ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

Ústav letecké dopravy

Možnosti simulace GNSS signálu se zaměřením na SDR

GNSS signal simulation options with a focus on SDR

Bakalářská práce

Studijní program: Technika a technologie v dopravě a spojích

Studijní obor: Letecká doprava

Vedoucí práce: Ing. Jakub Steiner

Jan Slezáček

Praha 2023

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K621.....Ústav letecké dopravy

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Jan Slezáček

Studijní program (obor/specializace) studenta:

bakalářský – LED – Letecká doprava

Název tématu (česky): **Možnosti simulace GNSS signálu se zaměřením na SDR**

Název tématu (anglicky): GNSS Signal Simulation Options With a Focus on SDR

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte následujícími pokyny:

- Cílem práce je zmapovat technologie a technologické přístupy k simulování signálu GNSS a sestavit generátoru GNSS signálu s využitím softwarově definovaného rádia a volně dostupných skriptů pro tyto účely.
- Úvod do GNSS.
- Přehled přístupů k GNSS simulaci.
- Možnosti GNSS simulace za pomoci SDR.
- Sestavení generátoru GNSS signálu.
- Ověření sestaveného zařízení.

Rozsah grafických prací: dle pokynů vedoucího závěrečné práce

Rozsah průvodní zprávy: minimálně 35 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: GitHub - osqzss/gps-sdr-sim: Software-Defined GPS Signal Simulator [online]. 2018
Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. The Journal of Global Positioning Systems. 2018,
GPS Performance Standards & Specifications

Vedoucí bakalářské práce: **Ing. Jakub Steiner**

Datum zadání bakalářské práce: **7. října 2022**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání bakalářské práce: **7. srpna 2023**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

doc. Ing. Jakub Kraus, Ph.D.
vedoucí
Ústavu letecké dopravy

prof. Ing. Ondřej Přibyl, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání bakalářské práce.

Jan Slezáček
jméno a podpis studenta

V Praze dne ..... 7. října 2022

Abstrakt

Tato bakalářská práce pojednává o problematice týkající se simulace GNSS signálu. Oproti standardním způsobům, jako live-sky testování či použití komerčních simulátorů, je zde uvažována simulace pomocí softwarově definovaného rádia. Tato varianta přináší výrazné snížení časové i finanční náročnosti celého procesu. Nejprve se práce zaobírá obecným fungováním GNSS se zaměřením na nejpoužívanější systém GPS. Následuje teorie mapující technologie a technologické přístupy k testování přijímačů a simulaci GNSS signálu obecně. Poté navazuje kapitola poskytující úvod do problematiky simulátorů založených na softwarově definovaném rádiu, včetně podrobného přehledu využitelného hardwaru a softwaru. Práce pokračuje praktickou částí, jejíž náplní je sestavení generátoru GPS L1 signálu s využitím HackRF SDR. Zde je obsažen podrobný postup kompletace zařízení za pomocí volně dostupných skriptů a jeho ovládání. Dále jsou popsány provedené testy simulátoru a jejich výsledky. V závěru je diskutován budoucí rozvoj a další uplatnění vytvořeného zařízení.

Klíčová slova: GNSS, globální navigační satelitní systémy, softwarově definované rádio, simulace signálu, spoofing

Abstract

This bachelor thesis deals with the issue of GNSS signal simulation. Compared to standard methods this paper is dedicated to simulation using a software-defined radio. This option is advantageous due to significant reduction in time and cost of the whole process. Firstly, the thesis talks about the operating principle of GNSS in general with a focus on the most used system - GPS. Next, mapping technology and technological approaches for receiver testing and signal simulation. This is followed by a chapter summarizing general information about simulators based on software-defined radios, including a detailed overview of available hardware and software. The thesis continues with a practical part, which deals with the assembly of signal generator using the HackRF SDR. A detailed procedure for building the device using open-source scripts and operating it is included. Subsequently, the performed validation tests and their results are described. To conclude the thesis, future development and potential applications of the created device are discussed.

Keywords: GNSS, global navigation satellite systems, software-defined radio, signal simulation, spoofing

Poděkování

Rád bych poděkoval panu Ing. Jakubovi Steinerovi za ochotné a svědomité vedení této práce a jeho nápomocné rady. Dále patří velké díky mé rodině, která mě při tvorbě práce plně podporovala. V neposlední řadě děkuji své přítelkyni za poskytnutý čas pro psaní tohoto díla a Bc. Simoně Blaškové za spolupráci při prováděných měřeních.

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem Možnosti simulace GNSS signálu se zaměřením na SDR vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k bakalářské práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 1. srpna 2023 .....

Podpis

Obsah

Seznam obrázků

Seznam tabulek

Seznam symbolů a zkratek

ABAS	Aircraft-based augmentation system
ADC	Analog-to-digital Converter
ADS-B	Automatic Dependent Surveillance - Broadcast
ASIC	Application Specific Integrated Circuit
ATM	Air Traffic Management
BOC	Binary Offset Carrier
BPSK	Binary Phase Shift Keying
BRDC	Broadcast
$C/N0$	Carrier-to-noise ratio
CDMA	Code-division multiple access
CNS	Communication, Navigation, Surveillance
ČVUT	České vysoké učení technické
DAC	Digital-to-analog Converter
ECEF	Earth-centered, Earth-fixed
EGNOS	European Geostationary Navigation Overlay Service
FD	Fakulta dopravní
FDMA	Frequency division multiple access
FM	Frekvenční modulace
FPGA	Field Programmable Gate Array
GBAS	Ground based augmentation system
GNSS	Globální satelitní navigační systém (Global navigation satellite system)
GPS	Global positioning system
HAE	Height above ellipsoid
HDOP	Horizontal dilution of precision
HFT	High-frequency trading
HW	Hardware
IRNSS	Indian Regional Navigation Satellite System
ITU	International Telecommunication Union

LLH	Latitude, Longitude, Height
MCX	Micro coaxial connector
MSPS	Megasamples per second
NDDS	Nuclear detonation detection system
NMEA	National Marine Electronics Association
OS	Operační systém
PC	Personal computer
PDOP	Position dilution of precision
PLD	Programmable logic device
PNT	Position, Navigation and Time
PPS	Precision Positioning Service
PRN	Pseudo-random noise
PSD	Power Spectral Density
QZSS	Quasi-Zenith Satellite System
RF	Radio frequency
RINEX	Receiver Independent Exchange Format
RNSS	Radio navigation satellite system
RTCM	Radio Technical Commission for Maritime Services
RTK	Real Time Kinematic
Rx	Příjem (Receive)
ŘLP	Řízení letového provozu
SBAS	Satellite based augmentation system
SDR	Softwarově definované rádio (Software-defined radio)
SMA	SubMiniature version A
SPS	Standard Positioning Service
SW	Software
Tx	Vysílání (Transmit)
USB	Universal Serial Bus
UTC	Universal Time Coordinated
VDOP	Vertical dilution of precision
Wi-Fi	Wireless network protocols

Úvod

Globální navigační satelitní systémy (GNSS) poskytují možnost přesného určení polohy, času a funkci navigace. V současnosti jsou každodenně využívány k mnohým účelům, jako doprava, distribuce elektrické energie či bankovní transakce. Tato velmi přesná a dostupná technologie usnadňuje život nejen běžným uživatelům, ale je také nedílnou součástí kritické infrastruktury států. Mezi takovou infrastrukturu se řadí i letecká doprava, která využívá GNSS jako hlavní zdroj pro své soudobé navigační systémy. Dále je tato technologie nezbytná pro fungování přehledových zařízení jako jsou radary či multilaterační systémy, kde GNSS poskytuje přesnou časovou synchronizaci.

Odvětví satelitní navigace využívá široké spektrum různých přijímačů od každodenně používaných mobilních telefonů, přes vysoce spolehlivé letadlové přijímače, až po špičkové armádní technologie zahrnující například naváděcí systémy balistických raket. Za účelem ověření požadované přesnosti takových zařízení je nezbytné jejich testování. Spolu s měřením v reálném prostředí lze zvolit variantu použití komerčního GNSS simulátoru. Simulace signálu je důležitým nástrojem pro testování přijímačů a umožňuje širokou škálu možností jako je nastavení atmosférických podmínek, ukládání a opakování provedených měření, spouštění chybových scénářů a další. Cena takových přístrojů se však pohybuje v řádech stovek tisíc korun.

Kombinaci zachování některých funkcí klasických simulátorů a rapidního snížení finančních nákladů přináší moderní metoda spočívající v simulaci GNSS signálu prostřednictvím softwarově definovaného rádia (SDR) a volně dostupného programového vybavení. Nevýhodou oproti komerčním simulátorům je omezení počtu funkcí a nastavení generovaného signálu. Tato práce si bere za cíl zmapovat přístupy k simulování signálu GNSS a jejich porovnání. Následně je rozebrán princip fungování GNSS simulátorů na bázi SDR se shrnutím dostupného technického a programového vybavení.

Praktický cíl práce spočívá v sestrojení GNSS simulátoru za pomoci pořízeného SDR a volně dostupného skriptu. Posléze je podrobně popsán postup tohoto procesu a kompletní ovládání takového zařízení. Přístroj je následně validován a jsou vyhodnoceny výsledky těchto měření. Sestavené zařízení lze do budoucna použít například pro testování výkonnosti GNSS přijímačů či za účelem měření odolnosti vůči nelegálnímu rušení. Dále bude simulátor využíván laboratoří CNS/ATM systémů na Ústavu letecké dopravy Fakulty dopravní ČVUT v Praze.

1 Globální navigační satelitní systémy

Pojem globální navigační satelitní systémy (také globální družicové polohové systémy, zkr. GNSS) je definován jako systém určitého počtu vesmírných družic obíhající okolo zeměkoule po daných trajektoriích, umožňující přesné určení polohy a dalších parametrů. Obecně se jedná o jakoukoliv konstelaci těchto satelitů nezávisle na jejich počtu, trajektorii či provozovateli.

Soubor informací získaných z přijatého GNSS signálu se souhrnně nazývá PNT (angl. Position, Navigation and Time). Jeho tři části jsou [1]:

- **Position** (česky určení polohy) je schopnost definovat polohu přijímače v určitém geodetickém systému (např. WGS84 pro GPS). Standardním výstupem je zeměpisná šířka, zeměpisná délka a nadmořská výška přijímače (angl. latitude, longitude, altitude; zkr. LLA).
- **Navigation** (česky navigace) je schopnost definovat současnou a požadovanou polohu přijímače po aplikaci směrových, orientačních a rychlostních korekcí. Díky tomu je možné přijímač využít pro vedení objektu z jednoho místa na druhé po určité trase.
- **Time** (česky určení času) je schopnost získat a dlouhodobě udržovat přesný čas v referenci k standardu UTC (angl. Coordinated Universal Time) kdekoliv na světě.

