce cyklostacionaritu v štatistických ukazateľoch[10]:

- prvého rádu – parametre ako primer, smerodatná odchylka, a pod., sa cyklicky opakujú
- druhého rádu – napr. autokorelačná funkcia vykazuje cyklickú podobnosť signálu so sebou samím

2.4.9 Korelačná a autokorelačná funkcia

Krížová korelačná funkcia dvoch signálov, $x(t)$ a $y(t)$, je funkciou podobnosti týchto signálov. Táto podobnosť je vyjadrerná sumou súčinu signálov pri rôznom časovom posune τ jedného z nich voči druhému:

$$R_{xy}(\tau) = \sum_{n=-\infty}^{\infty} x(n) \cdot y^*(n-\tau) \tag{2.14}$$

, kde $y^*(n)$ je konjugovaná verzia signálu $y(n)$.

Autokorelačná funkcia je krížovou koreláciou nad tým istým signálom, t.j. $x(t) = y(t)$, a teda:

$$R_{xx}(\tau) = \sum_{n=-\infty}^{\infty} x(n) \cdot x^*(n-\tau) \tag{2.15}$$

Autokorelácia je práve jedným z nástrojov, ktorým môžeme analyzovať cyklické prvky v signále, keďže sa tieto prvky opakujú s určitou periódou [11].

Pre signál určitej dĺžky N definujeme autokorelačnú funkciu ako:

$$R_{xx}(\tau) = \frac{1}{2N-1} \sum_{n=-N}^{N} x(n+\frac{\tau}{2}) \cdot x^*(n-\frac{\tau}{2}) \tag{2.16}$$

2.4.10 Výkonová spektrálna hustota

Výkonová spektrálna hustota (PSD) vyjadruje rozloženie výkonu signálu naprieč rôznymi frekvenciami. Je možné ju vyjadriť ako:

$$S_{xx}(f) = \lim_{N\to\infty} \frac{1}{N} \left| \sum_{n=0}^{N-1} x(n) e^{-i2\pi nf} \right|^2 \tag{2.17}$$

, kde výraz $\sum_{n=0}^{N-1} x(n)e^{-i2\pi nf}$ je Fourierova transformácia signálu [11].

Skrze využitie *Wiener–Khinchinovho teorému* je možné ukázať vzťah medzi autokoreláciou a výkonovou spektrálnou hustotou pomocou Fourierovej transformácie:

$$S_{xx}(f) = \sum_{\tau=-\infty}^{\infty} R_{xx}(\tau) e^{-i2\pi\tau f} \tag{2.18}$$

2.4.11 Spektrálna korelačná funkcia a jej odhad

Signál $x(t)$ je cyklostacionárny signál druhého rádu, ak autokorelačná funkcia $R_x(t,\tau)$ je periodickou funkciou nad t s periódou T_0, viď 2.16 pre pravdepodobnostný prístup, pre nepravdepodobnostný môžeme vyjadriť [12]:

$$\hat{R}_x(t,\tau) = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-N}^{N} x\left(t + nT_0 + \frac{\tau}{2}\right) \cdot x^*\left(t + nT_0 - \frac{\tau}{2}\right) \tag{2.19}$$

Autokorelačná funkcia sa potom nazýva *periodickou*, či *limitovane periodickou*, a môže byť reprezentovaná Fourierovou radou:

$$R_x(t,\tau) = \sum_{\alpha} R_x^{\alpha}(\tau) e^{j2\pi\alpha t} \tag{2.20}$$

Suma sa prevádza skrz celočíselné násobky základnej frekvencie $\alpha = m \cdot f_0 = m \cdot \frac{1}{T_0}$. Koeficienty Fourierovej rady môžeme spočítať nasledovne, pre pravdepodobnostný prístup:

$$R_x^{\alpha}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} R_x(t,\tau) e^{-j2\pi\alpha t} dt \tag{2.21}$$

, či pre nepravdepodobnostný prístup:

$$\hat{R}_x^{\alpha}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} x(t+\frac{\tau}{2}) x^*(t-\frac{\tau}{2}) e^{-j2\pi\alpha t} dt \tag{2.22}$$

$R_x^{\alpha}(\tau)$ sa nazýva *cyklická autokorelačná funkcia*, či *limitná cyklická autokorelačná funkcia* pre $\hat{R}_x^{\alpha}(\tau)$. Idealizovaná *cyklická spektrálna funkcia* môže byť vyjadrená ako Fourierova transformácia nasledovne:

$$S_x^{\alpha}(f) = \int_{-\infty}^{\infty} R_x^{\alpha}(\tau) e^{-j2\pi f\tau} d\tau \tag{2.23}$$

a tiež *limitná cyklická spektrálna funkcia* obdobne:

$$\hat{S}_x^{\alpha}(f) = \int_{-\infty}^{\infty} \hat{R}_x^{\alpha}(\tau) e^{-j2\pi f\tau} d\tau \tag{2.24}$$

Limitná cyklická spektrálna funkcia sa tiež nazýva *spektrálna korelačná funkcia (SCF)*.

Užitočnými variáciami pre cyklickú autokorelačnú funkciu a spektrálnu korelačnú

funkciu sú ich konjugované varianty:

$$R_{x^*}^{\alpha}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} R_x^*(t,\tau) e^{-j2\pi\alpha t} dt \tag{2.25}$$

, kde $R_x^*(t,\tau) = \frac{1}{2N-1} \sum_{n=-N}^{N} x(n+\frac{\tau}{2}) \cdot x(n-\frac{\tau}{2})$, a tiež:

$$S_{x^*}^{\alpha}(f) = \int_{-\infty}^{\infty} \hat{R}_{x^*}^{\alpha}(\tau) e^{-j2\pi f\tau} d\tau \tag{2.26}$$

Pričom pre necyklostacionárny signál platí $R_x^{\alpha}(\tau) = R_{x^*}^{\alpha}(\tau) = S_x^{\alpha}(f) = S_{x^*}^{\alpha}(f) = 0$ pre všetky $\alpha \neq 0$.

Pre cyklostacionárny signál, akákoľvek nenulová hodnota parmetru α, pre ktorú sú konjugované a nekonjugované formy SCF a cyklickej autokorelačnej funkcie tiež rôzne od nuly, je nazývaná *cyklickou frekvenciou.*

Odhad spektrálnej korelačnej funkcie Spektrálnu korelačnú funkciu (SCF) nemôžeme presne vypočítať, keďže nemáme k dispozícii nekonečný signál. Avšak je možné ju aspoň približne určit pre určité cyklické frekvencie na základe dostatočne dlhého signálu.

Pre výpočet SCF môžeme použiť 2 rôzne prístupy:

- *frekvenčné vyhladzovanie* – na základe vzťahu medzi výkonovou spektrálnou hustotou (PSD) a autokoreláciou môžeme priamo z diskrétnej Fourierovej transformácie signálu určiť *periodogram* ako normalizovanú mocninu magnitúdy spektra. Konvolúciou takéhoto periodogramu s oknom o určitej veľkosti (napr. obdĺžnikovým oknom) získame frekvenčne vyhladený periodogram. Pri nahradeni periodogramu jeho cyklickou variantou, kde namiesto mocniny spektra vezmeme jeho verziu ponásobenú komplexne združeným spektrom, získame SCF. Nevýhodou tohoto odhadu je limitácia na jednu cyklickú frekvenciu, Fourierova transformácia dlhého signálu a potenciálne drahá konvolúcia.

- *časové vyhladzovanie* – namiesto priemerovania (vyhladzovania) cyklického periodogramu naprieč spektrálnou frekvenciou sú spriemerované v čase viaceré cyklické periodogramy. Tieto periodogramy sú vypočítané z menších vzorkov signálu, ktoré sa v čase prelínajú.

Vzhľadom na menšiu výpočetnú náročnosť volíme časové vyhladzovanie, kde jednou z výpočetných techník je *metóda akumulácie FFT (FFT accumulation method, FAM)* [13].

FAM umožňuje vypočítať veľký počet bodových odhadov SCF pomocou [14]:

$$S_{xy_T}^{\alpha_i+q\Delta\alpha}(rL, f_j)_{\Delta t} = \sum_r X_T(rL, f_k) Y_T^*(rL, f_l) g_c(n-r) e^{-i2\pi rq/P} \tag{2.27}$$

, kde $g_c(n)$ predstavuje jednotkový obdĺžnikový pulz (okenná funkcia) a X_T (a Y_T, v našom prípade zhodné s X_T) sú komplexné demoduláty dané ako:

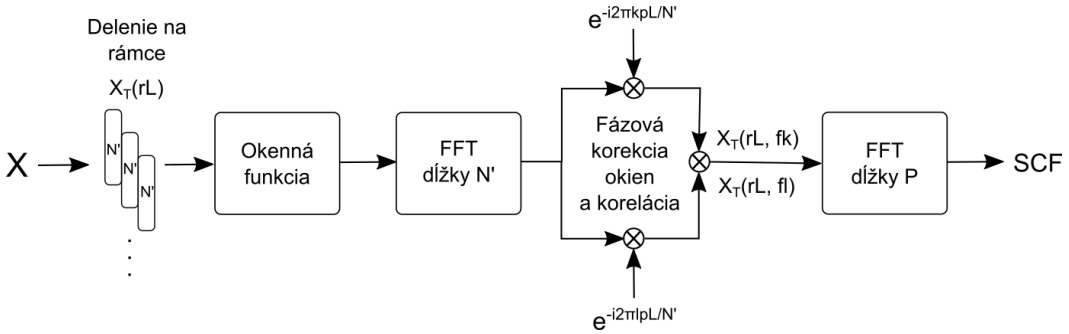
$$X_T(n, f) = \sum_{-N'/2}^{N'/2-1} a(r) x(n-r) e^{-i2\pi f(n-r)T_s} \tag{2.28}$$

V tejto funkcii $a(r)$ opäť predstavuje okennú funkciu, typicky Hammingovo okno, ktoré zmierňuje skokové okraje signálu $x(n-r)$ pri výpočte spektra.

Signál je vzorkovaný vzorkovacou frekvenciou $f_s = 1/T_s$, $T = N'T_s$ je dĺžka okna $a(r)$ a dĺžka okna $g_c(n-r)$ je NT_s, čo zároveň predstavuje dĺžku vstupného signálu.

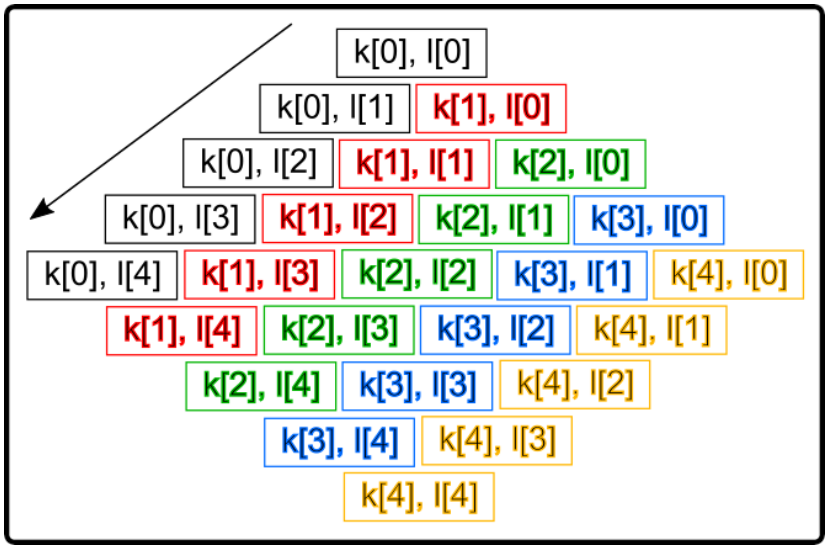
To znamená, že FAM rozdeľuje vstupný signál na rámce o veľkosti N', pričom posun medzi rámcami je L, takže rámce sa prekrývajú (typicky používaná hodnota prekryvu je $L = N'/4$). Vznikne $P = N/L$ rámcov, ktoré sú vstupom do DFT a výsledok je fázovo upravený vzhľadom k prvému (počiatočnému) rámcu. Každý z rámcov je následne postupne násobený so všetkými P rámcami, ktoré sú konjugované (korelácia). Výsledok každého násobenia o dĺžke P je opäť vstupom do DFT. Vzniknutý tenzor o veľkosti $N' \times N' \times P$ je následne potrebné preorganizovať do $(2 \times N' - 1)$ riadkov SCF, a to tak, že magnitúda každeho výsledku DFT je postupne vkladaná do riadkov pod sebou s odostupom $2 * N/N'$ a to tak, aby tvorili diagonálu smerom k ľavému okraju SCF. Rámce na rovnakom riadku sa prekrývajú o N/N'.

Situáciu je možné ilustrovať pomocou diagramu na obrázku 2.5 a schémy na obrázku 2.6.



Obrázek 2.5 Sekvenčný diagram výpočtu SCF [13].

Diagram SCF, ktorý je výsledkom metódy FAM, dáva do vzájomného vzťahu normalizovanú cyklickú frekvenciu (rozsah -1 až 1) a spektrálnu frekvenciu signálu (tiež normalizovanú do rozsahu -0,5 až 0,5).

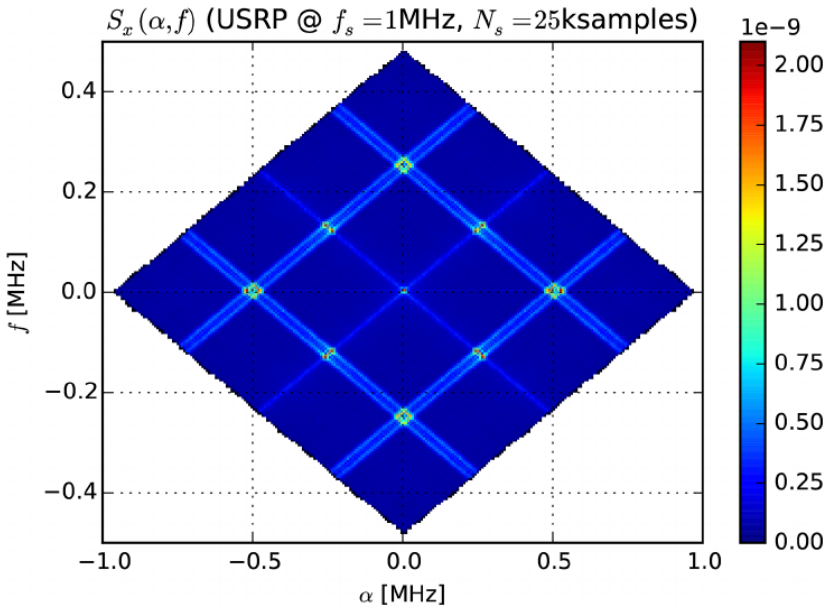


Obrázek 2.6 Schéma organizácie SCF diagramu.