1.1 Historie GNSS

Za předchůdce GNSS lze považovat pozemní rádiovou navigaci. Měření probíhalo na základě příjmu signálů vyslaných z jedné primární pozemní stanice (angl. master) a více sekundárních stanic (angl. slave či auxiliary). Následoval výpočet zpoždění těchto impulzů, ze kterého byla určena vzdálenost od stanic se známou polohou, z čeho byla odvozena poloha přijímače. Jako první z těchto systémů byl v roce 1942 spuštěn britský GEE. Ke konci 2. světové války následovaly americké systémy LORAN a DECCA [2, 3].

Po vypuštění první umělé družice do vesmíru, Sputnik 1 v roce 1957, se začalo uvažovat o využití satelitů pro určování polohy (tj. současný princip GNSS). Tato myšlenka byla uvedena do praxe roku 1964 vybudováním amerického vojenského systému TRANSIT (také NAVSAT), který sestával z šesti družic a byl využíván plavidly amerického námořnictva. Přesnost určení polohy dosahovala až 5 m. Dále mezi léty 1967 až 1978 proběhla výstavba systému Cyclon (také Cikada-M), který byl sovětskou obdobou projektu TRANSIT. Cyclon také sloužil pro námořní plavidla a

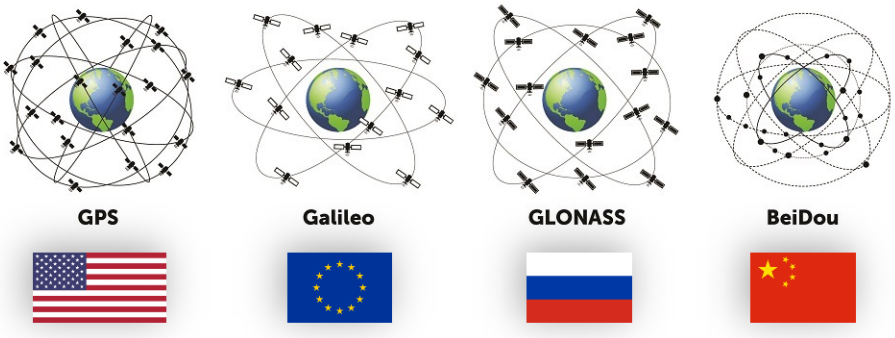
obsahoval celkem 31 družic. Oba zmíněné systémy používaly k určování polohy tzv. Dopplerův jev. Z důvodu nepřesnosti principu byl však ještě během 20. století jejich provoz ukončen [3].

Často používanou metodou určování polohy pomocí GNSS je tzv. trilaterace. Princip metody je založen na výpočtu zpoždění signálu mezi vysílačem a přijímačem a následným přepočtem na vzdálenost od družice. V trojdimenzionálním prostoru je nutná znalost vzdáleností od alespoň tří satelitů (blíže Kapitola 1.5). Prvním spuštěným GNSS systémem na základě trilaterace se stal v roce 1973 americký projekt Navstar GPS. Tři roky poté následoval sovětský (později ruský) systém GLONASS a na počátku 21. století čínský BeiDou a evropský Galileo [3].

1.2 GNSS konstelace

Jelikož pojem GNSS označuje všechny systémy satelitní navigace souhrnně, používáme pro jednotlivá uspořádání název konstelace. Ty se pak odlišují spravující zemí či organizací, počtem satelitů, počtem oběžných drah a jejich inklinací atd. V současné době existují čtyři provozuschopné konstelace s globálním pokrytím. Jejich grafické znázornění lze zhlédnout na Obrázku 1 [2, 4]:

- **GPS** – nejstarší systém z roku 1973 vlastněný armádou USA.
- **GLONASS** – ruský systém z roku 1976.
- **BeiDou** – čínský systém spuštěný roku 2000.
- **Galileo** – nejmladší systém spuštěný roku 2011, spravovaný Evropskou unií.



Obrázek 1: Čtyři základní GNSS konstelace [5]

Mimo tyto globální systémy existují také dvě konstelace s lokálním pokrytím. Jedná se o japonský QZSS (také Michibiki) a indický IRNSS (také NavIC). Signál z těchto satelitů lze přijímat pouze na území zmíněných států a v jejich okolí [2].

Za účelem zvýšení výkonnostních parametrů GNSS systémů se využívají tzv. augmentační systémy. Mezi nejpoužívanější patří SBAS, který poskytuje korekce pseudovzdálenosti a informace o integritě systému. Činí tak na základě dat z referenčních stanic a pokrývá vždy danou oblast (např. EGNOS území Evropy). V oblasti letecké dopravy se dále využívají augmentační systémy ABAS a GBAS. Vzhledem k zaměření praktické části práce na simulaci GPS signálu je dále v práci vysvětlen princip dané problematiky nejprve pro GNSS a poté konkrétně pro systém GPS [6].

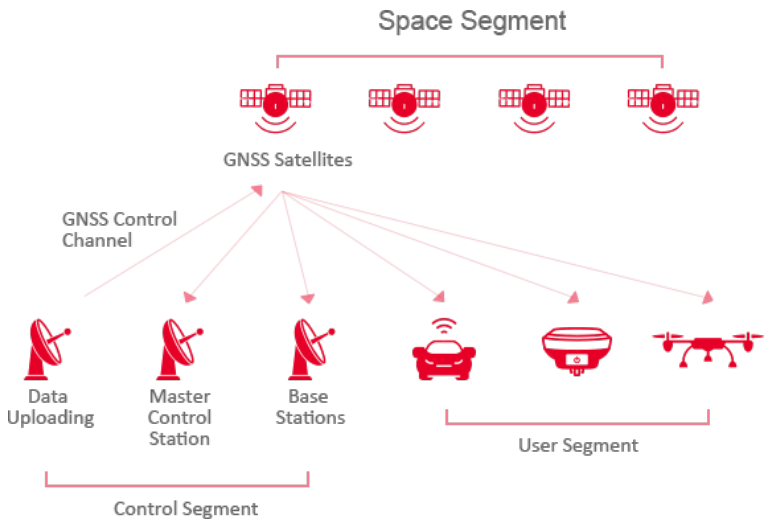
1.3 Architektura GNSS

I přes odlišné uspořádání jednotlivých konstelací GNSS (počet družic, výška a inklinace oběžných drah atd.) lze obecně rozdělit jejich architekturu na tři hlavní části - kosmický, řídící a uživatelský segment. Propojení těchto segmentů je zobrazeno na Obrázku 2.

Kosmický segment obsahuje jádro celého systému, tj. určitý počet umělých družic obíhající zeměkouli po drahách s přesně danými parametry. U současných GNSS systémů se používá 3 nebo 6 oběžných drah s inklinací 55° až 65°. Tyto družice vysílají k Zemi nepřetržitý jednosměrný rádiový signál, obecně s frekvencí 300 GHz a méně. Na palubě satelitů se také nacházejí velmi přesné atomové hodiny [2].

Řídící segment (někdy také pozemní) sestává z různých pozemních objektů, jejichž úkolem je řízení a monitorování celého systému. Tyto objekty mohou být například senzory, monitorovací stanice, centrální řídící středisko a další. Typickým zásahem do řízení je mírná úprava dráhy letu družice či korekce jejich hodin [7].

Uživatelský segment se skládá z jednotlivých GNSS přijímačů, které analyzují příchozí signál od družic a provádějí výpočty k určení PNT. Tyto přístroje pokrývají velkou škálu předmětů od mobilních telefonů a laptopů až po dopravní prostředky a vojenské technologie.



Obrázek 2: Segmenty GNSS [8]

1.4 GNSS signál

1.4.1 Struktura signálu

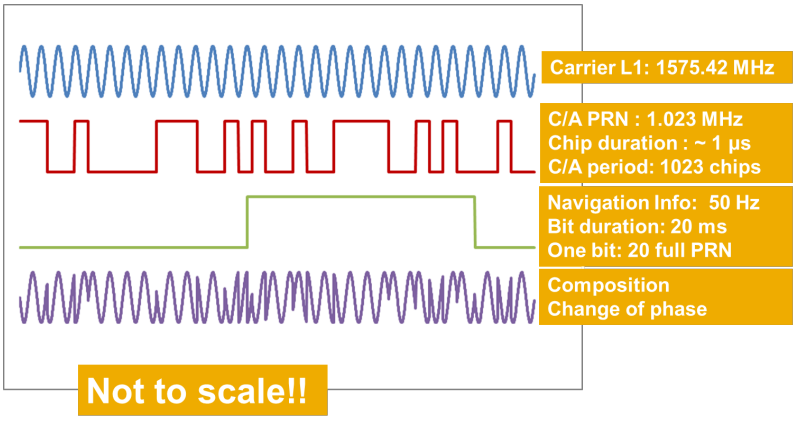
Základem každého GNSS systému je soustava satelitů s nepřetržitým rádiovým vysíláním. Toto vysílání vzniká nejčastěji jako kompozice třech signálů – nosné vlny, pseudonáhodného kódu (zkr. PRN) a navigační zprávy, jak lze zhlédnout níže na Obrázku 3. Princip vzniku konečného GNSS signálu spočívá v namodulování PRN a navigační zprávy na nosnou vlnu. Změny v sekvenci těchto dvou hlavních komponentů se následně projeví jako změny fázového posunu výsledné elektromagnetické vlny. V současné době se nejčastěji používá modulace BPSK (angl. Binary Phase Shift Keying), u moderních signálů také modulace BOC (angl. Binary Offset Carrier) [9, 10].

- **Nosná vlna** (angl. carrier) je základem pro GNSS signál. Jedná se o nepřetržité elektromagnetické vlnění ve tvaru sinusoidy s danou frekvencí. Každá GNSS konstelace vysílá na nosných frekvencích z určitých částí spektra L (tj. rozmezí 1 GHz – 2 GHz). Pásma pro GNSS signály jsou vyhrazena pouze k tomuto účelu a jejich jiné využití je zakázané [9].

- **Pseudonáhodný kód** (angl. pseudo-random noise, PRN) nazývaný také dálkoměrný, je posloupnost čísel 0 a 1 vysílaná s danou frekvencí. V důsledku velké periody opakování se zdánlivě jeví jako náhodná. Ve skutečnosti se jedná o přesně definovaný kód, který je unikátní pro každou z družic. V případě, že není využito fázového měření, je PRN v signálu přítomen především za účelem vypočítání vzdálenosti přijímač-satelit, tzv. pseudovzdálenosti

(blíže Kapitola 1.5.1). Při použití principu CDMA (viz Kapitola 1.5.2) je PRN využit také pro jednoznačnou identifikaci satelitu [3].

- **Navigační zpráva** je binárně zakódovaná posloupnost obsahující informace, jež mimo jiné umožňují přijímači jednoznačně určit polohu satelitu v čase. Skládá se z efemerid družice (popis oběžné dráhy v čase) a almanachu (popis všech oběžných drah systému, zdraví satelitu atd.) [3].

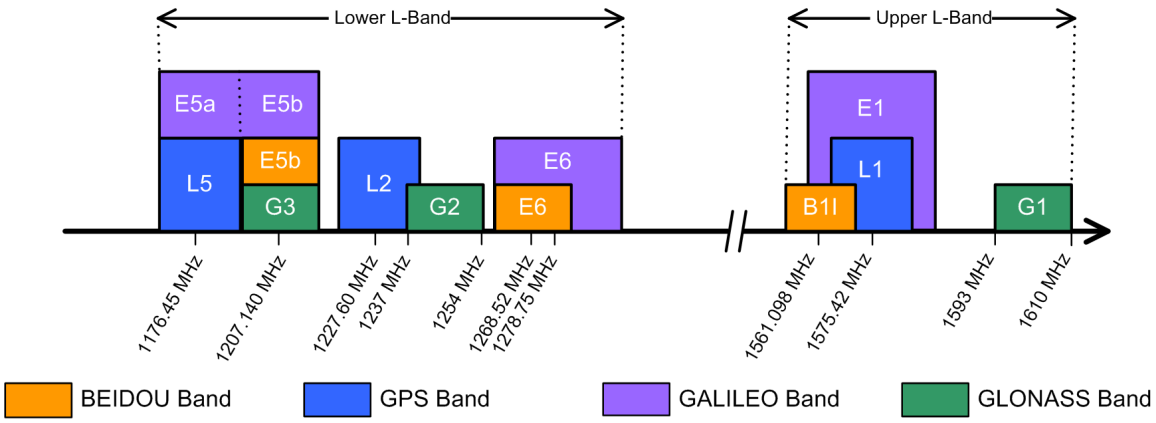


Obrázek 3: Příklad struktury GPS signálu [9]

1.4.2 Vyhrazené frekvence

U každého GNSS systému rozhodne Mezinárodní telekomunikační unie (zkr. ITU) o vysílacím pásmu, případně také o frekvenci nosné vlny. Pro tyto účely byly vyhrazeny oblasti v pásmu L pro systémy RNSS (rádiové navigační satelitní systémy). Jedná se o pásma 1164 MHz – 1300 MHz (tzv. lower L-band) a 1559 MHz – 1610 MHz (tzv. upper L-band). V současnosti každá konstelace vysílá alespoň na dvou různých frekvencích, díky čemuž je možné například zmírnění chyby, kterou způsobuje průchod signálu ionosférou [3, 11].

Pro danou konstelaci je rozsah vždy definován středovou frekvencí a šířkou pásma. V pásmu „upper L-band“ jsou poskytovány převážně služby pro veřejnost, zatímco v pásmu „lower L-band“ obvykle nalezneme vysílání pro specifické účely a autorizované uživatele. Frekvence jsou poté označeny různými písmeny dle dané konstelace. Systém GPS využívá L1, L2 a L5, systém Galileo E1, E5a, E5b, E6 apod. Kompletní rozdělení frekvencí u systémů GPS, Galileo, GLONASS a BeiDou shrnuje Obrázek 4 [12].



Obrázek 4: Frekvenční pásma GNSS konstelací [12]

1.4.3 Struktura GPS signálu

Jelikož americký systém GPS začínal jako ryze vojenský, byly jeho služby po civilním zpřístupnění roku 1983 rozčleněny. Pro neautorizované uživatele byla vyhrazena „standardní polohová služba“ (zkr. SPS), zatímco autorizovaným uživatelům slouží „přesná polohová služba“ (zkr. PPS) [3].

Systém GPS vysílá na třech frekvenčních pásmech:

- **Pásmo GPS L1** – frekvence: 1575,42 MHz, šířka pásma: 15,345 MHz
- **Pásmo GPS L2** – frekvence: 1227,60 MHz, šířka pásma: 11,000 MHz
- **Pásmo GPS L5** – frekvence: 1176,45 MHz, šířka pásma: 12,500 MHz

Systém GPS využívá CDMA přístupu. Všechny družice tak vysílají na stejné frekvenci a k jejich rozlišení dochází pomocí různých PRN kódů (blíže Kapitola 1.5.2). V současné době jsou pro civilní použití vysílány čtyři druhy signálů – původní L1 C/A a nově zavedené L2C, L5 a L1C. Mezi neveřejné služby se řadí původní signál P(Y) a zmodernizované signály L1M a L2M pro vojenské účely [13].

Signál L1 C/A (z angl. Coarse/Acquisition) je jedním z původních signálů (je vysílán od samotného spuštění systému) a poskytuje uživatelům službu SPS. Jedná se o základní PRN kód, který je namodulován na nosnou frekvenci L1. Je dostupný široké veřejnosti a jeho obsah není šifrovaný [3].

Signál P(Y) („P“ z angl. Precision) se řadí také mezi původní a poskytuje službu PPS. Charakteristikou se jedná o PRN kód, který je namodulován na frekvenci L1 nebo L2. Na rozdíl od

C/A kódu je jeho použití omezené pouze pro vojenské účely. Obsah P(Y) kódu je zašifrován tak, že některé jeho bity obsahují převrácenou hodnotu. Bez příslušného klíče – který určuje, o jaké bity jde – jej tak není možné dešifrovat a využít pro určení polohy [3].

Signál L2C je zmodernizovaný signál pro civilní využití v předprovozním stádiu vývoje. Ve vysílání je namodulován na frekvenci L2. V kombinaci s příjmem L1 C/A signálu umožňuje lepší korekci ionosférické chyby [14].

Signál L5 je zmodernizovaný signál určený výhradně pro zvýšení bezpečnosti letecké dopravy. Momentálně se nachází v předprovozním stadiu vývoje. Opět umožňuje lepší korekci chyb a má vyšší vysílací výkon [14].

Signál L1C je čtvrtým signálem pro civilní využití, který se nachází ve vývojovém stadiu. Jeho úkolem je především zajištění interoperability mezi systémy GPS a Galileo. K modulaci na nosnou vlnu požívá moderní metodu BOC [14].

Signály L1M a L2M („M“ z angl. Military) jsou zmodernizovanými signály výhradně pro vojenské použití. Ve vysílání jsou namodulovány na frekvenci L1 nebo L2 novou metodou BOC. V budoucnosti by měly nahradit P(Y) kódy, oproti kterým mají vyšší odolnost vůči rušení a vyšší vysílací výkon [15].

Mimo výše zmíněné frekvence existuje také pásmo GPS L3, které je využíváno systémem detekce jaderné detonace (zkr. NDDS) k určení, zdali a kde došlo k jadernému výbuchu. Dále je ve fázi vývoje pásmo GPS L4, které by mohlo sloužit jako další nástroj opravy ionosférické chyby. Přehled všech pásem GPS shrnuje Tabulka 1 [16].

Tabulka 1: Přehled frekvenčních pásem GPS [13]

Pásmo	Středová frekvence	Přístup	Dostupné služby
GPS L1	1575,42 MHz	CDMA	L1 C/A, P(Y), L1C, L1M
GPS L2	1227,60 MHz	CDMA	P(Y), L2C, L2M
GPS L3	1381,05 MHz	Využíváno pro detekci jaderných výbuchů	
GPS L4	1379,91 MHz	Ve fázi vývoje	
GPS L5	1176,45 MHz	CDMA	L5 I, L5 Q

1.5 Princip fungování GNSS

1.5.1 Obecný princip

Výpočet polohy GNSS přijímače je založen na následujícím principu. Signál vyslaný satelitem putuje rychlostí světla ($c \approx 3 \cdot 10^9\ m \cdot s^{-1}$). Při znalosti doby putování – jako rozdílu času vyslání a času příjmu – můžeme vzdálenost přijímač-satelit získat dosazením do Rovnice 1:

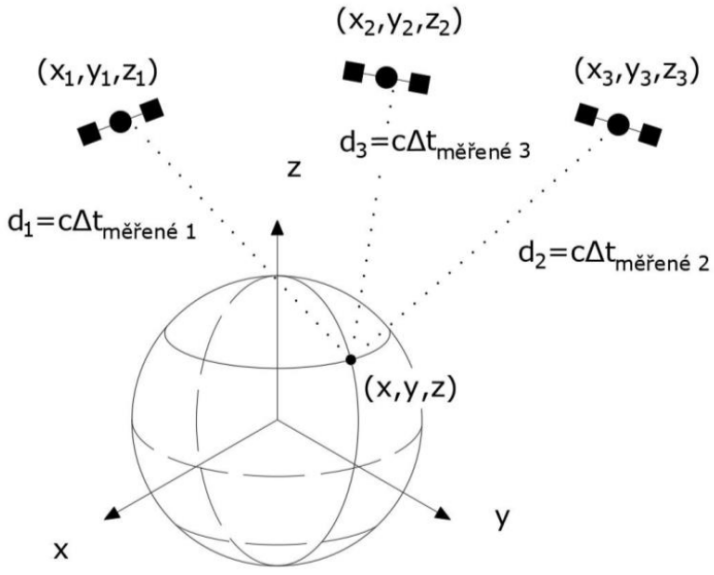
$$c \cdot \delta t = D \tag{1}$$

c = rychlost světla

δt = doba putování signálu od satelitu k přijímači

D = vzdálenost přijímač-satelit

Po určení této vzdálenosti se přijímač nachází na některém bodě kulové plochy se středem v poloze satelitu a poloměrem D. Ve 3D prostoru je zapotřebí znalost vzdáleností od alespoň tří satelitů, což zredukuje množinu řešení na dvě možné polohy, které vzniknou jako průnik tří kulových ploch. Po eliminaci jednoho řešení, které se nenachází v blízkosti povrchu Země, zbývá pouze jediná možná poloha přijímače, jak naznačuje Obrázek 5.