Rozlíšenie cyklickej frekvencie je dané ako:

$$\Delta\alpha = 1/N \tag{2.29}$$

Ukážku diagramu SCF je možné vidieť na obrázku 2.7.



Obrázek 2.7 Diagram SCF [15].

Metóda FAM je veľmi výpočetne náročná, avšak je možné urobiť isté kroky pre jej zjednodušenie za cenu straty presnosti. Namiesto ukladania jednotlivých rámcov môžeme vziať len ich priemer za cenu zníženia rozlíšenia. A následne môžeme vynechať výpočet sekundárnej FFT, vzhľadom na to, že zaberá podstatnú časť času (počíta sa

pre $N' \times N'$ rámcov o veľkosti P), a to že priemer hodôt pred a po vstupe do FFT je rovnaký.

Následne, ak namiesto preskupovania jednotlivých bodov do SCF zachováme tvar matice po výpočte korelácií a len spriemerujeme vypočítané hodnoty jednotlivých korelácií, dostaneme hrubý odhad SCF otočený o 45° vzhľadom k diagramu SCF.

Analýza SCF je značne zložitá, rôzne typy signálov vykazujú rôzne vzory v diagrame na základe svojich vlastností. Takáto analýza testovacích je ukázaná v praktickej časti.

2.5 Štandardné rádiové komponenty

V priebehu vývoja rádiotechniky došlo k ustáleniu komponentov potrebných k príjaniu či vysielaniu rádiových signálov. Tieto komponenty môžu byť v praxi implementované rôznym spôsobom, ale úloha každej z nich je z pohľadu systému stanovená tak ako popisujú jednotlivé časti nasledovnej kapitoly.

Pred uvedením jednotlivých komponentov je však vhodné upresniť čoho chceme dosiahnuť.

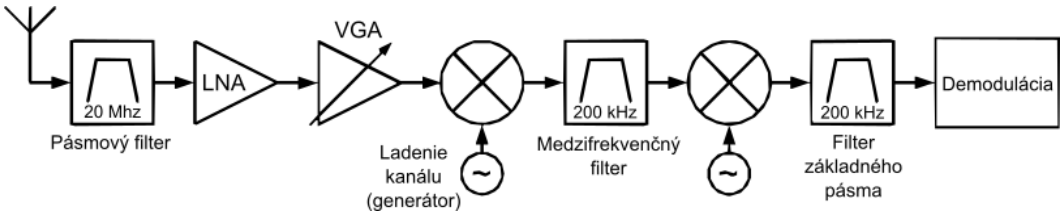
Vysielanie má za cieľ umožniť prenost informácie modulovaním nosnej elektromagnetickej vlny. Frekvencia nosnej vlny (RF) bývá často omnoho vyššia (napr. 2,4 GHz) ako frekvencia informácie (základné pásmo, baseband, BB; frekvencia napr. 20 – 40 MHz). Dôvod použitia tejto nosnej frekvencie je, že takto vyslaná vlna sa lepšie šíri priestorom, vyžaduje menší vyžiarený výkon. Zároveň je možné naladiť príjmač na jednu frekvenciu príjmu a používať rôzne frekvencie základného pásma.

Vysielanie vyžaduje kvalitnú vysielaciu anténu a vyšší výkon ako pri prijme, aby elektromagnetická vlna bola schopná vybudiť vzdialenú anténu príjmača. Často bývajú vysielacie antény obrovské (v minulosti celé budovy), aby pokryli čo možno najväčšiu oblasť (terestriálne vysielanie televízie a rádia).

Príjem sa snaží z fyzického média extrahovať a zdigitalizovať cieľový signál s čo možno najväčším možným ziskom dát pri čo najmenšej miere šumu. Túto úlohu komplikujú rôzne interferujúce signály z okolia, nedokonalosti prijímacích komponentov a tiež útlm signálu so vzdialenosťou od vysielača a skrze prekážky. S ohľadom na tieto úskalia je vhodné mať čo najlepšie naladený systém na cieľovú frekvenciu. Nasledujúce odseky popisujú jednotlivé súčasti a ako je u nich možné dosiahnuť čo najlepších výsledkov príjmu. O každej komponente by bolo možné písať rozsiahlu knihu, a preto s ohľadom na rozsah práce sú popísané naozaj stručne.

Je tiež dôležité dodať, že poradie prvkov ako je popísané v nasledujúcich odstavcoch nie je nevyhnutné (z výnimkou antény pre príjem) a často bývajú niektoré prvky

obsiahnuté na viacerých úrovniach príjmu signálu.



Obrázek 2.8 Štandardné komponenty potrebné k rádiovému príjmu[16].

2.5.1 Anténa

Anténou je každý elektrický vodič, v ktorom:

- pri príjme – vplyvom elektrickej zložky elektromagnetického žiarenia vzniká napätie. Napätie spôsobí tok elektrónov v smere okamžitého elektrického poľa, čim vzniká vo vodiči prúd. Takto indukovaný prúd sa odráža na konci vodiča a je reflektovaný opačným smerom. Je tak vytvorená prúdová vlna. Prúd vytvára kmitanie vo vodiči a je možné ho zachytiť a ďalej spracovať. Pri správnom nastavení veľkosti vodiča je možné synchronizovať už existujúcu kmitanie vo vodiči s aktuálne príjmaným signálom a prechádzajúci elektrický prúd tak zosilniť.
- pri vysielaní – vplyvom premenlivého kmitajúceho elektrického prúdu vzniká elektromagnetické žiarenie vyžarované do okolia.

Vhodná dĺžka antény súvisí s dĺžkou vlny elektromagnetického žiarenia. Vzhľadom na to, že jedna perióda vlny elektromagnetického žiarenia vyvoláva pozitívny i negatívny potenciál, je vhodné rozdeliť vodič na 2 polovice (pozitívna a negatívna, ktoré sa periodicky striedajú). Zároveň, jedna polvlna (sínusovej vlny) je symetrická a preto pre maximálne zosílenie je vhodné voliť vodič polovičnej dĺžky, t.j. 1/4 dĺžky elektromagnetickej vlny. Takáto anténa sa nazýva *dipól* (2 póly a 1/4 dĺžke vlny) a zaručuje optimálny príjem pri správnom nasmerovaní antény voči vysielaču, t.j. kolmo na vysielač. V prípade potreby je možné anténu zjednodušiť a využiť len jednu polvlnu. Takáto anténa je nazývaná *monopól*.

Na kvalitu signálu nemá žiaden iný prvok taký vplyv ako anténa. Výberom vhodného typu antény je možné podstatne zlepšiť odstup od šumu a zároveň poskytnúť ďalším prvkom v sústave kvalitnejší vstup. Výber vhodnej antény tak patrí i v dnešnej dobe k jednému z prvých najdôležitejších krokov pri návrhu rádiového systému.

Antény môžeme deliť podľa:

- **príjmaných vlnových dĺžok** - jedná sa o úsek spektra, na ktorý sa daná anténa zameriava, keďže nie je možné jednou anténou zachytiť celé elektromagnetické spektrum v rozumnej kvalite

  - úzkopásmové - zameriavajú sa na zachytávanie úzkeho pásma z cieľom maximalizovať zisk signálu a vyrušenie nežiadúcych (často blízkych) okolitých frekvencií
  - širokopásmové - zameriavajú sa na naladenie širšieho úseku spektra s možnosťou výberu žiadaného pásma flexibilne podľa potreby

- **smerovosti** - zameranie antény na príjem signálov len z určitého smeru
  - všesmerové - príjmajú signály zo všetkých strán, praktické hlavne u zariadení používaných v pohybe (v dopravných prostriedkoch, pri chôdzi, a pod.)
  - smerové - príjmajú signál z určitého smeru a zabraňujú rušeniu z iných smerov, vhodné hlavne na statickú inštaláciu

- **typu** - konštrukčne rôzne riešené antény, typicky podľa vzdialenosti k vysielaču, jeho vlastností a podľa prostredia, v ktorom nastáva príjem
  - prútové - základná všesmerová anténa použiteľná obecne u rôznych typov príjmačov (i prenosných), napr. u autorádií, domácich bezdrôtových sieťových smerovačov, vo vysielačkách, a pod.
  - parabolické - vysoko smerové antény, používané typicky staticky, pre zachytenie slabých satelitných signálov
  - Yagi-Uda - smerová anténa používaná pre príjem VHF pásma, využíva (konštruktívnu i deštruktívnu) interferenciu pre dosiahnutie väčšieho zisku signálu z určitého smeru
  - a ďalšie špecifické typy

- **polarizácie** - umožňuje do istej miery redukovať šum spôsobený odrazom
  - lineárne polarizované - horizontálne/vertikálne, prevážne rádiové a televízne vysielanie šíriace sa krajinou
  - kruhovo / elipticky polarizované - ľavotočivé/pravotočivé, využívané u satelitného vysielania, keďže je odolnejšia pri prechode atmosférou

- **smeru vysielania**
  - vysielacie - typicky napr. veľké vysielače poskytujúce rozhlasové a televízne vysielanie smerom k obyvateľstvu, zároveň i satelitné vysielače
  - príjmacie - napr. parabolické antény pre satelitný príjem
  - vysielacie i príjmacie zároveň - antény používané v modernej domácej elektronike ako napr. bezdrôtové smerovače, mobilné telefóny a pod.

Táto práca sa bude orientovať prevažne na bežne používané technológie pre geograficky lokálnu komunikáciu s krátkym dosahom, t.z. výber antén bude nasledovať tento trend a skôr sa zamerá na kompaktné a ľahko prenosné prútové antény.

2.5.2 Zosilovač signálu

Analógový signál zachytený anténou je obecne veľmi slabý pre priamy prevod na digitálny signál, či akékoľvek ďalšie spracovanie. Obdobne je tomu i u vysielania, kedy generovaný signál vyžaduje zosílenie pre úspešný prenos.

Podstatným problémom pri zosílení je prítomnosť šumu. Signál zachytený anténou už obsahuje istý šum. Či už je to šum spôsobený vplyvom okolia cieľovej frekvencie, alebo šum získaný silným rušivým vysielačom v okolí. Často však býva zdrojom šumu samotný príjmač (či vysielač), jeho rôzne elektronické komponenty, ako cievky a zdroje, môžu vnášať do príjmu svoj vlastný šum. Preto je dôležitá správna konštrukcia celého obvodu s ohľadom na zabránenie propagácie takéhoto šumu do signálu.

Šum získaný pri príjme anténou z okolia je takmer nemožné odstrániť, avšak je podstatné, aby zosilovač zachovával odostup šumu od signálu pri zosilovaní a aby nepridával ďalší šum už do skresleného signálu.

U SDR býva hneď jedym z prvých prvkov príjmu *zosilovač s nízkym šumom (LNA)*, ktorý umožňuje podstatne zlepšiť kvalitu signálu pred jeho spracovaním do digitálnej podoby. Typicky je realizovaný tranzistormi s prepojovacím účinkom (JFETs) alebo vysokou pohyblivosťou elektrónov (HEMTs), ktoré poskytujú vysoké zosilnenie. Zároveň sú riadené v móde vysokého prúdu, čo je málo energeticky účinné, ale zato redukuje skokový šum. Tieto tranzistory sú typicky doplnené o ďalšie prvky, špeciálne navrhnuté pre prácu s frekvenciami v nízkom, či vysokom pásme.

Ďalším typom zosilovača je *transimpedančný zosilovač*. Tento typ zosilovača využíva operačných zosilovačov, ktoré zachovávajú linearitu signálu a vnášajú minimálny šum pri zosilnení. Zvlášt účinné sú pri potlačení silného vysielača v blízkosti príjmaného pásma.

Tieto zosilovače sú používané na viacerých úrovniach príjmu, typicky po prevode do frekvencie ızákladného pásma a ďalej po prechode signálu rôznymi filtrami, typicky filtrami šumu.

2.5.3 Generátor

Generátor je prvok umožňujúci vytvárať pravidelné oscilácie na určitej frekvencii. Je tak možné vytvoriť signál, ktorý môže slúžiť ako:

- nosná vlna – slúžiť k vytvoreniu modulovaného signálu pri prenose. U generáto-

rov je veľmi dôležité zachovanie presnosti u vlastností generovanej vlny a to aj vzhľadom na zmeny prostredia (napr. teplota), či zmena vysielacieho výkonu.

- referenčná vlna – umožňuje demodulátoru extrahovať prenášaný signál z nosnej vlny, ktorá je na rovnakej frekvencii ako nastavená referenčna vlna.

V prípade potreby je možné pomocou generátorov vytvárať i zložitejšie signály. V prípade rádiového vysielania sa však jedná hlavne o presnosť a stability daného generátoru. Generátory signálov sú závislé na oscilačnom prvku s pravidelnou frekvenciou, ktorým môže byť napr. kryštál, a vyžadujú kalibráciu pre zredukovanie odchylky od požadovaného signálu na minimum.

2.5.4 Modulátor / Demodulátor

Modulátor je prvok zabezpečujúci zmenu elektromagnetickej vlny podľa prenášanej informácie. Táto zmena sa nazýva *moduláciou* a existujú rôzne základné formy takejto modulácie, ktoré menia určitú vlastnosť elektromagnetickej vlny, viď sekcia 2.4.

V moderných komunikačných prostriedkoch može byť používaných viacero modulačných techník naraz na dosiahnutie maximálneho využitia pásma.

Naopak *demodulátor* umožňuje z prijatého signálu získať pôvodnú informáciu, za predpokladu, že je známa použitá forma modulácie.

2.5.5 Filter šumu

Ako už zaznelo v predchádzajúcom odstavci, šum je prirodzene obsiahnutý v signáli v rôznych formách. Jeho prítomnosť je nežiadúca, a preto existujú rôzne formy je filtrácie zo signálu.

Najčastejším spôsobom filtrácie býva *dolná priepusť*, ktorá súvisí s faktom, že signál obsahuje prevažne frekvencie nižšie ako najvyššia možná a šum sa vďaka svojej náhodnej povahe prejavuje rýchlymi zmenami a teda vysokou frekvenciou. Z tohoto vyplýva, že vysokofrekvenčná zložka signálu obsahuje prevažne šum a je tak pre ďalšie použitie bezcenná a môže byť odfiltrovaná vhodne navrhnutým filtrom.

Šumom však nemusí byť len šumové pozadie, ale v prípade ladenia signálu v úzkom spektre frekvencií môže iná zložka spektra, so silnejším signálom, potlačiť žiadaný signál. Preto je dôležité odfiltrovať všetky zložky spektra mimo žiadané pásmo.