Obrázek 5: Příjem signálu od tří satelitů [17]

Ve skutečnosti však nelze přesně synchronizovat hodiny satelitu a přijímače. Z tohoto důvodu vstupuje do rovnice čtvrtá neznámá δt_0, která se rovná rozdíl času konstelace a přijímače. Pro jednoznačné určení polohy je tedy nutné přijímat signál od alespoň čtyř satelitů, jelikož přijímač počítá soustavu čtyř Rovnic 2 o čtyřech neznámých $(x, y, z, \delta t_0)$:

$$c \cdot \delta t_{mer,i} = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + c \cdot \delta t_0 \tag{2}$$

$\delta t_{mer,i}$ = naměřená doba putování signálu od i-tého satelitu k přijímači

x_i, y_i, z_i = poloha i-tého satelitu v čase vyslání signálu

x, y, z = poloha přijímače

δt_0 = rozdíl hodin satelitu a přijímače

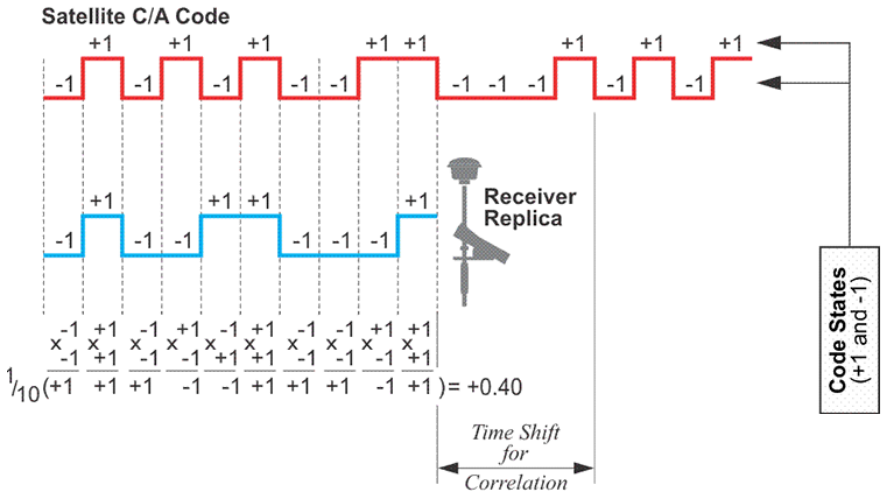
Součin $c \cdot \delta t_{mer,i}$ se také nazývá pseudovzdálenost. Podle Rovnice 2 se jedná o součet reálné vzdálenosti (vyjádřeno členem pod odmocninou neboli délkou vektoru) a vzdálenosti generované odchylkou hodin satelitu a přijímače. Pseudovzdálenost je proto pouze orientační hodnota, která neodpovídá skutečné vzdálenosti.

1.5.2 Postup určení polohy

Prvním nezbytným procesem po příjmu signálu je jednoznačná identifikace satelitu, který jej vyslal. K tomuto účelu se v současné době používá dvou metod - frekvenčního a kódového dělení. Při frekvenčním dělení (zkr. FDMA) vysílá každý satelit dané konstelace na nosné vlně s jinou frekvencí. Přijímač tak dokáže identifikovat satelit změřením této frekvence. Tuto metodu současně využívají pouze satelity ruského systému GLONASS. Druhým způsobem je kódové dělení (zkr. CDMA), při kterém všechny satelity vysílají na stejné nosné frekvenci a k jejich rozlišení dochází pomocí unikátních PRN kódů. Jedinou nevýhodou je omezené množství těchto kódů, jelikož lze využívat pouze ty, které mají dobré korelační vlastnosti (vysvětleno dále) [18, 19].

Po identifikaci satelitu přijímač načte repliku jím vysílaného PRN kódu a spustí ji. V tuto chvíli se replika a skutečně přijímaný signál shodují ale nejsou synchronizovány v čase. K tomuto účelu slouží tzv. autokorelace, což je proces, při kterém přijímač posouvá repliku v čase do doby, než bude plně synchronizována s originálem. Na začátku je nutné převést hodnoty kódu 0/1 (angl. code chips) do hodnot -1/1 (angl. code states). Dalším krokem je násobení vždy dvou code states, které se nacházejí ve stejném čase. Následně jsou výsledky násobení pro určitý časový úsek sečteny

a vyděleny jejich celkovým počtem. V případě dosažení plné korelace se výsledná hodnota rovná číslu 1. Grafická reprezentace autokorelace je znázorněna na Obrázku 6 [20, 21].



Obrázek 6: Princip autokorelace signálu [17]

Z předchozího výpočtu lze odvodit tzv. time-shift = čas, o který bylo nutné posunout repliku kódu, aby korelovala s originálem. Tato hodnota koresponduje s časem putování signálu od satelitu k přijímači, díky čemuž je získána neznámá $\delta t_{mer,i}$ a dosazena do Rovnice 2 [20].

Následuje přesné určení polohy daného satelitu. Díky znalosti $\delta t_{mer,i}$ je možné určit dobu vyslání signálu, která je dosazena do keplerovských rovnic popisující oběžnou dráhu družice. Ty jsou součástí efemerid a almanachu z navigační zprávy. Po tomto procesu získá přijímač polohu satelitu x_i, y_i, z_i, kterou dosadí do Rovnice 2 [20, 22].

Na závěr je do Rovnice 2 dosazena rychlost světla a po příjmu signálu z alespoň čtyř satelitů proběhne výpočet. Výsledkem je poloha přijímače (x, y, z) a chyba hodin přijímač-satelit (δt_0). Zbývajícím krokem je převod ze soustavy ECEF (X, Y, Z) do hodnot LLH (pro GPS např. systém WGS84) a času do formátu UTC. Data jsou poté dále distribuována prostřednictvím univerzálních formátů jako jsou NMEA 0183, RTCM SC-104, RINEX a další [23].

Výše zmíněná metoda výpočtu se jinak nazývá *kódová*. Často využívaným způsobem je také metoda *fázová*, která získává polohu přímým měřením fázových posunů vysílané vlny. Přestože se jedná o velmi přesnou metodu, její nevýhodou je neznámý počet vln mezi satelitem a přijímačem, který je k výpočtu nezbytný. Z tohoto důvodu musí být do systému zapojeny pozemní referenční stanice, u nichž je poloha přesně známa. Nejpoužívanější fázovou metodou je tzv. RTK (angl. Real

Time Kinematic), kdy se poloha jednoho bodu určuje jako relativní k bodu druhému (tj. k referenční stanici) [10, 23].

Po příjmu signálu lze u viditelných satelitů určit různé parametry. Pro vyjádření intenzity GNSS signálu se používá poměr výkonu přijatého signálu k intenzitě okolního šumu označovaný jako $C/N0$. Dále jsou často uváděny informace o poloze satelitu, kterými jsou azimut a elevace [24].

1.5.3 Chyby měření

V reálném prostředí je rozdíl hodin satelitu a přijímače pouze jednou z chyb měření. Další odchylky způsobuje například [6]:

- průchod signálu atmosférou, tj. ionosférická a troposférická chyba ($\varepsilon_{ion}, \varepsilon_{trop}$)
- chybné určení polohy satelitu, tj. efemeridická chyba (ε_{ephem})
- odraz signálu od jiných objektů, tj. chyba vícecestného šíření (ε_{mp})
- dilatace času a další méně významné chyby (ε)

Z důvodu přítomnosti těchto chyb je rovnice pro určení polohy z GNSS často uváděna ve tvaru, který zobrazuje Rovnice 3 [20, 6]:

$$c \cdot \delta t_{mer,i} = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + c \cdot \delta t_0 + \varepsilon_{ion} + \varepsilon_{trop} + \varepsilon_{ephem} + \varepsilon_{mp} + \varepsilon \quad (3)$$

Výsledek výpočtu je také ovlivněn polohovou chybou měření (zkr. PDOP), která je určena geometrickým rozložením satelitů kolem přijímače. Ta se skládá z horizontální (HDOP) a vertikální (VDOP) složky. Obecně lze říct, že pokud se satelity užívané k výpočtu polohy nacházejí dále od sebe, tak je tato chyba nižší než v případě, kdy jsou od sebe vzdáleny méně [6].

1.6 Rušení GNSS signálu

Spolu s rozvojem GNSS technologií dochází v současné době ke stále častějšímu výskytu GNSS rušení. Jde o stav, kdy je vysílán nežádoucí signál s obvykle vyšším výkonem než signál autentický. Většina zařízení upřednostní přijímat právě tento signál a dochází tak k úplnému zarušení přístroje nebo dokonce k chybnému určení polohy. Dle použité technologie lze GNSS rušení rozlišit na tři kategorie – jamming, spoofing a meaconing [25].

1.6.1 Jamming

V případě jammingu se jedná o vysílání signálu o vysokém výkonu na frekvenci blízké nebo shodné s GNSS. Po přijetí signálu dochází ke ztrátě autentického vysílání a přístroj není schopen vypočítat svou polohu ani další parametry. I přestože je tento druh rušení v mnoha zemích nezákonný, náklady na pořízení jammeru jsou poměrně malé. Jamming je tak velmi snadným, účinným a častým způsobem GNSS rušení [20, 25].

1.6.2 Spoofing

Komplexnějším ale také obtížněji proveditelným způsobem rušení je tzv. spoofing. V tomto případě se nejedná pouze o interferenci autentického signálu, nýbrž o jeho napodobení. Spoofer tak vysílá falešný GNSS signál, který je po přijetí chybně rozpoznán jako autentický a dochází k mylnému výpočtu polohy, času a dalších parametrů [20, 25].

Spoofing je také jednou z funkcí tzv. GNSS simulátorů, což jsou pokročilé přístroje, které slouží ke generování GNSS signálu. Dále vytvářejí fiktivní pohyb satelitů a umožňují například modelování dynamických pohybů vozidel, konfiguraci atmosférických vlivů či simulaci chybových scénářů. V běžném užívání se pojem spoofing pojí spíše s negativními vlivy, kdežto simulace bývá prováděna za účelem testování GNSS přijímačů [26].

U spoofingu se jedná o hůře odhalitelný druh rušení, který je ovšem nákladnější a komplikovanější na realizaci. S příchodem nových technologií se ovšem tyto náklady výrazně snižují a jednoduchý spoofer lze tak sestrojit i za pomocí softwarově definovaného rádia.

1.6.3 Meaconing

Poslední metodou GNSS rušení je tzv. meaconing, při kterém přístroj nejprve přijímá autentický signál a poté ho s určitým zpožděním a vyšším výkonem znovu vysílá. Tento zpožděný signál způsobí chybné určení polohy a času v přijímači. Útok má tudíž stejný výsledek jako spoofing, ale je hůře odhalitelný. Na rozdíl od předchozích dvou typů musí přístroj fungovat zároveň jako vysílač i přijímač [20, 27].

2 Možnosti GNSS simulace a testování GNSS zařízení

Systémy GNSS zažívají v posledních desetiletích významný rozvoj a jejich aplikace lze nalézt v širokém spektru odvětví, např. doprava (letecká, železniční, silniční), vojenství, geografie, geodézie a další. S aktuálním růstem je kladen větší důraz na přesnost, dostupnost, integritu a spojitost těchto systémů. Mimo satelitů je nutné výkonnostní parametry testovat také u samotných přijímačů. Mezi ně řadíme nejen precizní GNSS přijímače pro letadla, automobily, profesionální vojenskou techniku a geodetická zařízení, ale také každodenně používaná zařízení jako mobilní telefony, tablety či laptopy.

Tato kapitola přináší srovnání dvou hlavních možností testování GNSS přijímačů [28]:

- live-sky testování
- testování pomocí GNSS simulátorů

2.1 Live-sky testování

Prvním přístupem je tzv. live-sky testování neboli testování v reálném prostředí. Velice jednoduchý princip spočívá ve využití reálného signálu z GNSS satelitů. Ten může být přijímán přímým spojením s anténou, či jsou využity antény na budově společnosti, přes které je signál přenášen do laboratoří a následně pomocí koaxiálních kabelů nebo prostřednictvím Bluetooth přímo do testovaného přijímače [28].

Výraznou výhodou této metody je její jednoduchost a nízké náklady. Dále není nutné dlouze vyškolovat zaměstnance obsluhující zařízení či pořizovat další vybavení. Naopak nevýhodu je nemožnost celkově kontrolovat, regulovat či konfigurovat aspekty ovlivňující testování. Z toho důvodu jsou testy omezeny tím, co je dovoleno aktuálním stavem konstelace. Nelze testovat jakýkoliv poruchový stav satelitů, příjem signálu od momentálně nedostupných konstelací a signálů ve fázi vývoje či chování přijímače na jiné lokaci. Problémem může být také riziko momentálních interferencí s jinými signály. I přes nevýhody se mnoho českých firem stále kloní k přístupu live-sky testování, převážně z důvodu jeho snadné realizace. Výhody a nevýhody jsou shrnuty v Tabulce 2 [29, 28].

Tabulka 2: Výhody a nevýhody live-sky testování [28, 29, 30]

Výhody	Nevýhody
Nízké náklady	Riziko interference s jinými signály
Jednoduché provedení	Neopakovatelnost testu
Bez potřeby dalšího zařízení	Nemožnost ovládat/upravit signál
Minimální zaškolení obsluhy	Nemožnost testovat všechny konstelace
Bez nutnosti laboratoře	Nemožnost testování za jiných podmínek
	Testování vždy na daném místě
	Vyšší časová náročnost

2.2 Testování pomocí GNSS simulátorů

Druhým přístupem je testování přijímačů pomocí GNSS simulátorů nebo také generátorů GNSS signálu. V tomto případě se jedná o použití zařízení, které je schopno generovat signál totožný s tím, který je vysílán satelity. Po přijetí je tento signál rozpoznán jako autentický a je použit pro výpočet výkonnostních parametrů.

K vytváření signálu shodného s autentickým dochází uvnitř simulátoru pomocí softwarové aplikace na základě dat o přesné trajektorii GNSS satelitů v daný čas. Ty jsou do zařízení nahrány uživatelem (popř. automaticky) formou almanachu či efemerid. Typicky na základě uživatelem požadované polohy je poté vytvořen elektromagnetický signál, který je přenesen na anténu a vysílán na dané frekvenci. Alternativou je přímý přenos signálu přes kabel [29].

Moderní simulátory jsou často schopny i mnohem pokročilejších procesů než vysílání samotné statické polohové informace. Mnohdy je jejich součástí např. modelování dynamického pohybu vozidel ve všech šesti stupních volnosti. Dále je plně kontrolovatelný pohyb všech simulovaných satelitů v rámci více než jedné konstelace. Nechybí ani různé chybové scénáře obsahující např. ztrátu signálu či poruchu satelitu. Možná je také regulace atmosférických podmínek včetně nastavení teploty, oblačnosti či troposférických a ionosférických chyb [31, 32].

Z výše uvedeného vyplývají hlavní výhody GNSS simulátorů, kterými jsou: plná kontrola a regulace vysílaného signálu, testování chybových a poruchových scénářů, použití reálně nedostupných konstelací, nastavení environmentálních podmínek a simulace pokročilejších procesů jako pohybu vozidel. Kladným aspektem je také možnost ukládání jednotlivých testů a

jejich následné opakování. Na druhou stranu může být nevýhodou možnost špatného nastavení testu či nutnost pořízení dalšího vybavení, proškolení obsluhy a s tím spojené navýšení nákladů. Výhody a nevýhody testování pomocí GNSS simulátorů jsou uvedeny v Tabulce 3 [31, 32].

Tabulka 3: Výhody a nevýhody GNSS simulátorů [30, 31, 32]

Výhody	Nevýhody
Plná kontrola nad vysílaným signálem	Vyšší náklady
Testování více konstelací	Nutnost pořízení dalšího zařízení
Možnost opakovat testování	Zapotřebí laboratoř
Nastavení environmentálních podmínek	Nutné proškolení obsluhy
Bez rušení cizími signály	Možnost špatného nastavení
Časově nenáročné	

GNSS simulátory lze rozčlenit do dvou kategorií. První jsou „profesionální“ simulátory od osvědčených firem, které obsahují kompletní vybavení (HW + SW) pro simulaci GNSS signálu. Druhá kategorie umožňuje simulaci s využitím tzv. softwarově definovaného rádia, což je přístroj, jehož fungování určuje uživatelem nahraný software.

2.2.1 Profesionální GNSS simulátory

Pod tímto pojmem si lze představit jakékoliv kompletní zařízení schopné generovat GNSS signál. Tyto simulátory jsou tzv. ready-to-use a k provozu potřebují pouze zdroj elektrické energie, vysílací anténu a často také připojení k internetu. Součástí zařízení je vždy hardware, který na základě požadavků generuje GNSS signál a často také ovládací software. HW zahrnuje různé základní desky s přesnými postupy a sadami instrukcí [33].

Díky výše zmíněným informacím jsou profesionální simulátory schopny vykonávat pouze funkce, pro které byly navrženy, což je odlišuje od SDR simulátorů. Výhodou použití technologie komerčních simulátorů je vysoká přesnost dosažených výsledků vycházející z dlouhodobých zkušeností výrobců a jejich specializace v tomto oboru. Jako nevýhody lze uvést velmi vysoké pořizovací náklady (řádově stovky tisíc až milion korun [34]) a až na výjimky nemožnost využití zařízení pro jiné účely [33].

V současnosti disponují profesionální GNSS simulátory typicky následujícími funkcemi [32, 35]:

- simulace všech konstelací s celosvětovým pokrytím na vícero kanálech
- simulace regionálních konstelací (IRNSS, QZSS)
- simulace augmentačních signálů (SBAS)
- vysílání veřejných i šifrovaných signálů
- ukládání testovacích scénářů a jejich opětovné spouštění
- nastavení atmosférických podmínek
- implementace vlivu jammingu a spoofingu
- modelování dynamických trajektorií

Většina výrobců implementuje do svých zařízení moderní simulační techniku hardware-in-loop (HIL), při níž je používán nejen signál vypočítaný přístrojem, ale také reálný signál ze satelitů GNSS. To velice usnadňuje tvorbu navigační zprávy a snižuje čas přípravy simulace. HIL je jedním ze způsobů tzv. real-time simulace [36].

Lze rozlišovat dvě elementární varianty profesionálních GNSS simulátorů:

➤ **Vektorové generátory signálu** – zařízení, u nichž lze nastavit jako jednu z možností vysílání GNSS signálu. V některých případech je nutné modul pro GNSS k tomuto přístroji dokoupit. Jedním z výrobců takových zařízení je např. *Rohde & Schwarz* [37].

➤ **Specifické GNSS simulátory** – přístroje, které vysílají pouze GNSS signály. Tento druh simulátorů v současné době na trhu převažuje a jako příklad výrobce můžeme uvést firmu *Spirent* [35].