Použitím filtra analógového k dolnej priepusti, t.z. *horná priepusť* filtrujúca frekvencie nižšie než je požadovaná, a kombináciou s dolnou priepusťou je vytvorený *pásmový filter*, ktorý mnohonásobne zlepšuje príjem.

3 SOFTWARE DEFINED RADIO

Software defined radio (SDR) alebo tiež softvérovo definované rádio je rádiový systém, ktorého časti typicky realizované hardvérovými prvkami sú nahradené softvérom. Typicky sa jedná o prvky, ktoré boli v minulosti realizované analógovými prvkami (cievky, tranzistory, a pod.), napríklad ako filtre šumu, zosilovače, frekvenčné zmiešavače, modulátory a demodulátory, či ich súčasti. Koncept SDR existuje už od prvých dôb spracovania signálov číslicovými systémami, avšak až v poslednej dobe dosiahla technika dostatočnej úrovne na plnohodnotné spracovanie a manipuláciu signálov v softvéri v reálnom čase.

Definícia SDR je cielene veľmi obecná a jej formulácia sa líši medzi rôznymi zdrojmi. Dôležitým zdieľaným prvkom je jednoduchosť úpravy rádiového vysielania či príjmania len pomocou zmeny softvéru bez potreby úpravy platformy, na ktorej SDR operuje. Ultimátnym cieľom je dosiahnutie takých možností SDR, aby bolo možné vysielať na ľubovoľnej frekvencii, s ľubovoľnou moduláciou, šírkou pásma, či preniesť ľubovoľný dátový tok[17].

3.1 História SDR

Termín *softvérové rádio* bol vytvorený Josephom Mitola III, aby ukázal odklon od hardvérovo založených rádiových systémov k systémom, kde prevažuje softvér.

Vývoj SDR staval na postupnom rozvoji rôznych hardvérových komponentov, a to hlavne analógovo-digitálnych (ADC) a digitálno-analógových prevodníkov (DAC), digitálnych signálnych procesorov (DSP), programovateľných hradlových polí (FPGA) a procesoroch s obecným použitím.

Hlavný dopyt po jednoducho rekonfigurovateľnom rádiovom systéme prišiel zo strany armády, ktorá vyžadovala systém umožňujúci komunikovať s viacerými používanými technológiami, od satelitnej komunikácie, cez vzdušnú až po pozemnú, s použitím jednotného zariadenia. Zároveň je vyžadovaná istá miera udržateľnosť zariadení, ktoré majú oveľa dlhší životný cyklus ako spotrebná technika. Poslednou výhodou je možnosť preniesť existujúci funkčný systém zo staršej platformy na novší hardvér bez potreby zložitých úprav. Tieto výhody viedli k vývoju SDR vrámci viacerých programov rôznych svetových armád (za všetky napr. SpeakEasy I/II, JTRS, či ESSOR)[17].

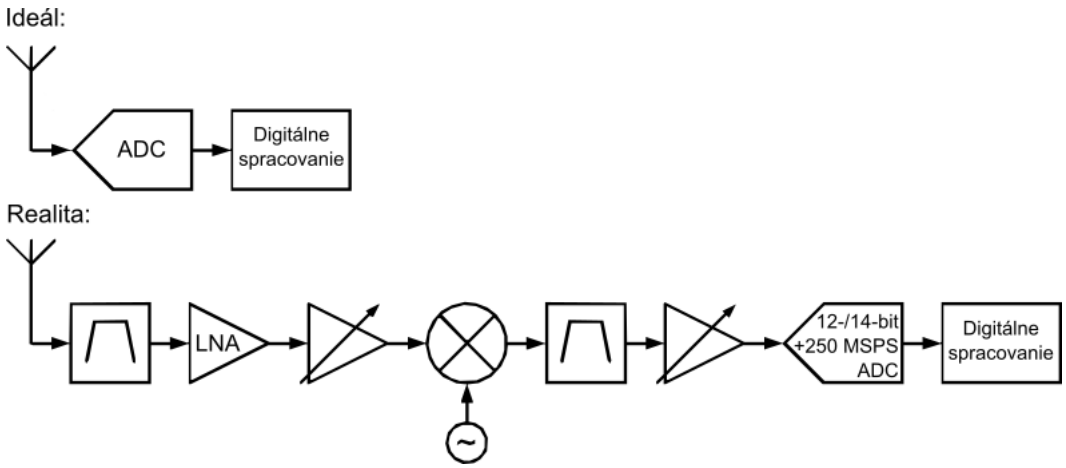
Motiváciou v privátnom sektore je hlavne rýchly a flexibilný vývoj nových bezdrôtových štandardov a, obdobne ako u armády, jednoduchý upgrade existujúceho hardvér na tieto štandardy.

V súčasnej dobe presakuje použitie SDR i medzi jednotlivcov vďaka cenovej dostupnosti, a to ako komponentov SDR, tak i celých SDR riešení. Zo začiatku boli nadšencami

a rádioamatérmi používané zvukové karty počítačov, ktoré obsahovali ADC a DAC s rozumnou presnosťou[18]. Ich zameranie na spracovanie audia však obedzovalo spracovávaný rozsah frekvencií, čo značne limitovalo ich použitie. Veľký boom využívania SDR nastal s nástupom väčšej integrácie týchto obvodov a ich zlacnenie. Spočiatku išlo o zaujímavé hračky ako RTL DVB-T adaptér, modifikovateľný pre SDR použitie, či rad1o Badge k CCCamp 2015, z ktorého sa časom vyvinul HackRF SDR. Dnes existujú sofistikované riešenia použiteľné ako profesionálmi, tak i laickou verejnosťou, najmä vďaka bohatej komunite, ktorá sa stará o vývoj softvéru i hardvéru.

3.2 Komponenty SDR

Ako každý rádiový systém i SDR obsahuje základné komponenty. Na rozdiel od klasických (analógových) systémov je však väčšinu implementovaná v softvéri. To znamená, že analógový signál získaný anténou je v takmer nezmenenej podobe prevádzaný na digitálny a ďalšie manipulácie už prebiehajú v digitálnej rovine. Avšak z fyzikálneho hľadiska nemá ADC nekonečný dynamický rozsah a ani nekonečnú vstupnú šírku pásma, preto je stále potrebné vstupný signál predfiltrovať, aby ho bolo možné využiteľne previesť na digitálny signál, viď 3.1.



Obrázek 3.1 Komponenty SDR a spracovanie rádiového príjmu[16].

Analógovo-digitálny prevodník je preto základnou a jednou z najdôležitejších častí SDR. Vyžaduje vysokú presnosť a odolnosť. Na rozdiel od klasických rádiových systémov prevádza modulovaný signál priamo do digitálnej podoby bez potreby prevodu do medzifrekvencie. V digitálnej podobe je možné vzorkovaný signál ďalej ľubovoľne upravovať. ADC je typicky súčasťou komplexnejšieho system-on-a-chip (SoC) riešenia, ktoré zahŕnuje napr. konfigurovateľný zosilovač, či rôzne filtre (napr. vstupný pásmový filter)[8].

Programovateľné hradlové pole je cenným prvkom najmä pri návrhu nových štandardov rádiovej komunikácie. Umožňuje vytvorenie takmer akéhokoľvek hardvérového prvku bez potreby fyzickej zmeny platformy. Zároveň je takto doplnená súčasť rýchlosťou veľmi blízka skutočnému hardvéru. Jediným limitujúcim faktorom FPGA je počet obsiahnutých hradiel.

Digitálny signálový procesor môže byť dedikovaným prvkom, súčasťou SoC, implementovaný na FPGA alebo len čisto v softvéri vďaka vysokej rýchlosti moderných procesorov. Umožňuje rýchlu filtráciu signálu a jeho predspracovanie pred cieľovou operáciou, čo môže byť vizualizácia, analýza, či spätné vysielanie.

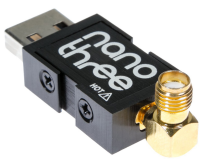
3.3 Súčasný stav SDR

Moderné SDR platformy ponúkajú omnoho viac možností ako ich predchodcovia. V provom rade poskytujú možnosť spracovávania oveľa väčších frekvenčných rozsahov, sú kompaktnejšie, často obsahujú FPGA modul, ktorý umožňuje rapídne spracovanie signálu, a v neposlednej rade sú energeticky nenáročné, takže je možné ich používať i vrámci prenosných zariadení v teréne. Vlastnosti vybraných SDR platforiem sú zhrnuté v tabuľke 3.1.

Nasledujúce odstavce bližšie popisujú jednotlivé platformy.

3.3.1 RTL SDR

RTL SDR je široká rodina zariadení založených na čipe RTL2832U, pôvodne slúžiaca ako DVB-T príjmač pre PC [19]. Čip posiela zachytené I/Q vzorky signálu priamo do pripojeného zariadenia, čo umožňuje ich jednoduché spracovanie. Od roku 2012, kedy bola objavená táto vlastnosť, sa rozšírilo množstvo zariadení používajúcich tento čip a stali sa veľmi populárnymi.



Obrázek 3.2
NooElec NESDR
Nano 3 RTL
SDR

RTL SDR je jediné spomenuté zariadenie, ktoré nepodporuje vysielanie a jeho frekvenčný rozsah je užší než u iných SDR. Tento nedostatok však vyvažuje svojou kom-

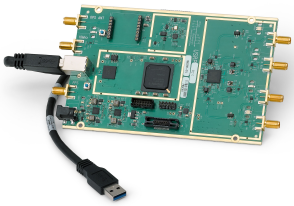
	USRP B2x0	**HackRF**	**bladeRF**	**LimeSDR**	**Pluto SDR**	**RTL-SDR**	**XTRX**
Rozsah ladenia	70 MHz - 6 GHz	1 Mhz - 6 GHz	300 MHz - 3.8 GHz	30 MHz - 3.8 GHz	325 MHz - 3.8 GHz (70 MHz - 6 GHz, hack)	22 MHz - 2.2 GHz	30 MHz - 3.7 GHz
Duplex	MIMO	½ SISO	SISO	MIMO	SISO	Len príjem	MIMO
Max. vzorkovacia frekvencia	61.44 MSPS	22 MSPS	40 MSPS	61.44 MSPS	61.44 MSPS	3.2 MSPS	120 MSPS SISO / 90 MSPS MIMO
ADC/DAC rozlíšenie	12-bit	8-bit	12-bit	12-bit	12-bit	8-bit	12-bit
Max. šírka pásma	56 MHz	20 MHz	28 MHz	61.44 MHz	20 Mhz (56 MHz, hack)	3.2 MHz	120 MHz
Počet kanálov	1 (2 for B210)	1	1	2	1	1	2
Vysielací výkon	10dBm+	až 15dBm (frekv. závislé)	6dBm	0 až 10dBm (frekv. závislé)	7 až 9dBm (frekv. závislé)	N/A	0 až 10dBm (frekv. závislé)
RF obvod	AD9364 / AD9361	MAX5864	LMS6002D	LMS7002M	AD9363	RTL2832U	LMS7002M
Embedded	nie	nie	nie	nie	nie	nie	áno
Teplotné senzory	nie	nie	nie	áno	nie	nie	áno
Frekvenčná stab.	±2 ppm	±20 ppm	±1 ppm	±2.5 ppm	±25 ppm	±25 ppm	±0.5 ppm, <±0.01 ppm s GPS
GPS synchron.	cez doplnok	nie	nie	nie	nie	nie	vstavaná
Zbernica	USB 3	USB 2	USB 3	USB 3	USB 2	USB 2	PCIe x2, USB 3 adapt. a viac (skrze FPGA)
Teoret. priepust. zbernice	5 Gbit/s	480 Mbit/s	5 Gbit/s	5 Gbit/s	480 Mbit/s	480 Mbit/s	10 Gbit/s
Rozmery	97 x 155 mm	124 x 80 mm	87 x 131 mm	100 x 60 mm	170 x 120 mm	40 x 60 mm	30 x 51 mm
Doplnkové vlast.	GPIO	GPIO	GPIO	GPIO	žiadne	žiadne	GPIO, GPS, rozhranie pre SIM

Tabulka 3.1 Porovnanie SDR platforiem [20][21]

paktnosťou a jednoduchou prenositeľnosťou, čo z neho robí ideálne zariadenie pre sledovanie rádiových frekvencií v teréne.

3.3.2 USRP a Pluto SDR

Široké spektrum zariadení Universal Software Radio Peripheral (USRP) od spoločnosti Ettus Research sa zameriava prevažne na profesionálov či priemyselné použitie. Tomu odpovedá i cenová kategória, kedy väčšina zariadení presahuje cenu dostupnú amatérskym užívateľom. USRP má modulárnu architektúru, kde je oddelená RF doska od výpočetnej dosky, čo umožňuje jednoduchšiu výmenu či upgrade. Výhodou USRP je tiež množstvo nástrojov, ktoré sú dodávané spolu s USRP zariadeniami, kvalita prevedenia a podpora.



Obrázek 3.3 Ettus USRP B210

Obrázek 3.4 Adalm Pluto SDR

Lacnejšou variantou je Pluto SDR priamo od spoločnosti Analog Devices, výrobcu ADC pre USRP. Toto zariadenie je určené predovšetkým ako vývojový kit a edukačná platforma, preto neposkytuje rozsiahle možnosti USRP. Avšak vďaka objavenému hacku, ktoré využíva fakt, že použité ADC AD9363 je prakticky totožné s výkonnejším AD9364, je možné rozšíriť možnosti AD9363 na úroveň AD9364 jednoduchou úpravou parametrov čipu. Tento trik robí z Pluto SDR cenný nástroj, avšak oproti svojim drahším konkurentom zaostáva vo frekvenčnej stabilite, rýchlosti zbernice a obsahuje len jeden kanál.

3.3.3 HackRF One

HackRF One je vývojové pokračovanie rad1o SDR z CCCamp 2015 kempu pre hackerov. Napriek relatívne obmedzenému hardvéru má stále veľmi veľkú podporu v komunite, ktorá rozvíja zaujímavé schopnosti tohoto zariadenia, ako napr. sweep funkcionalitu vďaka ktorej je možné v rýchlom slede ladení získať prehľad o celom spektre. Cenová dostupnosť zariadenia je veľmi priaznivá, a zároveň použité ADC MAX5864 je veľmi energeticky úsporné, vďaka čomu je možné ho ľahko použiť v teréne. Na druhú stranu je HackRF One už pomerne zastaralé a očakáva sa uvedenie nástupcu.

Obrázek 3.5 Great Scott Gadgets HackRF One

PortaPack H1/2 je nadstavba pre HackRF One, ktorá umožňuje jednoduché použitie HackRF v teréne. Pomocou displeja a ovládacích prvkov je možné sledovať vybrané pásmo, dekódovať isté typy signálov, vysielať kódované signály vybraných typov, zaznamenávať a neskôr znovu vysielať signály, a mnoho ďalšieho. Zariadenie je plne prenosné a až na obmedzený výpočetný výkon poskytuje veľmi užitočný prehľad o okolitom RF signále a umožňuje prevádzať i niektoré typy útokov.

Obrázek 3.6 PortaPack H2

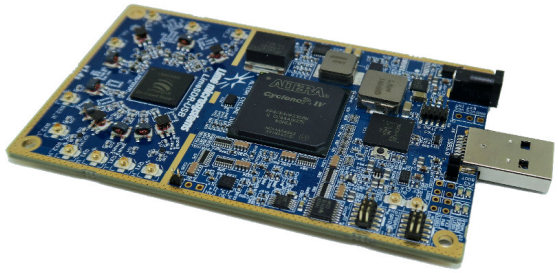
3.3.4 bladeRF a LimeSDR

Zariadenia bladeRF a LimeSDR sú postavené na ADC od spoločnosti Lime Microsystems. Táto spoločnosť sa zameriava hlavne na SDR, ktoré ponúka pre priemyselné použitie.

bladeRF od spoločnosti Nuand využíva staršie ADC LMS6002D, ktoré ako prvé

intergrovalo kompletný programovateľný RF transciever (prímač i vysielač) na jednom čipe. bladeRF je plnohodnotné SDR s Intel Altera Cyclone IV FPGA, ktoré vďaka vysokému počtu hradiel umožňuje implementovať i komplikované rádiové stacky ako napr. WiFi štandard. Spoločnosť Nuand toto podporuje vývojom bladeRF-wiphy HDL implementácie.

LimeSDR je voľným pokračovaním, vytvoreným priamo firmou Lime Microsystems, ktoré používa novšiu iteráciu ADC LMS7002M. Tá umožňuje pokryť väčšiu šírku pásma, poskytuje viac kanálov a operuje s väčšou vzorkovacou frekvenciou.



Obrázek 3.7 Lime Microsystems LimeSDR

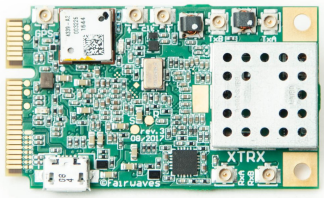
3.3.5 XTRX

XTRX od spoločnosti Fairwaves je jedným z prvých zariadení v dostupnej cenovej kategórii, ktoré je embedovateľné. Je to husto integrovaná doska s miniPCIe rozhraním, ktorá poskytuje PCIe x2 2.0 rýchlosti prenosu. XTRX využíva rovnaké ADC LMS7002M ako LimeSDR, využíva Xilinx Artix FPGA, GPS modul pre presnú synchronizáciu hodinového signálu a mnoho ďalšieho.

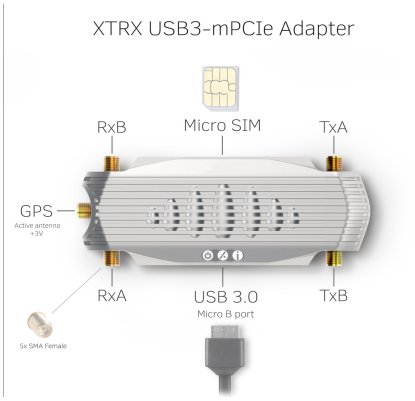
Formát miniPCI je navyše vysoko kompaktný a umožňuje ľahké zapojenie do rôznych systémov. XTRX je dodávané spolu s USB 3 adaptérom, ktorý je vhodný pre použitie vo fáze prototypovania. S určitými úpravami je možné XTRX použiť i pre analýzu HF pásma.

Spoločnosť Fairwaves bola od uvedenia XTRX včlenená do Lime Microsystems, ktorá prevzala ďalší vývoj XTRX a aktuálne ponúka v predpredaji LimeSDR XTRX, ktorá je zmodernizovaným modelom XTRX a vďaka podpore výrobcu ADC vyhlasuje, že bude dosahovať lepších výsledkov ako XTRX.

XTRX je bežne používané zariadenie pre komerčné účely, napr. spoločnosťou Vo-



Obrázek 3.8 Fairwaves XTRX



Obrázek 3.9 XTRX USB 3 adaptér

dafone vyvinutý prototyp umožňuje vytvoriť extrémne lacnú lokálnu stanicu pre 5G prenos použiteľnú napríklad ako privátnu podnikovú bezdrôtovú sieť.

4 BEZPEČNOSŤ RÁDIOVÝCH SYSTÉMOV

Vzhľadom k povahe rádiového signálu je takmer nemožné zabrániť jeho odposluchu. U zariadení umiestnených v prostredí s hustou populáciou je navyše zložité, ak nie nemožné, dopátrať páchateľa bezdrôtového útoku, a to za predpokladu, že zariadenie útočníka nevykonáva útok automaticky bez jeho prítomnosti.

Preto je nutné bezdrotové zariadenia ochrániť pred celým spektrom útokov popisovaných v nasledujúcom odstavci.

4.1 Typy útokov

Napriek fyzickej nedostupnosti na cieľové zariadenie je súbor možných útokov na bezdrôtové zariadenia naozaj obsiahly [22]. Mnoho z uvedených útokov je založených na útokoch aplikovaných na klasické "drôtové siete". Útoky sa vždy snažia ohroziť jeden zo základných pilierov bezpečnosti – súkromie, dostupnosť alebo integritu cieľa.

Sniffing je metódou, pri ktorej SDR "počúva" a zachytáva cieľový signál a útoči tak na *súkromie* správ posielaných bezdrôtovým kanálom. Pritom plne nezáleží na tom, či je správa šifrovaná alebo nie, pretože okrem obsahu správy je možné získať ďalšie cenné dáta ako: identitu odosieľateľa a príjemcu, časové značky spojené s prenosom, úroveň intenzity signálu (korelujúcu so vzdialenosťou od vysielača), typ modulácie, použité frekvenčné pásmo, a pod.

Side-channel útok je metóda zbierajúca a analyzujúca údaje o fyzických parametroch prenosového hardvéru, napr. ako šum alebo vyžiarený výkon, ktoré sú vysielané integrovanými obvodmi počas spracovávania operácií súvisiacich s cieľom útoku.

Jamming je útok typu DoS (denial of service), ktorý môže nadobúdať dvoch podôb – buď je cieľové zariadenie zahrnuté nadmierou žiadostí, ktoré v rámci použitého protokolu potrebuje spracovať (či už odmietnuť alebo prijať). Alebo sa jedná o prehlušenie rádiovej komunikácie pomocou generovania silného rušivého šumového signálu na komunikačnom kanále (či kanáloch). Tento útok cieli na *dostupnosť* služieb poskytovaných cieľovým zariadením.

Spoofing operuje na základe využitia vlastností komunikačného protokolu. Umožňuje vytvoriť chybový avšak stále valídny signál vysielaný z SDR smerom k cieľovému zariadeniu. Použitím chybového signálu je ďalej možné "prepašovať" do cieľa chybové dáta alebo dokonca škodlivý kód pre čiastočné, či plné ovládnutie cieľového zariadenia

s cieľom zasiahnuť jeho výkonnosť, ovplyvniť prenos dát, alebo umožniť použitie iných typov útoku. Tento typ útoku primárne cieli na *integritu* cieľa.

Replay útok zachytáva valídnu komunikáciu, kopíruje ju a preposiela ju späť. Umožňuje tak útočníkovi stať sa legitímnym (podvrhnutým) účastníkom komunikácie, narúšať korektný sled komunikácie, spôsobovať flooding či jamming, alebo jednoducho opakovať zachytené správy. Jedná sa o útok na *integritu*, keďže pri správne prevedenom útoku cieľ nedokáže rozpoznať správy od útočníka od správ od legitímneho účastníka komunikácie.

Flood útok je typ DDoS (distributed denial of service) útoku s cieľom zanechať zariadenie nedostupné pre oprávnenú komunikáciu tým, že sú zahltené dostupné (komunikačné či výpočetné) prostriedky cieľa. Tento útok má za cieľ *dostupnosť*.

Re-injection útok je podobný "Replay" útoku s rozdielom, že správy sú upravované pred odosielaním späť. Tým narušuje *integritu* a *súkromie* prenosu.

Jedným s využití tohoto typu útoku v kombinácii s jammingom je tzv. *rolljam* útok [23]. Tento útok je použiteľný na diaľkové ovládania starších áut. Princípom ochrany je pseudonáhodný generátor kódov v diaľkovom ovládaní synchronizovaný s generátorom v aute. Každý kód je po použití kľúčom zahodený a v prípade prijatia autom tiež zahodený na príjmacej strane. Kľúč vygeneruje nový kód, ktorý môže byť následne použitý pre overenie.

Príjmač v aute kontroluje prijatý kód voči určitej sade potencionálnych budúcich kódov. Generátor v aute tak zostáva synchronizovaný s generátorom v kľúči v prípade chyby komunikácie alebo stláčania tlačidla kľúča mimo dosah auta.

Rolljam útok umožňuje využiť aktuálny kód prenášaný nezabezpečeným spôsobom a to tak, že pomocou jammingu bráni príjmu aktuálneho kódu autom. Zároveň vďaka úzkopásmovému filtru dokáže tento kód zachytiť. Úročník pokračuje v blokovaní komunikácie až kým obeť nevyšle nový kód. Útočník si zapamätá aj tento kód, čo znamená, že má aktuálne 2 platné kódy k dispozícii. Útočník následne ukončí jamming a odošle prvý prijatý kód do auta, čo umožní obeti bez podozrenia otvoriť auto. Útočník tak získa najbližší kód v sekvencii použiteľný pre otvorenie auta.

4.2 Útok pomocou SDR

Viaceré z popísaných útokov je možné relatívne jednoducho implementovať pomocou SDR. Spoločným pre všetky SDR je *sniffing*, kde limitáciou je len rozsah príjímateľných a spracovateľných frekvencií, presnosť získaných IQ vzorkov z ADC a kvalita použitej

antény. Sniffing však často vyžaduje dlhý časový úsek pre úspešné získanie cenných informácií.

Replay útok je ďalším z pomerne jednoduchých útokov, avšak nie všetky SDR umožňujú okrem príjmu i vysielanie. Dôvodom je často cena, vzhľadom k potrebe kvalitného DAC k existujúcemu ADC a špecifických DSP obvodov. Ďalším parametrom je vysielací výkon a kvalita použitej antény, aby bol signál schopný dosiahnuť cielený príjmač. Podstatným problémom je i rýchlosť odozvy, kde napr. Bluetooth Low Energy protokol vyžaduje odpoveď do $150\mu s$ [24].

Použitie *jammingu* je veľmi jednoduché na základe generovania náhodného "šumového"signálu na cieľovej frekvencii, ale zároveň kladie veľké nároky na vysielací výkon, keďže obecne výkon SDR býva obmedzený. Zároveň mnoho moderných protokolov funguje na princípe channel hopping-u, kedy je v pravidelných intervaloch menená frekvencia prenosu. Pokrytie veľkého rozsahu frekvencií jammingom je náročné a zároveň vyžaduje techniku, ktorá je ľahko odhaliteľná.

Flood útok je možné použiť len pre protokoly bez jednoducho prelomiteľného kryptografickěho zabezpečenia, čo v dnešnej dobe obsahuje len obmedzené množstvo cieľov.

Re-injection útok nachádza využitie pri slabo chránených protokoloch, ako napr. rolljam popísaný vyššie. Zásadné pre prevedenie útoku je správne načasovanie a poznatky o frekvencii či frekvenciách komunikácie (môže byť získaná sniffingom).

5 SOFTVÉR A NÁSTROJE

Softvér používaný v súvislosti s SDR je značne diverzifikovaný a predovšetkým vysoko výpočetne náročný.

Variabilita spočíva v spolupráci mnohých vrstiev softvérových abstrakcií. Od DSP kódu filtrov v Hardware Description Language (HDL) implementovanom na FPGA, až po kód vo vysokoúrovňovom jazyku, ktorý popisuje spracovanie signálu.

Softvér popísaný v tejto kapitole sa zameriava na zjednodušenie práce v tejto zložite úlohe.

5.1 Knižnice a API pre SDR

Každý SDR produkt je dodávaný s nízkoúrovňovými knižnicami pre nastavenie a interakciu s SDR hardvérom. Tieto knižnice umožňujú pristupovať k interným registrom zariadenia, ladiť sledovanú frekvenciu, upravovať parametre filtrov, spúšťať snímanie a vysielanie, či ďalšie komplexnejšie úlohy.

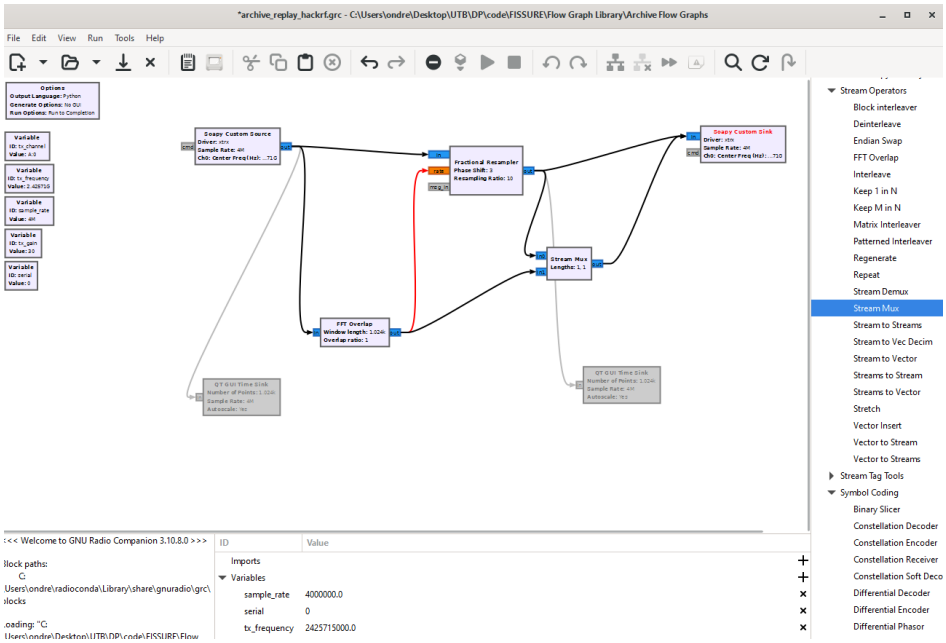
SoapySDR je nezávislé API a knižnica pre interakciu s SDR. Abstrahuje širokú škálu knižníc SDR zariadení, čo umožňuje vývojárom písať softvér, ktorý môže interagovať so rôznymi SDR zariadeniami skrze jednotné API. Knižnica je ľahko rozšíriteľná a modulárna, takže je možné doplňovať podporu pre ďalšie SDR zariadenia. Pod povrchom stále využíva nízkoúrovňové knižnice pre špecifické SDR.