V rámci bakalářské práce byla provedena rešerše současného stavu trhu, na jejímž základě byla vytvořena myšlenková mapa obsahující aktuální výrobce GNSS simulátorů, jejich produkty a specifické parametry těchto zařízení. Dle výzkumu jsou předními výrobci firmy *Spirent, Safran, Syntony GNSS, LabSat, Rohde & Schwarz* a další. Zároveň bylo zjištěno, že je možné zakoupit také bazarové simulátory prostřednictvím serverů jako např. *Ebay*. Pro příklad jsou z rešerše uvedeny 3 profesionální simulátory, včetně bodového popisu [35, 38, 37]:

Spirent: GSS9000

- specifický GNSS simulátor, fotografie na Obrázku 7
- simulace GPS, Galileo, GLONASS, BeiDou, QZSS, IRNSS, SBAS, spoofing
- technika HIL, uživatelský software SimGEN
- přesnost pseudovzdálenosti: 0,3 mm RMS, relativní rychlost: 120 km/s
- Cena: cca **620 000,- Kč**

Obrázek 7: Simulátor GSS9000 [35]

Safran (dříve Orolia): Skydel GSG-7

- specifický GNSS simulátor, fotografie na Obrázku 8
- simulace GPS (L1, L2, L5), Galileo, GLONASS, BeiDou, QZSS, IRNSS, SBAS
- technika HIL, uživatelský software Skydel
- přesnost pseudovzdálenosti: 1 mm, relativní rychlost: 1500 km/s
- Cena: na vyžádání (předchůdce GSG 5/6 cca **700 000,- Kč**)

Obrázek 8: Simulátor Skydel GSG-7 [38]

Rohde & Schwarz®: SMBV100B

- generátor elektromagnetického signálu, fotografie na Obrázku 9
- včetně funkce GNSS simulátoru, dále např. vysílání signálů 5G, LTE, WLAN atd.
- simulace GPS (L1, L2, L5), Galileo, GLONASS, BeiDou, QZSS, SBAS
- různé možnosti modulací (amplitudová, I/Q, digitální)
- Cena: cca **760 000,- Kč**

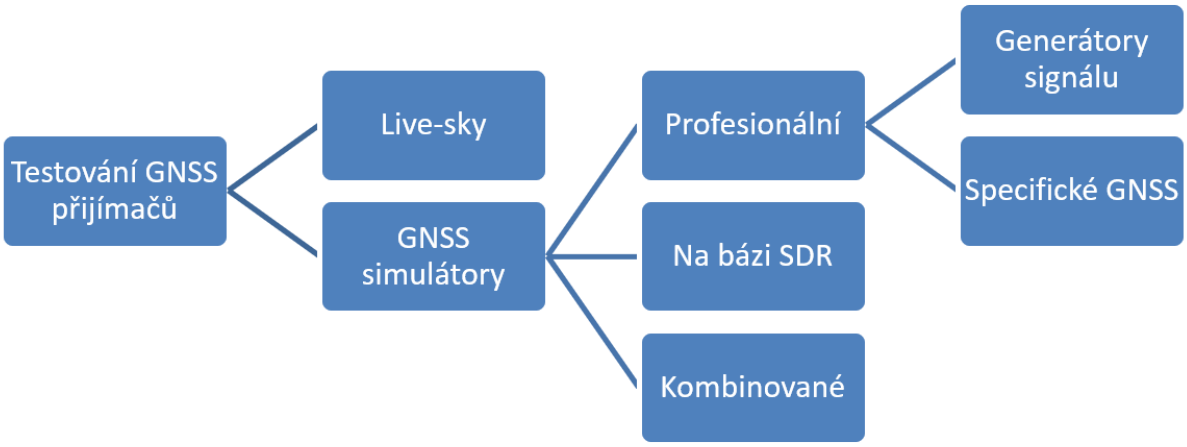
Obrázek 9: Simulátor SMBV100B [37]

2.2.2 GNSS simulace pomocí SDR

Druhá kategorie zahrnuje simulátory GNSS signálu, které jsou založeny na zařízení s názvem softwarově definované rádio (zkr. SDR). Tento způsob simulace obsahuje mnoho výhod jako například univerzální využití této technologie či výrazné snížení pořizovacích i provozních nákladů. GNSS-SDR simulaci se podrobně věnuje Kapitola 3.

Pro úplnost lze přidat třetí možnost simulace, která vznikla kombinací obou předchozích. Tato varianta se na trhu začala vyskytovat teprve v cca posledních dvou letech a spočívá v prodeji klasických profesionálních simulátorů, jejichž některé hardwarové prvky (např. mateřské desky) byly nahrazeny softwarově definovanými rádii. Toto uspořádání umožňuje rozsáhlejší možnosti uživatelské konfigurace, nesnižuje ovšem vysoké pořizovací náklady. Jako příklad lze uvést simulátor BroadSim od *Safranu* [39] či zařízení GSS6300 od firmy *Spirent* [40].

Možnosti testování GNSS přijímačů shrnuje Obrázek 10.



Obrázek 10: Dělení způsobů testování GNSS přijímačů

3 Simulace GNSS signálu pomocí SDR

Metoda GNSS simulace, v kontextu této práce, spočívá v generování GNSS signálu pomocí softwarově definovaného rádia. Jedná se o techniku, při které je hardware přístroje plně programovatelný a lze ho modifikovat a využít více způsoby podle použitého softwaru. Při testování GNSS přijímačů se tak SDR simulátor může chovat např. jako jammer či spoofer. Díky tomu není nutné pořizovat více zařízení a lze použít jediné softwarově definované rádio pro více účelů [33].

První výhodou SDR oproti klasickým simulátorům je tedy široké spektrum možností, jak lze rádio využít. Jako druhý benefit lze zmínit významné snížení nákladů, které se pojí s pořízením i samotným provozem zařízení. Při uvážení ceny elektřiny cca 6 Kč/kWh (k únoru 2023, [41]) lze provést porovnání nákladů u dvou typických zástupců profesionálního a SDR simulátoru, které je uvedené v Tabulce 4 [33].

Tabulka 4: Porovnání nákladů u GNSS simulátorů [38, 41, 42, 43]

Parametr	Safran Skydel GSG-7	bladeRF x40
Spotřeba energie (průměr)	400 W	3 W
Náklady na energii, 100 h chodu	240 Kč	1,8 Kč
Pořizovací náklady	cca 700 000 Kč	cca 12 000 Kč

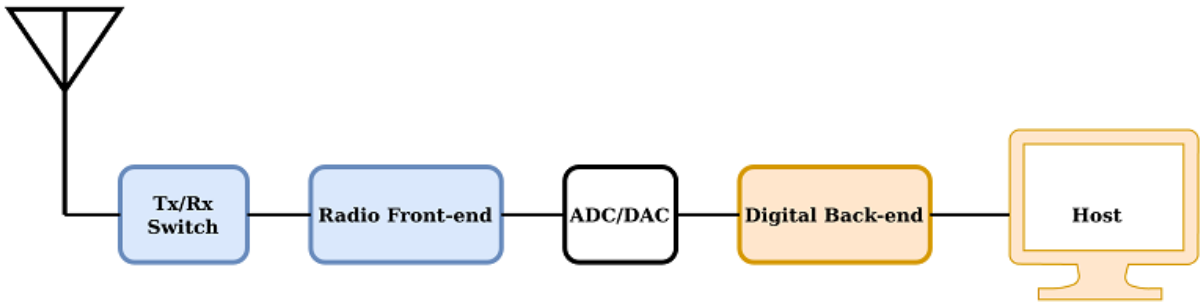
Na základě uvedených vlastností je možné považovat použití SDR pro GNSS simulaci jako alternativu k testování pomocí standardních simulátorů. Přesto je nutné vzít v úvahu, že tato metoda se začala aplikovat teprve v posledních letech a její vývoj stále probíhá. Tato kapitola popisuje princip fungování SDR a přináší přehled výrobců těchto zařízení a volně dostupných programů pro simulaci GNSS signálu. V závěru jsou uvedeny příklady provedených SDR simulací.

3.1 Softwarově definované rádio

Softwarově definované rádio je dle definice radiokomunikační zařízení, jehož základní systémy, sestávající se standardně z analogových komponentů, byly nahrazeny softwarovými prostředky na digitální bázi. Tento princip umožňuje uživateli regulovat parametry zařízení softwarově bez nutnosti fyzického zásahu, čímž výrazně narůstá flexibilita využití takového přístroje. Na rozdíl od klasických vysokofrekvenčních přijímačů či vysílačů zde tak často nenajdeme typické součástky jako směšovače, filtry, zesilovače, modulátory apod. [44].

Klasické rádio je tzv. hardware-based, to znamená, že jeho součástky byly sestrojeny pro provoz jedné funkce na dané frekvenci, kterou lze změnit pouze jejich výměnou. SDR naproti tomu umožňuje "přeprogramování" těchto součástek, jelikož jejich funkce je podmíněna softwarově. Díky tomu jsou SDR schopna pracovat na širokých škálách frekvencí, nejnovější modely až 0 – 16 GHz. SDR tak lze využít pro vysílání nebo příjem FM (zkr. frekvenční modulace) rozhlasových vln obvykle náležící rozsahu 87,5 MHz až 108 MHz, letadlových ADS-B zpráv (angl. zkr. Automatic Dependent Surveillance – Broadcast) na frekvenci 1090 MHz, GNSS signálu na rozsahu 1,1 GHz až 1,7 GHz i Wi-Fi signálu na hodnotách 2,4 GHz a 5 GHz [45, 46].

Zatímco elektromagnetický signál je zařízením přijímán nebo vysílán v analogové formě, uživatel s těmito daty pracuje ve formě digitální. Základní strukturu SDR lze tak rozdělit na dvě části, jak naznačuje Obrázek 11. Jedná se o analogový front-end (na Obrázku 11 modře) a digitální back-end (na Obrázku 11 oranžově). Přechod mezi těmito částmi zajišťuje příslušný převodník [46].

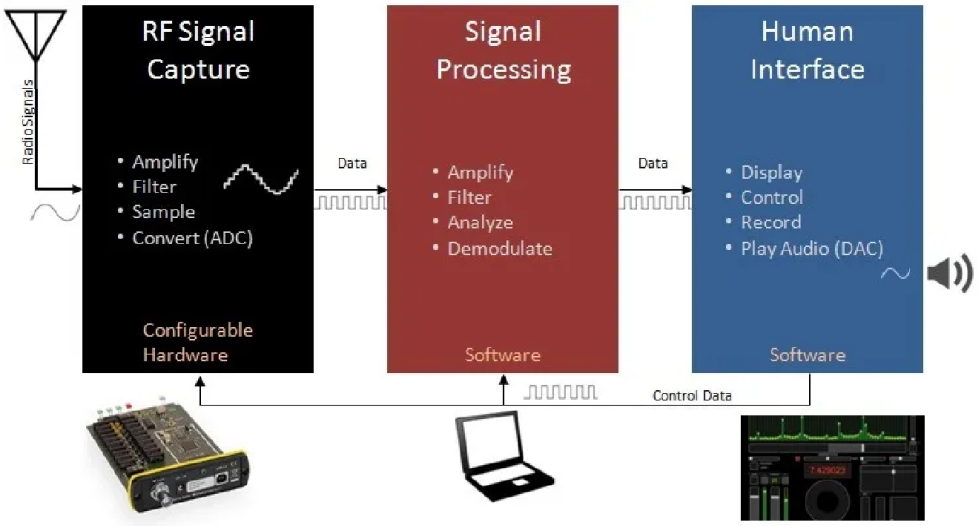


Obrázek 11: Schéma softwarově definovaného rádia [46]

Front-end je obecně část přístroje, která je viditelná pro uživatele. V případě SDR se jedná o celek, který se obvykle skládá z komponentů umožňující příjem (angl. zkr. Rx) či vysílání (angl. zkr. Tx) elektromagnetického signálu. Dále může obsahovat i klasické hardwarové prvky jako zesilovače či filtry za účelem dosažení lepších parametrů. K front-endu se také připojují různé externí prvky jako antény, atenuátory či redukce. Dle jednotlivých typů SDR lze rozlišit rádia v jeden čas pouze vysílající či přijímající (tzv. half-duplex) a ta, která umožňují vykonávat oba procesy zároveň (tzv. full-duplex) [46, 47].