Osmocom je komplexný open source projekt. Obsahuje obdobné API ako SoapySDR a navyše poskytuje rôzne softvérové komponenty pre mobilnú komunikáciu. Obsahuje nástroje pre GSM, GPRS a súvisiace technológie, umožňujúce používateľom experimentovať, vyvíjať a analyzovať mobilné siete.

5.2 Workflow nástroje

Tieto nástroje umožňujú vytváranie komplexných sekvencí na príjem, spracovanie, modifikáciu či vytváranie a vysielanie signálov.

GNU Radio je open-source softvérový vývojový nástrojový balík pre budovanie SDR systémov. Poskytuje prostredie pre vytváranie grafových popisov systémov pre spracovanie signálu pomocou jednoduchých signálových blokov a implementáciu rôznych rádiových komunikačných systémov, čo z neho ho robí populárny softvér medzi výskumníkmi, nadšencami a profesionálmi v oblasti bezdrôtovej komunikácie.



Obrázek 5.1 GNU Radio

Fissure je softvérová platforma zameraná na kybernetickú bezpečnosť a analýzu signálov. Poskytuje nástroje na analýzu a dekódovanie rôznych digitálnych signálov, čo je užitočné pre profesionálov v oblasti bezpečnosti, nadšencov do rádií a výskumníkov [25]. Bohužiaľ, formát kódu Fissure je ťažko rozšíriteľný, čo nedovoľuje ďalej stavať na tomto základe.

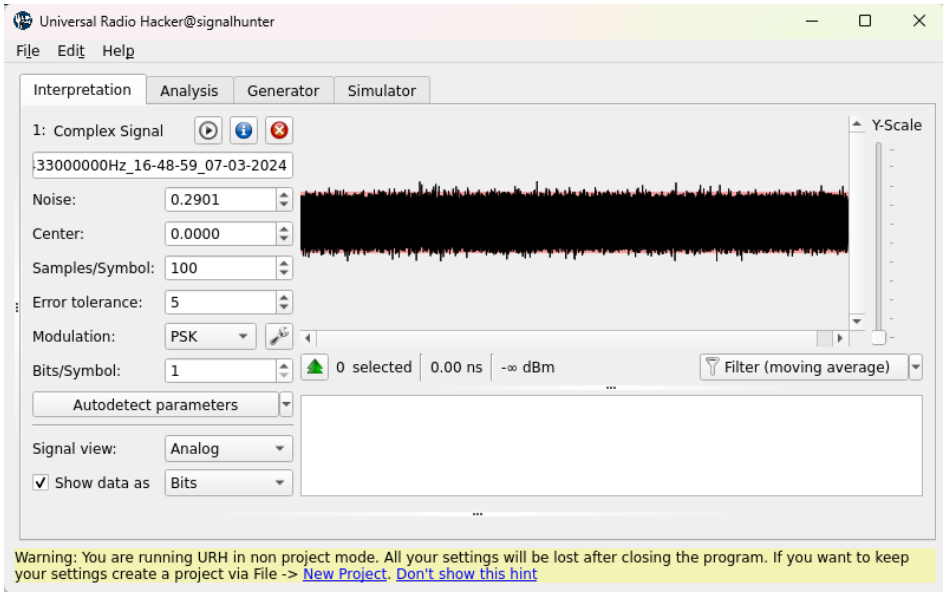
Snout je softvérový nástroj zameraný na mapovanie a penetračné testovanie IoT sietí. Je založený na GNU Radio, Wiresharku, Scapy knižnici pre manipuláciu packetov a využíva Bluetooth LE toolkit.

Universal Radio Hacker je open-source nástroj na analýzu rádiových prenosov. Umožňuje používateľom nahrávať signály, analyzovať ich a reverzným inžinierstvom získavať informácie z rádiových komunikácií.

5.3 Vizualizácia spektra

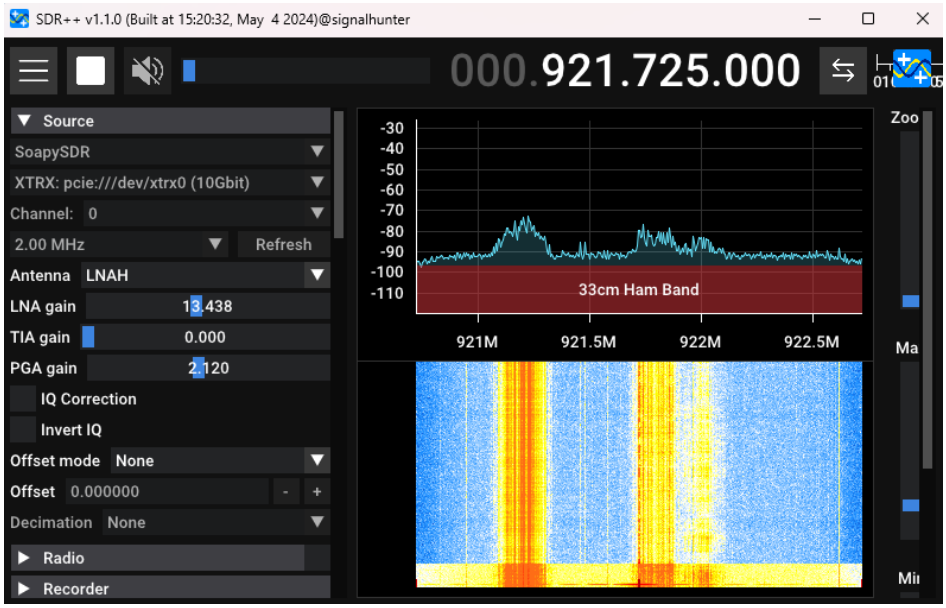
SDRAngel je open-source multiplatformná SDR vizualizačná aplikácia s používateľsky prívetivým rozhraním. Podporuje rôzne platformy SDR a poskytuje funkcie pre analýzu spektra, demoduláciu a moduláciu signálov v rôznych frekvenčných pásmach.

SDR# (SDRSharp) je populárna vizualizačná SDR aplikácia pre systém Windows. Ponúka jednoduché a intuitívne užívateľské rozhranie pre ladenie a demoduláciu rôznych rádiových signálov pomocou kompatibilného SDR hardvéru.



Obrázek 5.2 Universal Radio Hacker

SDR++ je open-source multiplatformná SDR aplikácia navrhnutá pre flexibilitu a výkon. Svojím prostredím sa nápadne podobá na SDR#. Podporuje platformy Windows, Linux i Android a rôzne SDR hardvérové zariadenia. Ponúka prispôsobiteľné užívateľské rozhranie a širokú škálu funkcií na spracovanie signálov.



Obrázek 5.3 SDR++

5.4 Pomocné nástroje

Artemis 3 je softvérová databáza viac než 370 rôznych druhov signálov, ktorá umožňuje prehliadanie, vyhladávanie a identifikáciu signálov na základe if vodopádového modelu a parametrov signálu ako je frekvencia či modulácia.

II. PRAKTICKÁ ČASŤ

6 NÁVRH SYSTÉMU S SDR

S využitím poznatkov získaných pri analýze existujúcich SDR riešení a vhodného softvér môžeme v nasledujúcich sekciách zostaviť zariadenie vhodné na komplexnú analýzu RF.

6.1 Analýza požiadavkov pre návrh systému

Systém pre detekciu potenciálnych vektorov útoku by mal byť v prvom rade prenosný. Väčšina zariadení pre lokálnu komunikáciu má slabý výkon a ich odhalenie vyžaduje buď veľmi dobre nastavený prijímací systém spolu s pokročilými filtrami alebo možnosť priblíženia sa k zdroju signálu čo najbližšie. Vzhľadom na vysokú cenu a zložitú prenositeľnosť prvého riešenia je vhodnejšie zvoliť prenositeľné zariadenie. Voľba jednotlivých komponentov tak musí brať do úvahy ich energetickú náročnosť a praktičnosť prevozu či prenosu.

Spolu s prenositeľnosťou zariadenia vyvstávajú i otázky spojené s užívateľským rozhraním. Keďže operačná doba zariadenia bude vzhľadom k batériovému napájaniu obmedzená, užívateľ bude musieť vyhodnotiť situáciu v teréne a minimálne získať vhodné vzorky signálu na neskoršiu analýzu. Systém by tak mal disponovať zobrazovaciou jednotkou pre okamžitú spätnú väzbu k užívateľovi. Zobrazovacia jednotka by mala byť doplnená o vstupné zariadenie pre zmenu parametrov SDR. Nároky na napájanie zariadenia týmto podstatne vrastú, preto je nutné obmedziť spotrebu ostatných komponent na minimum.

S ohľadom na možnosti moderných SDR systémov, ktoré pokrývajú pásmo VHF a UHF frekvencií a čiastočne i pásmo SHF, je vhodné podporiť čo najväčšiu možnú časť týchto pásiem výberom antén(y) ladených čo možno najviac uprostred vybraných úsekov spektra.

Zároveň je vhodné uvažovať nad systémom, ktorý podporuje viac ako 1 prenosový kanál, čo umožňuje okrem simultánnej analýzy viacerých pásiem i použitie rôznych typov antén pre rôzne RF vstupy bez manuálnej výmeny.

V neposlednej rade, je vhodné zvoliť dostatočne výpočetne výkonný systém, aby bolo možné príjmaný signál podľa potreby spracovávať. Moderné algoritmy signálovej analýzy vyžadujú vysoký výkon, napr. pri použití cyklostacionárnej analýzy.

Zo softvérového hľadiska je vhodné založiť systém na existujúcich komponentoch, ako je operačný systém (OS), ovládače, vizualizačné knižnice a programy pre zobrazenie RF signálov, demodulačné a dekódovacie knižnice, či ich moduly.

6.2 Výber hardvérových komponentov

V období Covid pandémie nastal nedostatok niektorých typov tovaru, medzi ktorými sa ocitli i vysoko sofistikované čipy využívané v SDR. Preto dostupnosť SDR bola a stále je značne obmedzená.

Z SDR platforiem popísaných v sekcii 3 boli vybrané nasledovné zariadenia ako kandidátne:

- HackRF One – zariadenie má (aj napriek mierne obemdzenému hardvéru) veľmi dobrú podporu v komunite, bohužiaľ však v čase nákupu nebolo k dispozícii. Každopádne, aj vďaka existencii nástavby PortaPack H2 je možné toto zariadenie využiť ako referenčné pre porovnanie s navrhovaným systémom.
- LimeSDR – táto platforma sa javila ako ideálna najmä vďaka pomeru kvality a ceny. Bohužiaľ doposial zostáva na trhu nedostupnou, a preto ju nie je možné použiť.
- XTRX – táto platforma je založená na rovnakom ADC/DAC SoC ako LimeSDR, čo jej prináša všetky výhody tohoto systému. Zároveň prináša potenciálnu možnosť využitia miniPCIe zbernice s rýchlejším prenosom údajov. Nevýhodou je, že XTRX ako prototypový projekt má len slabú podporu komunity a podpora od výrobcu Fairwaves v medzičase zanikla s odkúpením spoločnosti.

XTRX napriek nedostatku podpory od komunity i od výrobcu bola dostupná na trhu za rozumnú cenu, a práve z tohoto dôvodu bola vybraná pre využitie.

Komplementárne k SDR bolo potrebné vybrať výpočetnú platformu pre spracovanie signálu, beh podporného operačného systému a súvisiacich programov. Škála takýchto systémov zahrňuje:

- mikrokontroléry typu ESP32 – energeticky vysoko úsporné, avšak tieto zariadenia nemajú dostatočný výpočetný výkon ani vhodné rozhrania pre pripojenie komplexných systémov typu SDR
- ˇminipočítače SoC typu Raspberry Pi – dostatočne výkonné pre beh bežných desktopových aplikácií, zároveň však energeticky úsporné, pričom umožňujú pripojenie rôznych foriem periférií
- plnohodnotný počítačový systém, napr. notebook – výkonné a prenositeľné, avšak nepraktické pre prácu v teréne a časté prenášanie pri hľadaní vhodného signálu. V minulosti bolo možné využiť miniPCIe zbernicu v notebookoch, v dnešnej dobe sú skôr vzácnosťou. Alternatívou je využitie M.2 slotu, ktorý však v moderných notebookoch býva využitý SSD diskom, a preto nedostupný.

	Raspberry Pi 4	**Raspberry Pi 5**
Procesor	Quad-core 64-bit ARM SoC @ 1.8GHz	Quad-core 64-bit ARM SoC @ 2.4GHz
Operačná pamäť	až 8GB LPDDR4-3200 SDRAM	až 8GB LPDDR4X-4267 SDRAM
Periférie		
	2x USB 3.0, 2x USB 2.0	2× USB 3.0, 2× USB 2.0
	MIPI DSI display port	2× 4-kanálové MIPI kamera/display porty
	-	PCIe 2.0 x1 interface

Tabulka 6.1 Porovnanie výpočetných platforiem [26] [27]

Z uvedených riešení prichádza v úvahu hlavne systém typu Raspberry Pi, keďže je cenovo dostupný, ľahko prenosný, energeticky nenáročný, a je možné ho ľahko nahradiť v prípade chyby.

V pôvodnom návrhu bolo uvažované Raspberry Pi 4 v súčinnosti s USB 3 adaptérom pre XTRX. Avšak uvedenie Raspberry Pi 5 na trh prinieslo ďalšie možnosti. Porovnanie relevantných vlastností týchto dvoch platforiem je vidiet v tabuľke 6.1.

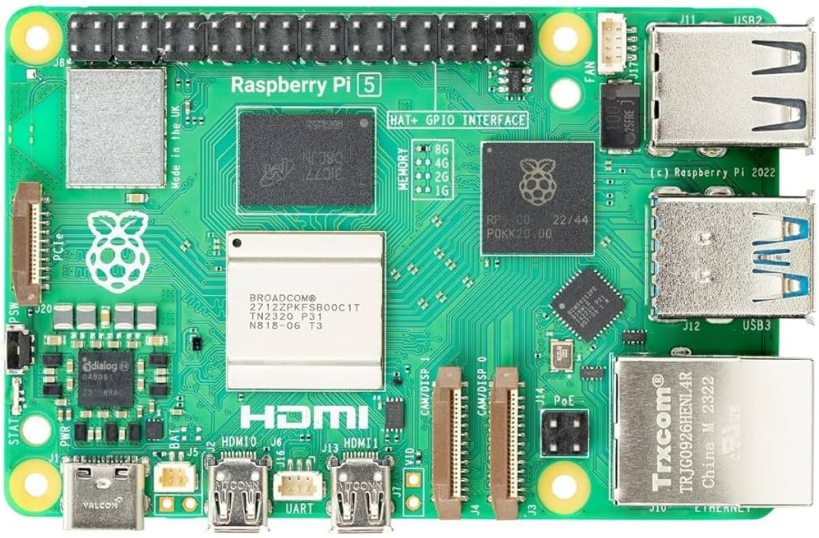
Ako je vidieť Raspberry Pi 5 je podstatne výkonnejší systém, čo umožňuje rýchlejšie spracovanie dát s väčšou efektivitou. Zároveň Raspberry Pi 5 poskytuje novú PCIe periférium, ktorú je možné využiť spolu s miniPCIe zbernicou XTRX. Takéto spojenie umožnuje značne zvýšiť priepustnosť dát medzi XTRX a Raspberry Pi.

Raspberry Pi 5 však používa špeciálne rozhranie pre prístup k PCI zbernici pomocou 16-pinového FFC konektora. Z toho dôvodu je potrebné využiť špeciálne navrhnutý adaptér, tzv. HAT dosku, ktorá sa dá k minipočítaču pripojiť. Zvolená bola HatDrive! Bottom od spoločnosti Pineberry Pi, originálne cielená na pripojenie M.2 SSD diskov. Toto rozšírenie poskytuje M.2 rozhranie s konfiguráciou typu M-key.

Na pripojenie XTRX zostáva doplniť adaptér prevodu z miniPCI na M.2, ktorý poskytuje M.2 rozhranie typy B & M a jednoducho sa dá zapojí do HatDrive!.

Pre interakciu s užívateľom bol zvolený dotykový 7 palcový TFT display pripojený cez DSI rozhranie. Dotyková vrstva je pripojená k I2C rozhraniu Raspberry Pi. Display je originálnym príslušenstvom Raspberry Pi, takže má plnohodnotnú podporu v operačnom systéme Raspberry Pi OS.

Všetky batériové systémy navrhnuté pre Raspberry Pi sú určené ako záložné zdroje energie UPS. Toto napájanie nie je ideálne, ale je priamo navrhnuté pre potreby Raspberry Pi, takže jeho kapacita by mala stačiť. Pre napájanie je využitý doplnok Geekworm X1202 špeciálne vyvinutý pre Raspberry Pi 5, ktorý sa pripája pomocou POGO pinov na spodnú stranu dosky Raspberry Pi. Tento doplnok má kapacitu na sadu 4 batérií typu 18650 so sumárnou kapacitou 12000 mAh. Doplnok je schopný



Obrázek 6.1 Raspberry Pi 5

libxtrx	Vysokoúrovňová knižnica pre prácu s XTRX
libxtrxll	Nízkoúrovňová knižnica pre XTRX
libxtrdsp	DSP funkcionalita pre XTRX
libusb3380	Ovládač USB 3 adaptéra pre XTRX
xtrx_linux_pcie_drv	PCIe ovládač pre XTRX

Tabulka 6.2 Zoznam knižníc a ovládačov používaných XTRX

dodávať až 5A prúdu, čo by malo postačovať pre potreby systému.

6.3 Výber softvérových komponentov

S použitím hardvérových komponentov je vhodné použiť i kompatibilné softvérové komponenty. Medzi tieto sa radí operačný systém s podporou Raspberry Pi 5 – Raspberry Pi OS, založený na Debian Bookworm.

Pre využitie XTRX je nutné nainštalovať vhodný softvér a to ako knižnice – libxtrx, libxtrxll, libxtrxdsp a libusb3380, tak i ovládače – XTRX PCIe ovládač. Dostupnosť knižníc a ovládačov je zhrnutá v tabuľke 6.2.

Súčasťou libxtrx je i kompatibilné rozhranie so SoapySDR, ktoré umožňuje používať XTRX s rôznymi softvérovými nástrojmi.

Všetky knižnice a ovládače uvedené v tabuľke 6.2 sú dostupne z GitHub-u firmy MyriadRF na adrese .

Jedným z takých je SDR++, ktorý okrem okamžitej vizualizácie príjmaných dát umožňuje využívanie rôznych pomocných modulov. SDR++ využíva knižnicu Dear ImGUI, ktorá poskytuje veľmi ľahké a rýchle UI prostredie. Vďaka prehľadnosti kódu je veľmi jednoduché SDR++ upravovať a s podporou viacerých platforiem i vlastného

vysielacieho serveru je tento softvér ideálny pre súčinné využitie na viacerých platformách zároveň.

6.4 Zostavenie systému a nastavenie softvéru

Po nainštalovaní Raspberry Pi OS na microSD kartu je potrebné previesť jeho nastavenie. U novo predstaveného Raspberry Pi 5 prebieha stále živý vývoj, a preto niektoré vlastnosti, vrátane PCIe podpory je potrebné explicitne povoliť v konfiguračných nastaveniach.

Raspberry Pi 5 poskytuje k tomuto účelu `config.txt` súbor v `boot` adresári. V tomto súbore je nutné povoliť `dtparam` parameter `pciex1` a tiež `dtoverlay` nastavenie `pcie-32bit-dma-pi5`, ktorě jednak povolujú použitie PCIe rozhrania a zároveň umožňujú 32-bitovú Direct Memeory Access (DMA) komunikáciu na 64-bitovom systéme, čo je nutná požiadavka pre XTRX.

Zároveň je potrebné pre flexibilnú DMA alokáciu pridať do štartovacích parametrov Linux jadra parameter `coherent_pool=32M`.

Následne je možné zostaviť požadovaný softvér a otestovať funkcionalitu XTRX pomocou `test_xtrx` utility dodávanej spolu s libxtrx knižnicou. Zostavený a funkčný systém je možné vidieť na obrázkoch 6.2 a 6.4.

Obrázek 6.2 Zostavený systém s bežiacim SDR++

Obrázek 6.3 Zostavený systém, bočný pohľad

V systéme je nastavená SystemD služba, ktorá spúšťa SDR++ aplikáciu hneď po spustení systému a v prípade nečakaného ukončenia aplikácie sa ju do 5 sekúnd pokúsi znovu spustiť.

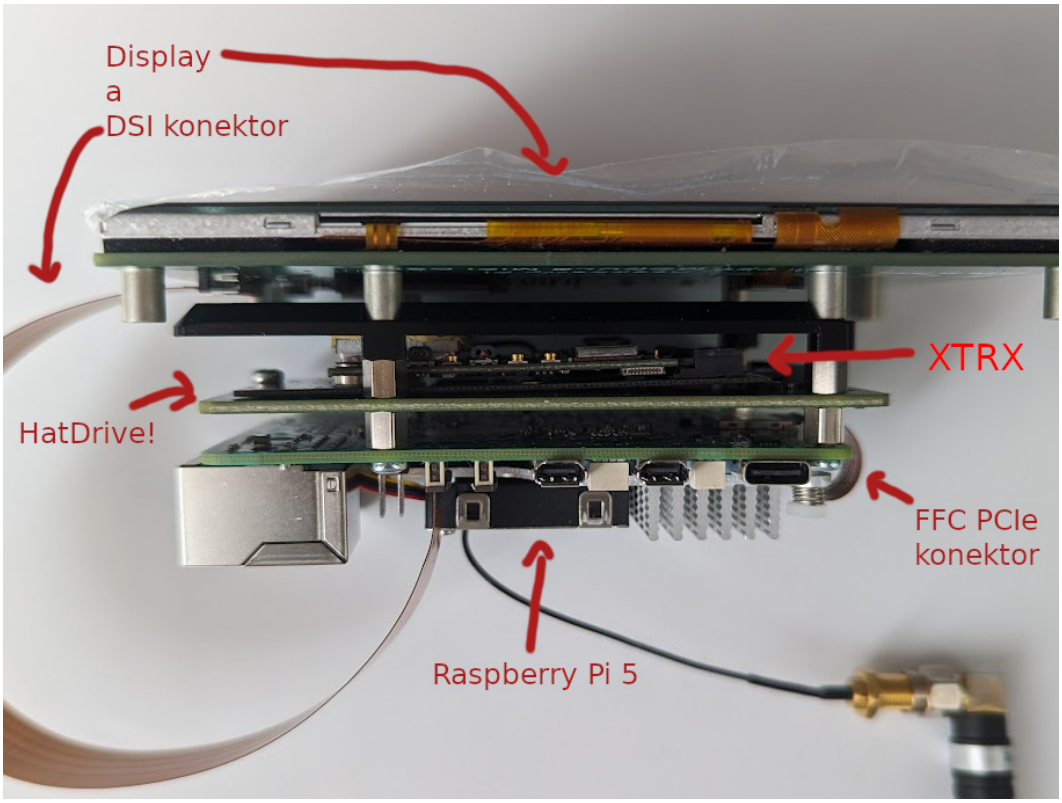
Pre zostavené zariadenie bolo navrhnutých viacero boxov, ktoré umožňujú jednoduchšiu manipuláciu a používanie. Jednou z reštrikcií, ktoré viedli k viacerým verziám boxov je dĺžka FPC konektoru vedúceho z Raspberry Pi k XTRX. Špecifikácia Raspberry Pi umožňuje maximálnu dĺžku 40 mm, a preto bolo nutné predĺžiť hĺbku zariadenia [28]. Návrh boxov bol prevedení v aplikácii Autodek Fusion 360 a je priložený v elektronickej prílohe k práci.

6.5 Návrh automatizácie identifikácie možných vektorov útoku

Sekcia 2 naskytuje možný spôsob výpočtu spektrálnej korelačnej funkcie. Vzhľadom na to, že väčšina elektromagnetických signálov produkovaných ľuďmi vykazuje cyklostacionárne vlastnosti v SCF, môžeme tejto skutočnosti využiť.

Pre výpočet SCF môžeme využiť existujúce prostriedky pre prácu so signálom poskytnuté v open-source aplikácii SDR++. Vďaka dostupnosti zdrojových kódov je možné aplikáciu preložiť pre cieľovú ARM architektúru.

SDR++ navyše využíva SIMD inštrukcie, ktoré urýchľujú výpočty nad vektorovými dátami, skrze knižnicu VOLK. VOLK abstrahuje SIMD inštrukcie do podoby



Obrázek 6.4 Zostavený systém, interné usporiadanie

užitočných funkcií pre urýchlenie práce so signálom naprieč rôznymi architektúrami. Raspberry Pi 5 je založená na architektúre ARM Cortex-A76, ktorá poskytuje rozšírenie inštrukčnej sady o NEON SIMD inštrukcie [26]. Tejto vlastnosti môžeme využiť pre podstatné urýchlenie výpočtu SCD.

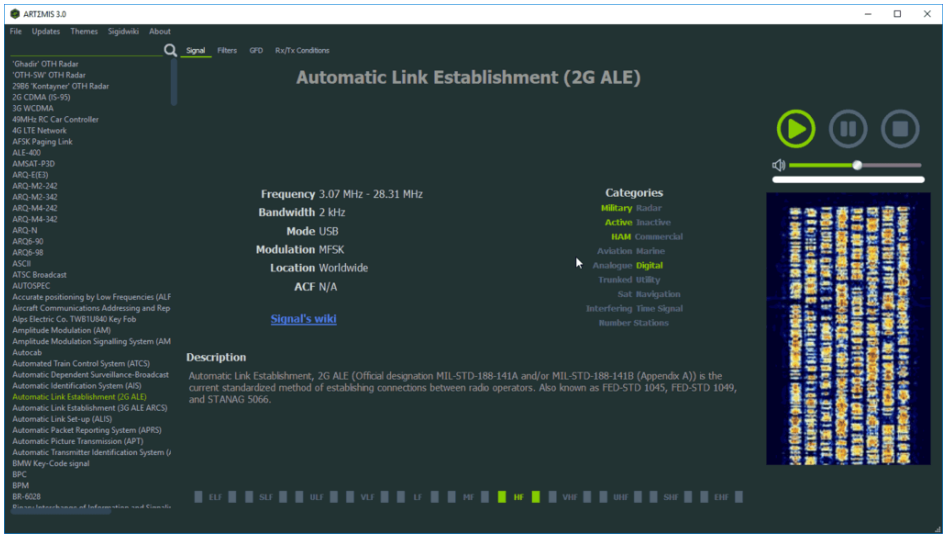
Vypočítanú SCD funkciu so zjednodušením navrhnutým v sekcii 2.4.11 môžeme zobraziť v aplikácii namiesto vodopádového diagramu.

SCD je v diagrame orientovaná tak, že jej horizontálna os približne odpovedá rozlíšeniu vo frekvencii a vertikálna os približne odpoveda rozlíšeniu v cyklickej frekvencii. Vďaka tomu je možné asociovať signály zobrazené v spektre na SCF, v ktorej je možné vidieť cyklostacionárne vlastnosti signálu prítomného na sledovanej frekvencii.

Z poznatkov o známej frekvencii a z cyklostacionarity signálu môžme uvažovať o pravdepodobnej prítomnosti žiadaného signálu. Podozrenie si môžeme overiť v aplikácii Artemis, ktorá listuje známe signály na frekvenciách, na ktorých sa bežne vyskytujú. Artemis tiež obsahuje vzorku vodopádového diagramu, ktorú môžeme porovnať s vodopádovým diagramom sledovaného signúalu, viď obrázok 6.6.

Na základe týchto poznatkov môžeme zhodnotiť možnosti útoku a zostaviť vhodný plán útoku, čím sa táto práca už detailnejšie nezaoberá.

Obrázek 6.5 Prehľad navrhnutých boxov



Obrázek 6.6 Artemis

Rozmery (ŠxVxH)	20cm x 11cm x 8cm
Výdrž batérie	2 4 hodiny (max.5,2 h)
Frekvenčný rozsah	30 MHz – 3,8 GHz
Max. šírka kanála	teoret. 90 MHz, prakticky 15–20 MHz
Periférie	2x USB2.0, 2x USB3.0, Rj-45, 2x micro HDMI, 4x SMA (2x Rx, 2x Tx)

Tabulka 7.1 Vlastnosti navrhnutého zariadenia SignalHunter

7 TESTOVANIE SYSTÉMU

Zostavené zariadenie, pre jednoduchšiu orientáciu ho môžeme pomenovať ako SignalHunter (SH) môžeme otestovať z viacerých hľadísk:

- z hľadiska kvalitatívneho
- z hľadiska cieleného použitia
- z hľadiska porovnania s inými zariadeniami s podobným, či rovnakým účelom

Z kvalitatívneho hľadiska sa jedná predovšetkým o užívateľský komfort, UI/Ux návrh, výdrž batérie, rozmery, maximálnu spracovateľnú šírku kanálu (bandwidth), dostupné periférie a podobne.