Back-end je naopak část přístroje, jež je uživateli neviditelná. Základem tohoto segmentu SDR je tzv. programovatelné hradlové pole (angl. Field Programmable Gate Array, FPGA), které umožňuje konfiguraci tzv. programovatelných logických obvodů (angl. Programmable Logic Device, PLD). Díky tomu je možné libovolně nastavovat logiku celého systému a docílit tak požadované funkce. FPGA je opakem obvodů ASIC (tzv. zákaznický integrovaný obvod), jejichž funkce je pevně naprogramována již z výroby. Back-end může dále obsahovat programovatelné směšovače, vzorkovače, FIFO paměti (angl. first in, first out) a přenosové rámce, které zajišťují spojení s uživatelským rozhraním (např. PC) [46, 47, 48].

Obrázek 12 přináší jinou interpretaci fungování SDR, konkrétně při příjmu signálu. Černý blok znázorňuje front-endový HW, červený blok představuje back-end a modrý blok lze nazvat výstupem procesu pro uživatele.

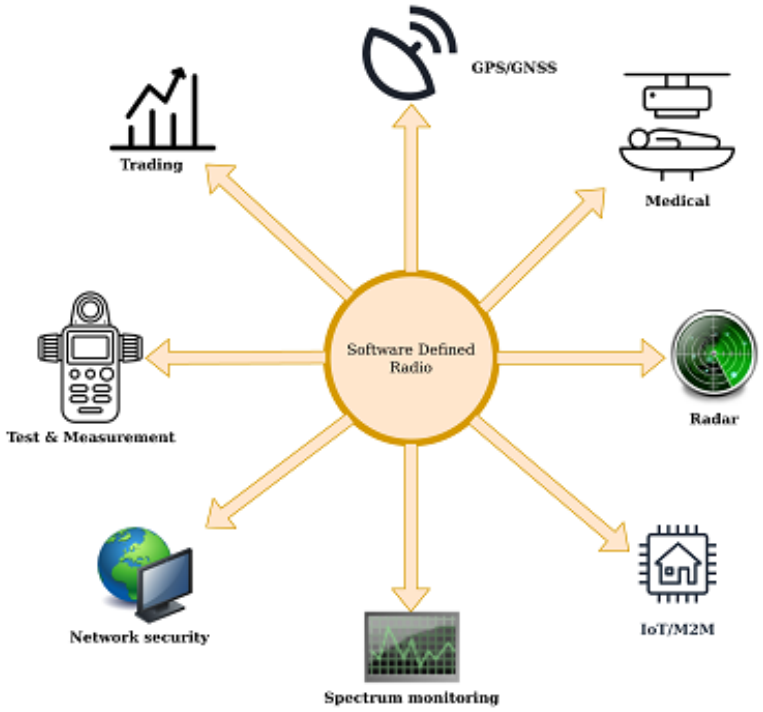


Obrázek 12: Schéma SDR při příjmu [49]

Jelikož front-end funguje na analogové bázi a back-end naopak na digitální, je třeba, aby obě části propojoval tzv. **převodník**. Při příjmu se jedná o převod spojitého signálu na diskrétní a je tudíž zapotřebí ADC převodník (angl. analog-to-digital converter). Pokud je přístroj v pozici vysílače, jde naopak o převod diskrétních dat na spojitá a je tak vyžadován DAC převodník (angl. digital-to-analog converter). SDR podporující funkce Rx i Tx musí disponovat oběma typy převodníků [46].

Výrobce rádia určuje typ ovládání, přes které uživatel interaguje se systémem. Většinu zkoumaných SDR v této práci je nutné připojit k počítači s instalovaným ovládacím softwarem (např. GNU Radio). Mezi takové přístroje lze zařadit např. LimeSDR, bladeRF, nebo ADALM-PLUTO. Existují ovšem i tzv. „standalone“ zařízení, která jsou obohacena o vlastní ovládací prvky a lze je tak používat samostatně (v tomto případě by na Obrázku 11 chyběl prvek „Host“). Příkladem je verze SDR HackRF s nástavbou Portapack [43, 50, 51, 52].

Softwarově definovaná rádia v současnosti zažívají rapidní rozvoj a spektrum jejich využití se stále rozšiřuje, jak je ilustrováno na Obrázku 13. Téměř každodenní využití nalezneme v odvětvích jako radarové technologie, spektrální analýza či GNSS. V nedávné době se SDR začala objevovat i v oblastech medicíny, kde jsou implementována do různých vysokofrekvenčních technologií jako je magnetická rezonance či pokročilé modely protéz a implantátů. Z netradičních využití lze zmínit např. vysokofrekvenční obchodování (angl. High-Frequency Trading, HFT) [46].



Obrázek 13: Souhrn možného využití SDR [46]

3.2 Srovnání použitelných SDR

Použití SDR v GNSS aplikacích není novinkou, ovšem často se omezuje na případy, kdy se rádio nachází ve funkci GNSS přijímače. Využití SDR jakožto GNSS vysílače je zmiňováno pouze v jednotkách odborných publikací (viz Kapitola 3.4) a tímto tématem se zabývají spíše amatérští nadšenci. Jelikož se tato práce zabývá mj. zhotovením GNSS SDR simulátoru, byla provedena podrobná rešerše trhu s SDR zařízeními, která by vyhovovala tomuto účelu. Zkoumané produkty včetně popisu jejich vlastností jsou řazeny abecedně a jejich cena odpovídá stavu z května 2023. Na konci výčtu se nachází souhrn těchto SDR v Tabulce 5.

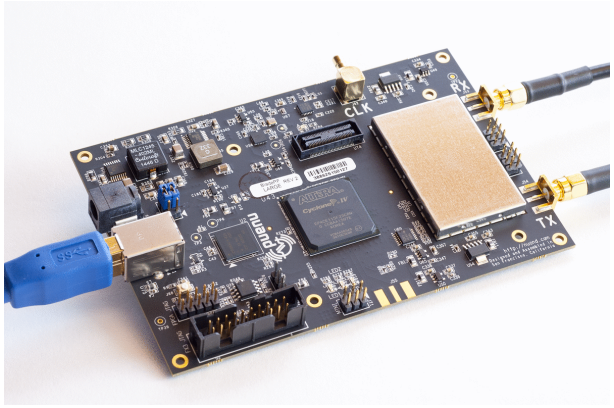
3.2.1 ADALM-PLUTO

Rádio od společnosti Analog Devices Inc., které je zmiňováno autory různých softwarů pro generování GNSS signálu. Typově se jedná o full-duplex zařízení, jež je primárně určeno jako learning module. Svým frekvenčním rozsahem pokrývá hodnoty 325 MHz až 3,8 GHz a poskytuje 12bitové vzorkování s rychlostí až 61 MSPS (odpovídá milionu vzorků za sekundu). Disponuje 2x SMA konektorem (pro Tx a Rx) a 2x microUSB konektorem (pro napájení a připojení k PC). Ovládání přístroje je možné přes aplikace GNU Radio, MATLAB, Simulink, či skrze jazyky C, C++, Python a další. Volně dostupnou dokumentaci nabízí výrobce na svých stránkách. Jedná se o zařízení dostupné za nízkou cenu u mnoha prodejců, které je dodáváno včetně dvou antén. Nejnižší cenová nabídka se pohybuje okolo **4 900,- Kč** přímo od výrobce. SDR je vyobrazeno na Obrázku 14 [50].

Obrázek 14: Zařízení ADALM-PLUTO [50]

3.2.2 bladeRF x40

Zařízení vyráběné firmou Nuand zmiňované v softwarech pro generování GNSS signálu a také v mnohých článcích o spoofingu. Jedná se full-duplex SDR, které využívá FPGA typu Altera Cyclone IV. Jeho frekvenční rozsah pokrývá 300 MHz až 3,8 GHz a disponuje převodníkem s 12bitovým vzorkováním o rychlosti 40 MSPS. Přístroj je vybaven 2x SMA konektorem (pro Tx a Rx), USB 3.0 vstupem pro připojení k PC a tzv. clock konektorem pro připojení hodin. Ovládání lze provádět například skrze volně dostupnou aplikaci GNU Radio. Dokumentace od výrobce je veřejně dostupná. Jde o SDR za středně vysokou cenu, které je nabízeno více prodejci. Nejnižší cenová nabídka je **11 000,- Kč** přímo od výrobce. Zařízení znázorňuje Obrázek 15 [43].



Obrázek 15: Zařízení bladeRF x40 [43]

3.2.3 HackRF One

Přístroj od výrobce Great Scott Gadgets, jež je opět zmiňován mnohými autory skriptů pro generování GNSS signálu. Zařízení je typu half-duplex. Jeho frekvenční rozsah je 1 MHz až 6 GHz a umožňuje 8bitové vzorkování rychlostí až 20 MSPS. Hardware disponuje 3x SMA konektorem (označené ClockIn, ClockOut a anténa) a 1x USB vstupem typu 2.0 pro připojení k PC. Uživatel může k ovládání používat volně dostupné aplikace jako např. GNU Radio či SDR#. K zařízení je bezplatně dostupná dokumentace přímo od výrobce. V závěru jde o SDR za nízkou cenu, jež je nabízeno více prodejci. Aktuálně nejnižší cena za kus je **6 200,- Kč**. Přístroj lze zhlédnout na Obrázku 16 [51, 53].

Obrázek 16: Zařízení HackRF One [51]

3.2.4 LimeSDR Mini

SDR od společnosti Lime Microsystems, jehož využití je zmiňováno ve více softwarech pro generování GNSS signálu a v rámci různých článků o spoofingu. Toto profesionální full-duplex zařízení disponuje FPGA typu Intel MAX 10 a transceiverem LMS7002M. Umožňuje vysílání a příjem na rozsahu 100 kHz až 3,8 GHz s 12bitovým vzorkováním rychlostí až 31 MSPS. Na přístroji malých rozměrů lze nalézt 2x SMA vstup (pro Tx a Rx) a 1x USB 3.0 konektor pro připojení k PC. Pro ovládání je třeba použít specifickou aplikaci LimeSuiteGUI či GNU Radio s pluginem gr-limesdr. K dispozici je volně dostupná dokumentace přímo od výrobce. LimeSDR Mini je zařízení za středně vysokou cenu nabízené menším počtem prodejců. Nejnižší cenová nabídka je současně **8 500,- Kč**. Fotografie zařízení se nachází na Obrázku 17 [52, 54].