Pre veličiny, ktoré su ťažko merateľné, ako napr. užívateľský komfort či UI/UX, môžeme vyzdvihnúť pozitívne a negatívne vlastnosti SH. Medzi pozitíva patrí veľká dotyková obrazovka, design umožňujúci jednoduchý prenos a pozorovanie (box je navrhnutý tak, aby zariadenie na stole stálo), ľahké ovládanie pomocou veľkých tlačítiek (SDR++ je navrhnuté pre použitie i na systéme Android). Medzi negatíva môžeme zaradiť nepresnosť dotykovej vrstvy, ťažkopádnosť ovládania pri menších prvkoch UI, a pod.

Kvantitatívne hodnoty môžeme zhrnúť v tabuľke 7.1. Hľadisku cieleného použitia sa venujú nasledujúce 2 odstavce.

7.1 Testovanie systému imitáciou reálneho cieľa

Pre imitáciu cieľa najprv potrebujeme zostaviť testovaciu zostavu. V našom prípade pozostáva z testovaného zariadenia, notebooku pre zaznamenávanie výsledkov a sekundárneho zariadenia XTRX pripojeného k notebooku, ktoré slúži na generovanie testovacieho signálu, viď obrázok 7.1.

Pre potreby testovania boli vybrané 2 typické signály, ktoré sa prejavujú odozvou v SCF. Sú nimi signály modulované BPSK a QPSK digitálnou moduláciou. Pre účely

Obrázek 7.1 Testovacia zostava bez SH

generovania týchto signálov bol vytvorený skript v jazyku Python, ktorý vytvára náhodné symboly v maximálnom rozsahu podporovanom danou moduláciou (t.j. 0–1 pre BPSK a 0–3 pre QPSK).

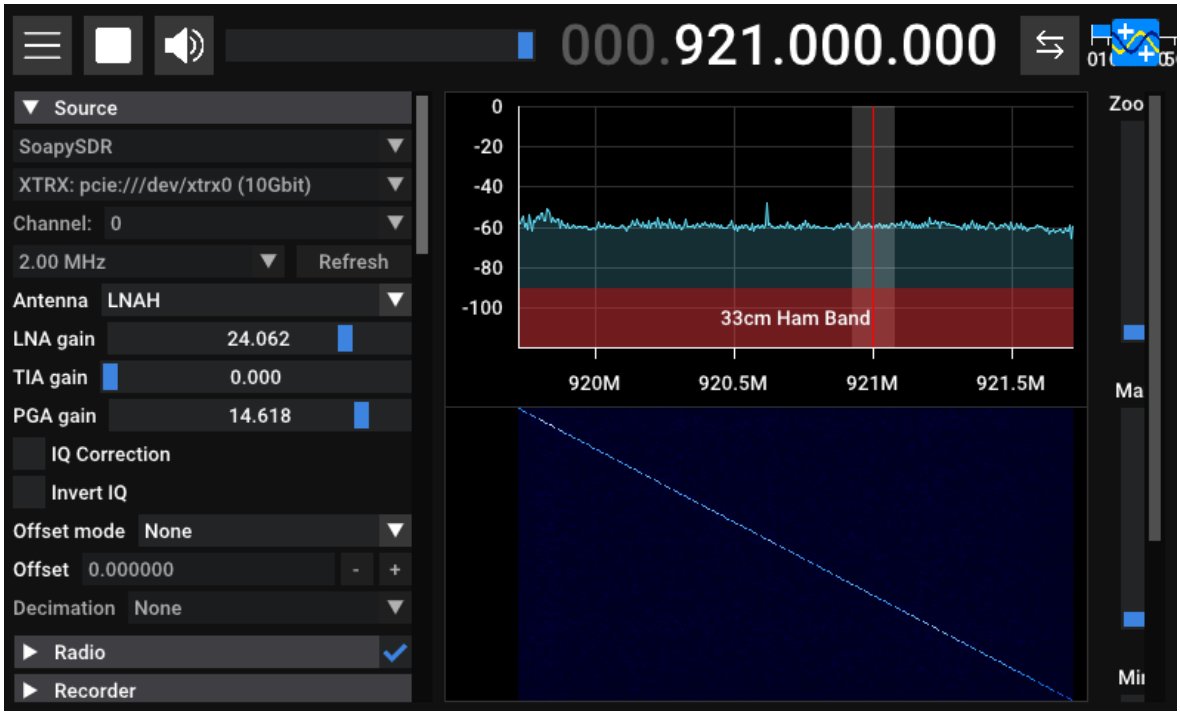
Tento skript využíva SoapySDR k prenosu QPSK vlny s frekvenciou 1 MHz, amplitúdou 0,1 a šírkou pásma 62,5 kHz. V modelovom príklade popísanom nižšie bola frekvencia nosnej vlny (carrier) nastavená na 921 MHz. Obrázok 7.2 zobrazuje situáciu originálneho spektra, kedy nedochádzalo k prenosu signálu.

Pre porovnani obrázok 7.3 zobrazuje situáciu pri vysielaní signálu QPSK.

V pravom dolnom kvadrante obrázku 7.3 je možné postrehnúť jasný kríž, ktorý zobrazuje všetky 4 fázové posuvy QPSK.Je potreba si uvedomiť, že zobrazená SCF je otočená oproti skutočnej SCF o 45°. Ďalej je možné postrehnúť ohraničenie v polohách -0,5 a +0,5, čo odpovedá frekvencii signálu 1MHz.

Pre porovnanie si môžeme zobraziť situáciu so signálom BPSK s rovnakými hodnotami ako u QPSK. Situácia na obrázku 7.4 je oveľa menej zreteľná, pretože BPSK otáča fázu o 180°, a tá splýva s hlavnou diagonálou.

V každop prípade je možné vidieť, že signál má odozvu v SCF a je teda možné ho identifikovať.



Obrázek 7.2 SCF diagram pred vysielaním akéhokoľvek signálu

7.2 Nasadenie systému v reálnej situácii

Pre porovnanie s predošlou situáciou je vhodné nasadiť zariadenie do reálnych podmienok. Pre testovanie bol zvolený známy signál generovaný bezdrôtovým dverným zvončekom. Tieto systémy pri stlačení tlačidla vysielajú kódovaný sled, typicky ASK modulovaných, symbolov, ktorými sa identifikujú u centrálnej stanice, aby došlo k rozozvučeniu správneho zvončeka.

Situácia je ilustrovaná na obrázku 7.5, kedy došlo k sledu stlačení tlačítka a na vodopádovom diagrame je vidieť jasný vzor v okolí frekvencie 433 MHz.

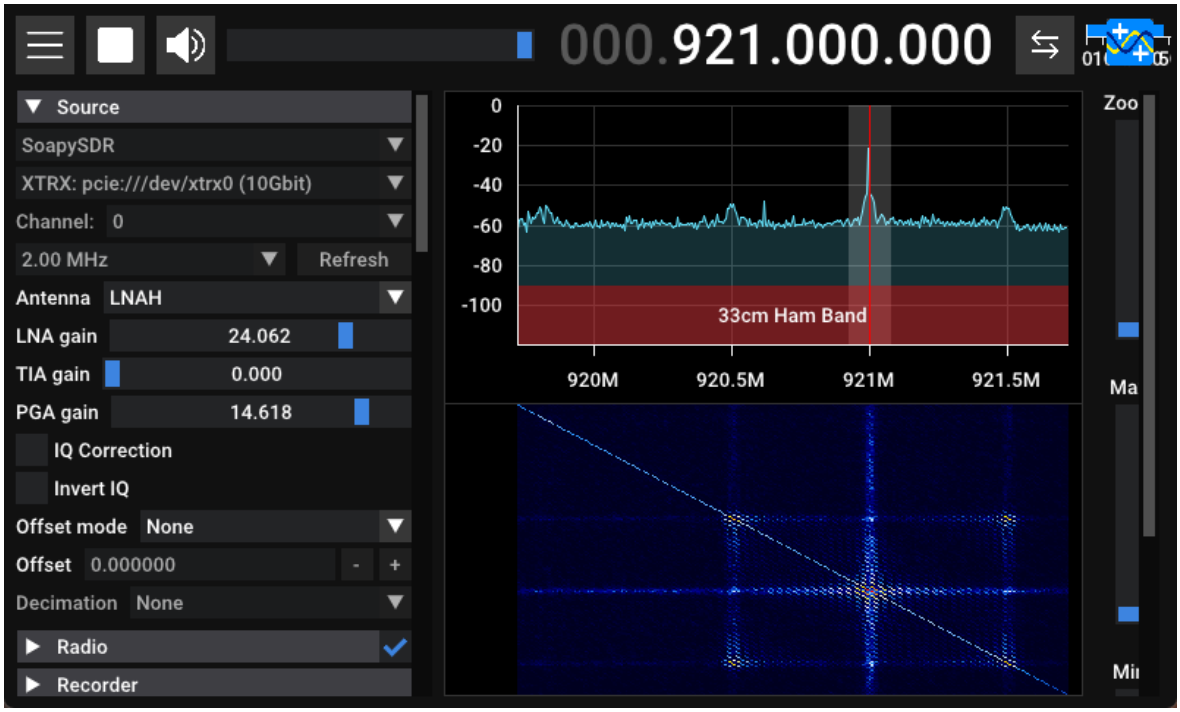
Situácia v SCF je pre každé stlačenie obdobná, viď obrázok 7.6. Stlačenie vytvára krížový vzor v SCF pričom ramená kríža sú rozstrapatené, čo odpovedá kódovaniu v amplitúdovej modulácii.

Posledným hľadiskom testovania je otestovanie SH vzhľadom k už existujúcim riešeniam. Tejto problematike sa venuje nasledovný odstavec.

7.3 Porovnanie s existujúcimi riešeniami

Z pohľadu plánovaného užitia navrhnutého SH prichádza do úvahy 1 zariadenie na základe zistení z odstavca 3.3, ktoré môžeme porovnať s navrhnutým zariadením. Všetky ostatné SDR vyžadujú užitie externého zariadenia pre spracovanie dát. Týmto zariadením je PortaPack H2, ktoré je nadstavbou nad HackRF One.

PortaPack H2 využíva menší display a ovládanie je vyriešené pomocou otáčacieho



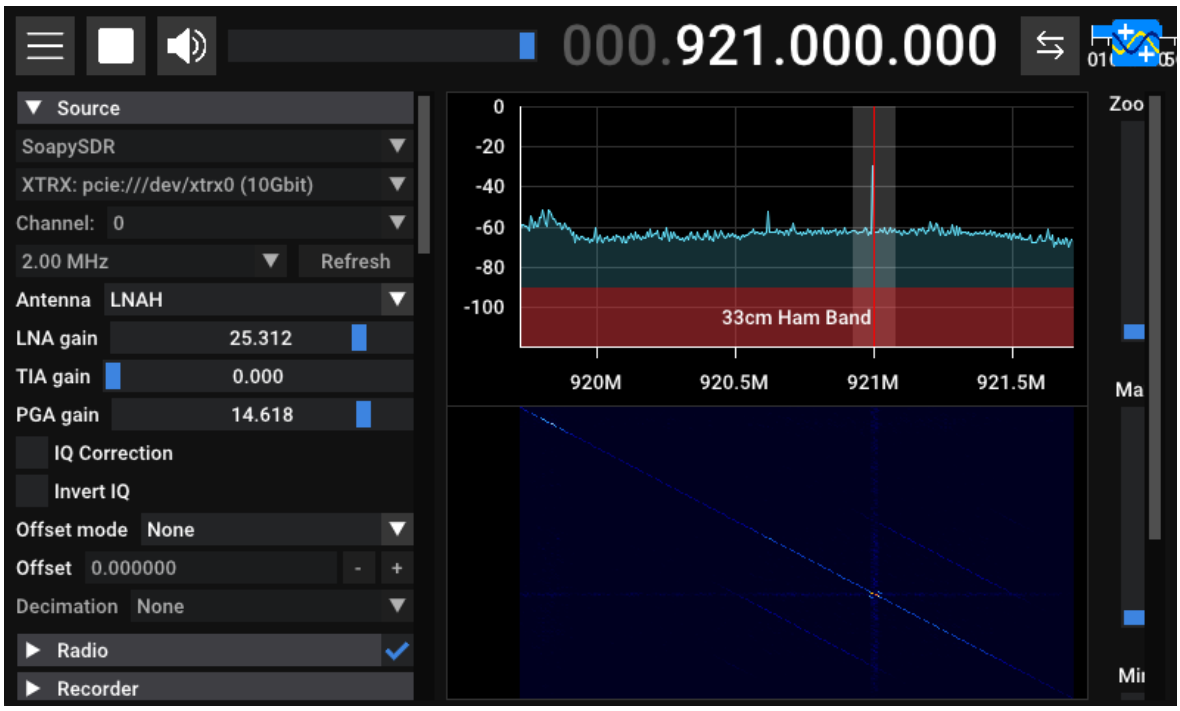
Obrázek 7.3 SCF diagram pri vysielaním QPSK signálu

potenciometru a 5 tlačítok. Toto zariadenie operuje na vlastnom operačnom systéme, ktorý je vytváraný komunitou [29].

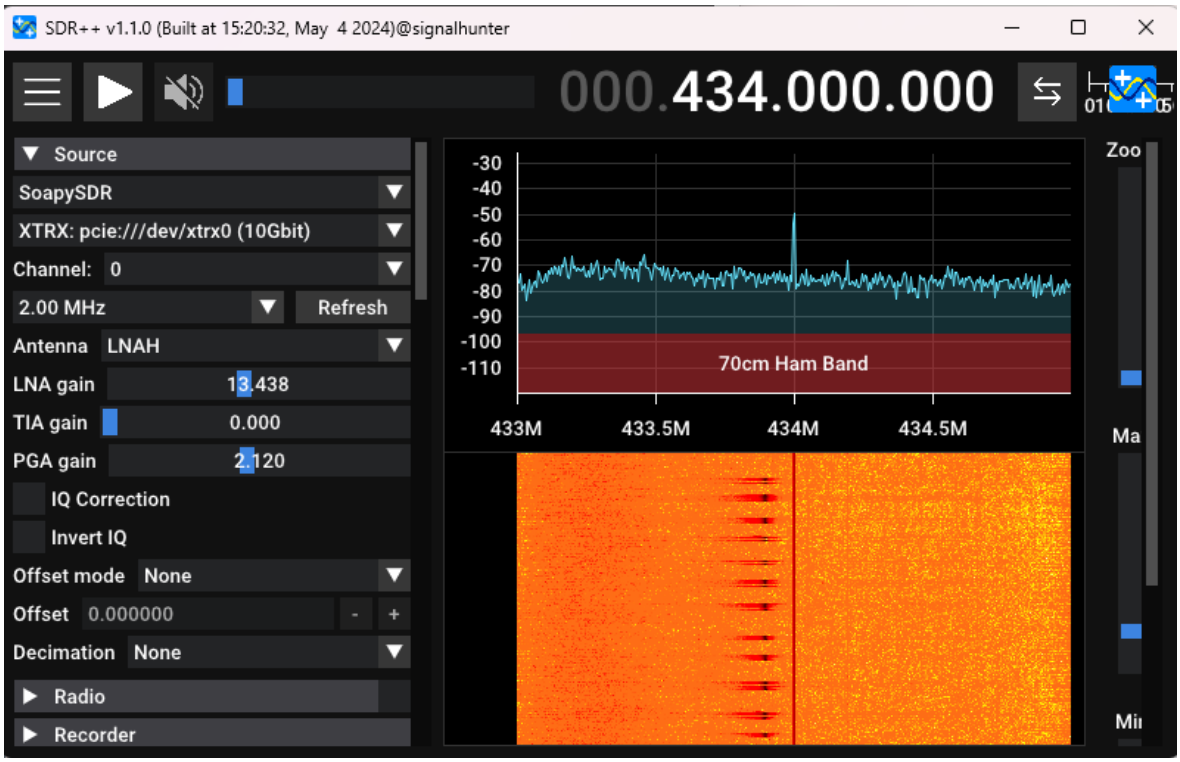
Firmware je svojimi funkciami orientovaný na komunitu ľudí, ktorý vyhľadávajú špecifické frekvencie a demodulujú signály príjmané na nich. To znamená, že je tak možné demodulovať signály analógovej slow-scan televízie (SSTV), signály z meteorologických rádiosond, RDS informácie z terestriálneho vysielania rádia a pod.

Zariadenie je vysoko prenosné, avšak nedisponuje veľkým výpočetným výkonom, v ktorom ho ďaleko predčí navrhovaný SH. Z pohľadu detekcie skrytých signálov je tak zariadenie len obtiažne použiteľné, keďže takéto signály je možné na PortaPack detekovať len zo spektra.

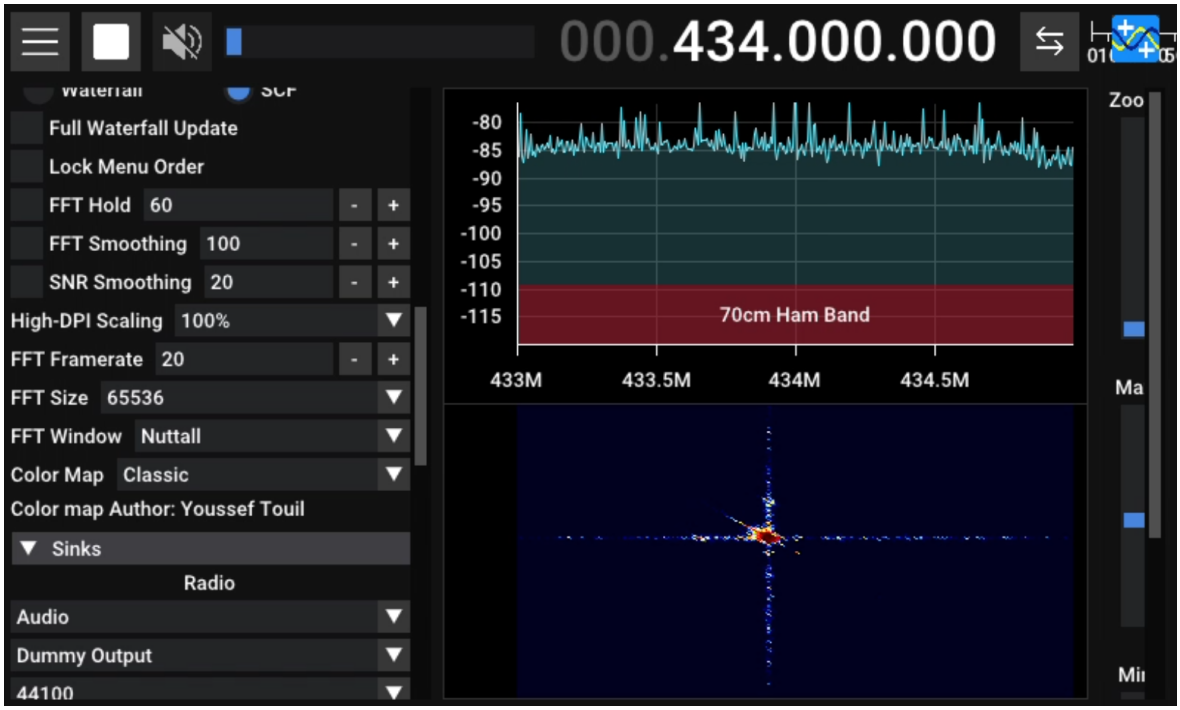
Zároveň, napriek možnosti rozširovania firmware je táto metóda zdĺhavá a obtiažna. Navrhované SH zariadenie umožňuje (s periférnym zariadením klávesnice) vytváranie a exekúciu skriptov napr. v jazyku Python (podobne ako boli poUžité pre účely testovania) a je tak možné jeho správanie meniť “v teréne” a reagovať tak na prípadné nejasnosti v zachytenom signále.



Obrázek 7.4 SCF diagram pri vysielaním BPSK signálu



Obrázek 7.5 Vodopádový diagram pri signále dverného zvončeka



Obrázek 7.6 SCF diagram pri signále dverného zvončeka

ZÁVER

Cieľom tejto práce bolo preskúmanie spôsobu, ktorým by bolo možné detekovať neznáme zdroje signálu v spektre a vytriediť signály s cyklostacionárnym charakterom, ktoré vykazujú najväčší potenciál pre prenášanie cenných dát a tak sú vhodné na prevedenie útoku. Práca v tomto smere priniesla nové prenosné zariadenie využívajúce najnovšie, voľne dostupné, hardverové komponenty, ktoré skombinovala do zariadenia s dostatočne veľkým výkonom na prevedenie základnej cyklostacionárnej analýzy.Takéto zariadenie má potenciál na automatizáciu vyhľadávania nezabezpečených signálov a ich exploitáciu.

Cieľom ďalšieho výskumu by malo byť preskúmanie možností takéhoto zariadenia, zlepšenie kvality vypočítaných cyklostacionárnych charakteristík a uplatnenie zariadenia v automatickom prevedení rôznych typov útokov na zistené kandidátne signály v spektre.

Spolu s týmto by autor práce rád poukázal na veľmi obmedzené informácie a počet kvalitných článkov pojednávajúcich o SDR. Je jeho presvedčením, že táto disciplína je veľmi rozšírením koníčkom, SDR sa používajú v priemysle, armáde i pri ochrane (napr. pred útokmi dronov), a preto by mala byť dostupnosť kvalitnej literatúry na túto tému samozrejmosťou. Práve z tohoto dôvodu je vhodné túto tému ďalej rozvíjať a pokračovať vo vývoji pokročilých penetračných nástrojov založených na modených výpočetných prostriedkoch.

SEZNAM POUŽITÉ LITERATURY

[1] GRIFFITHS, D. J.: *Introduction to Electrodynamics*. Čtvrté vydání, 2013, ISBN 978-1-10842-041-9.

[2] NASA: Radio Spectrum. [online], [cit. 13. května 2024]. Dostupné z WWW: `https://www.nasa.gov/directorates/heo/scan/spectrum/radio_spectrum`.

[3] PAWLAK, R.: Umělé zdroje elektromagnetického pole. In *Elektromagnetické pole a člověk: O fyzice, biologii, medicíně, normácg a síti 5G*, editace Łukasz LAMŻA, Varšava: Ministerstvo digitalizace, 2019, ISBN 978-83-916146-5-5, s. 32–37.

[4] Article 2: Nomenclature. In *Radio Regulations*, Ženeva: International Telecommunication Union, první vydání, 2020, ISBN 978-92-61-30301-3, s. 25–26.

[5] DOBEŠ, J.; ŽALUD, V.: *Moderní rádiotechnika*. BEN - technická literatura, 2006, ISBN 80-7300-132-2.

[6] FARUQUE, S.: *Radio Frequency Modulation Made Easy*. Cham: Springer International Publishing, první vydání, 2017, ISBN 978-3-319-41200-9.

[7] ZIELIŃSKI, T. P.: *Introduction to SDR: IQ Signals and Frequency Up-Down Conversion*. Springer International Publishing, 2021, ISBN 978-3-030-49256-4, s. 483–515, [cit. 13. května 2024]. Dostupné z DOI: `10.1007/978-3-030-49256-4_17`.

[8] COLLINS, T. F.; GETZ, R.; PU, D.; aj.: *Software-defined radio for engineers*. Artech House, 2018, ISBN 978-1-63081-459-5.

[9] OPPENHEIM, A. V.; BUCK, J.; DANIEL, M.; aj.: *Signals & systems*. Pearson Educación, 1997, ISBN 9780138147570.

[10] ANTONI, J.: Cyclostationarity by examples. *Mechanical Systems and Signal Processing*, ročník 23, č. 4, 2009: s. 987–1036, ISSN 0888-3270, [cit. 13. května 2024]. Dostupné z DOI: `doi:/10.1016/j.ymssp.2008.10.010`.

[11] BESSON, O.: Introduction to Spectral Analysis, [cit. 13. května 2024]. Dostupné z WWW: `https://pagespro.isae-supaero.fr/IMG/pdf/slides_asp_eng.pdf`.

[12] ZHANG, H.; RUYET, D. L.; TERRÉ, M.: Spectral correlation of multicarrier modulated signals and its application for signal detection. *EURASIP Journal on Advances in Signal Processing*, ročník 2010, 2009.

[13] VADIVELU, R.; SANKARANARAYANAN, K.; SRUTHI, K.: Implementation of modified time-smoothing algorithms and its comparative analysis in spectrum sensing. *European Journal of Scientific Research*, ročník 80, č. 2, 2012: s. 237–243, ISSN 1450-216X.

[14] ROBERTS, R.; BROWN, W.; LOOMIS, H.: Computationally efficient algorithms for cyclic spectral analysis. *IEEE Signal Processing Magazine*, ročník 8, č. 2, 1991: s. 38–49, [cit. 13. května 2024]. Dostupné z DOI: doi:/10.1109/79.81008.

[15] CARTER, N.: *Implementation of cyclic spectral analysis methods*. Dizertační práce, Naval Postgraduate School, 1992.

[16] RIVES, M.; KOHLER, E.; DAVIES, T.: ADCs of SDR: Parameters, Design Considerations and Implementations, 2011, [cit. 13. května 2024]. Dostupné z WWW: https://www.wirelessinnovation.org/assets/documents/ADCs-of-SDR_r3p1_1_.pdf.

[17] ULVERSOY, T.: Software Defined Radio: Challenges and Opportunities. *IEEE Communications Surveys & Tutorials*, ročník 12, č. 4, 2010: s. 531–550, [cit. 13. května 2024]. Dostupné z DOI: doi:10.1109/SURV.2010.032910.00019.

[18] EWING, M.: *ABCs of Software Defined Radio*. Amer Radio Relay League, 2012, ISBN 978-0-87259-632-0.

[19] CSETE, A.; CHRISTIANSEN, S.: Evaluation of SDR Boards and Toolchains. Technická zpráva, SDR Makerspace, 2020, [cit. 13. května 2024]. Dostupné z WWW: https://www.klofas.com/blog/2020/satnogs-station-and-minicircuits-lna-modifications/Evaluation_of_SDR_Boards-1.0.pdf.

[20] FAIRWAVES: XTRX: The first ever truly embedded SDR. [online], 2018, [cit. 13. května 2024]. Dostupné z WWW: https://www.crowdsupply.com/fairwaves/xtrx.

[21] GETZ, R.: ADALM-PLUTO Detailed Specifications. [online], 2021, [cit. 13. května 2024]. Dostupné z WWW: https://wiki.analog.com/university/tools/pluto/devs/specs.

[22] BYBYK, R.; OPIRSKYY, I.; MCINTOSH, M.: SDR Receivers as a New Challenge to Cybersecurity Wireless Technology. In *Cybersecurity Providing in Information and Telecommunication Systems*, ročník 3188, 2021, ISSN 1613-0073, s. 108–119.

[23] GitHub: RollJam 315MHz / 433MHz (Research & How-To). [online], [cit. 13. května 2024]. Dostupné z WWW: https://github.com/CR11CS/RollJam-315MHz-433MHz.

[24] PICOD, J. M.; LEBRUN, A.; DEMAY, J. C.: Bringing software defined radio to the penetration testing community. In *Black Hat USA Conference [online]*, 2014, [cit. 13. května 2024. Dostupné z: https://www.blackhat.com/docs/us-14/materials/us-14-Picod-Bringing-Software-Defined-Radio-To-The-Penetration-Testing-Commu pdf.

[25] POORE, C.: FISSURE. In *Proceedings of the GNU Radio Conference [online]*, ročník 7, 2022, [cit. 13. května 2024. Dostupné z: https://pubs.gnuradio.org/index.php/grcon/article/view/122/102.

[26] Raspberry Pi 5. [online], 2023, [cit. 13. května 2024]. Dostupné z WWW: https://datasheets.raspberrypi.com/rpi5/raspberry-pi-5-product-brief.pdf.

[27] Raspberry Pi 4 Model B. [online], 2023, [cit. 13. května 2024]. Dostupné z WWW: https://datasheets.raspberrypi.com/rpi4/raspberry-pi-4-product-brief.pdf.

[28] Raspberry Pi Connector for PCIe. [online], 2023, [cit. 13. května 2024]. Dostupné z WWW: https://datasheets.raspberrypi.com/pcie/pcie-connector-standard.pdf.

[29] GitHub: Havoc firmware for PortaPack). [online], [cit. 13. května 2024]. Dostupné z WWW: https://github.com/furrtek/portapack-havoc/.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AM	amplitudová modulace
API	aplikačné užívateľské rozhranie
ASK	klíčování aplitudovým posuvem
DMA	direct memory access
FM	frekvenční modulace
FSK	klíčování frekvenční posuvem
IT	informační technologie
OS	operačný systém
PM	fázová modulace
PSK	klícování fázovým posuvem
SCD	spectrálna korelačná hustota
SCF	spectrálna korelačná funkcia
SH	Signal Hunter
SDR	Software Defined Radio
UI	užívateľské rozhranie
UX	užívateľský zážitok

SEZNAM OBRÁZKŮ

SEZNAM TABULEK