Obrázek 17: Zařízení LimeSDR Mini [52]

3.2.5 RTL-SDR V3

Zařízení, které je zmiňováno v některých programech pro generování GNSS signálu a jehož výrobcem je stejnojmenná společnost RTL-SDR. Pokrývá frekvenční rozsah 500 kHz až 1,75

GHz a převodník umožňuje 8bitové vzorkování o rychlosti 3,2 MSPS. Přístroj velikostí podobný LimeSDR Mini disponuje 1x SMA konektorem a 1x USB konektorem pro připojení k PC. Ovládání SDR lze provádět přes aplikace GNU Radio, SDR# apod. Dokumentace je zdarma dostupná přímo na webu výrobce. Jde o zařízení za velmi nízkou cenu s více nabídkami prodejců. V tomto případě je nutné před implementací provést testování v roli GNSS vysílače, jelikož většina článků zmiňuje použití jen v pozici přijímače. Nejnižší cenová nabídka činí **700,- Kč** přímo od výrobce [55].

3.2.6 SiGe GN3S Sampler v3

Rádio vyvinuté společností SiGe ve spolupráci s Univeristy of Colorado speciálně pro GPS aplikace a zmiňované v SW pro generování GNSS signálu. Poskytuje 2bitové vzorkování, frekvenční rozsah není znám. Na přístroji se nachází 1x MCX konektor a 1x miniUSB port pro připojení k PC. SDR lze ovládat přes program MATLAB a je k dispozici volně dostupná dokumentace. Zařízení lze pořídit za nízkou cenu, ovšem pouze u jednoho prodejce. Je opět nutné testování, zdali je možné použití v roli GNSS vysílače. V současné době je jediná cenová nabídka **1 800,- Kč** [56, 57].

3.2.7 USRP N210

Profesionální SDR vyráběné společností Ettus, jehož použití lze nalézt v mnoha skriptech pro generování GNSS signálu i v různých článcích o spoofingu. USRP je typově full-duplex SDR s FPGA Xilinx Spartan 3A DSP. Umožňuje příjem a vysílání na širokém rozsahu 0 až 6 GHz se 14bitovým vzorkováním o vysoké rychlosti 100 MSPS. Zařízení disponuje různými RF a Ethernet konektory a také vstupem pro napájení. Ovládání umožňují aplikace jako např. GNU Radio, LabVIEW, Simulink atd. Výrobce poskytuje bezplatnou dokumentaci. Závěrem se jedná o přístroj za vysokou cenu, který lze pořídit od různých prodejců. Aktuální nejnižší cena čítá **61 600,- Kč**. Rádio lze zhlédnout na Obrázku 18 [58, 59].

Obrázek 18: Zařízení USRP N210 [58]

Tabulka 5: Souhrn dostupných SDR

Č.	Název	Rozsah frekvencí	Vzorkování	Duplex	Cena
1	ADALM-Pluto	325 MHz - 3,8 GHz	12 bit, 61 MSPS	Full	4 900 Kč
2	bladeRF x40	300 MHz - 3,8 GHz	12 bit, 40 MSPS	Full	11 000 Kč
3	HackRF One	1 MHz - 6 GHz	8 bit, 20 MSPS	Half	6 200 Kč
4	LimeSDR Mini	100 kHz - 3,8 GHz	12 bit, 31 MSPS	Full	8 500 Kč
5	RTL-SDR V3	500 kHz - 1,75 GHz	8 bit, 3,2 MSPS	*nezn.*	700 Kč
6	SiGe GN3S Sampler	*neznámý*	2 bit	*nezn.*	1 800 Kč
7	USRP N210	0 - 6 GHz	14 bit, 100 MSPS	Full	61 600 Kč

3.3 Dostupné open-access softwary

Po výběru SDR je nutné zvolit vhodný software, který je schopen generovat GNSS signál. Ten je sepsán v určitém programovacím jazyce, jako např. C, C++, Python, MATLAB atd. V základu lze tyto kódy rozdělit na volně dostupné (tzv. open-access) a placené. Mimo tyto dvě varianty je také možné si program vytvořit, jak například učinil Radek Šindelář z Fakulty elektrotechnické ČVUT v Praze v rámci své bakalářské práce [60].

Pro účely této práce byla s cílem udržení nízkých nákladů provedena podrobná rešerše open-access kódů, jejíž výsledky jsou uvedeny níže. Veškeré vyhledané skripty se nacházely na platformě *GitHub*. Celkem byly nalezeny tři projekty, které lze považovat za relevantní. Položky jsou řazeny dle počtu hvězdiček udělených projektům ostatními uživateli platformy GitHub. Z výčtu byly vyřazeny softwary s nedostatečným popisem či nízkým uživatelským hodnocením [61].

3.3.1 Skript „gps-sdr-sim“

První skript od autora *osqzss* (celým jménem Takuji Ebinuma) je s 2100 hvězdičkami nejlépe hodnoceným SW pro generování GNSS signálu. Program sepsaný z naprosté většiny v jazyce C umožňuje vytvoření aplikace, která je schopna generovat soubory obsahující GPS signál v binárním formátu (přípona .bin), textovém formátu (přípona .txt), formátu CSV (přípona .csv) a další. Proces obsahuje vytvoření navigační zprávy a PRN na frekvenci GPS L1 [62].

V manuálu (soubor README) je zmíněn postup, ve kterém je použit program Microsoft Visual Studio. V něm je nutné vytvořit nový projekt, do kterého uživatel nahraje dva soubory z GitHub adresáře. Následně je vytvořena aplikace pro generování samotných souborů. Její používání poté spočívá v zadávání příkazů do příkazového řádku, jejichž výčet je uveden na konci manuálu. Kromě funkce vytváření soborů statické polohy lze uvést i pokročilé možnosti generování dynamických trajektorií. Ke správnému fungování je nutné aplikaci dodat efemeridy konstelace GPS ve formátu BRDC (angl. Broadcast), které jsou volně dostupné na internetu. Postup práce s tímto projektem je podrobněji popsán v Kapitole 4 [62].

Pro správné fungování doporučuje autor použití následujících SDR: ADALM-PLUTO, bladeRF, HackRF a USRP. V jiném projektu na GitHub se nachází také implementace pro LimeSDR. Manuál je dále členěn na postupy týkající se jednotlivých zařízení. Z hlediska SW vyžaduje aplikace použití operačního systému Windows. Projekt má také rozsáhlou uživatelskou podporu [62].

3.3.2 Skript „gps-sdr-sim-realtime“

Skript od uživatele *gym487* se 120 hvězdičkami umožňuje real-time simulaci GPS signálu. Jedná se o techniku, při které ubíhá čas v systému stejně jako v reálném světě (podmnožinou je již zmíněná HIL simulace). Jelikož popis projektu z velké částí odpovídá popisu Skriptu 1 „gps-sdr-sim“, jde pravděpodobně o implementaci této techniky do již známého kódu, který ji sám o sobě neumožňuje. Oproti originálu byl program sepsán v jazycích C, CSS, Python a další. Požadavky na OS, doporučená SDR a postupy generování jsou v naprosté většině shodné se skriptem ”gps-sdr-sim“ [63, 64].

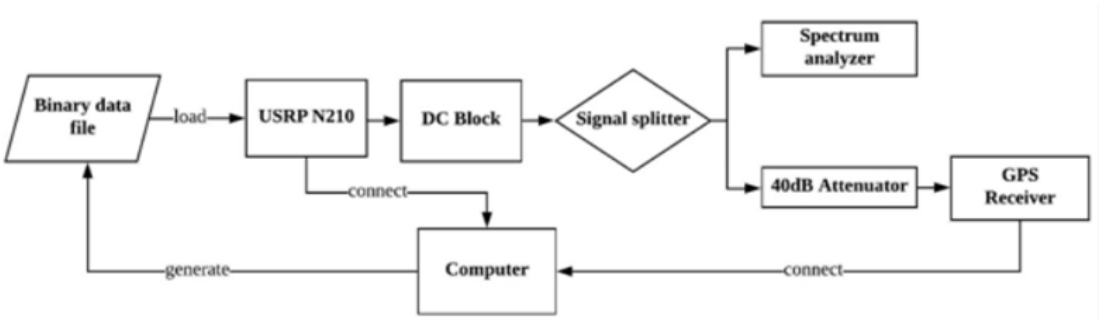
3.3.3 Skript „multi-sdr-gps-sim“

Posledním skriptem je program od uživatele *Mictronics* se 100 hvězdičkami, který je také založený na skriptu v Kapitole 3.3.1. Dle popisu lze pomocí softwaru sepsaném v jazyce C generovat signál GPS L1 pro SDR ADALM-PLUTO či HackRF. Správné fungování opět vyžaduje aktuální efemeridy systému GPS. Výčet funkcí je rozšířený o některé příkazy a provoz aplikace je kromě OS Windows možný i na Linuxu [65].

3.4 Příklady použití SDR ke generování GNSS signálu

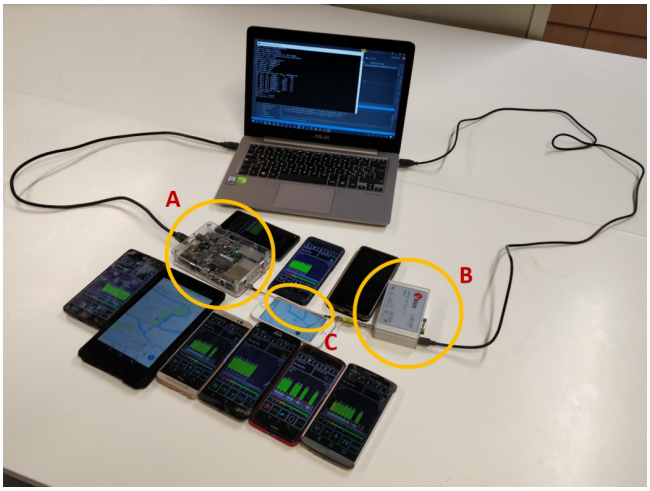
Generátory GNSS signálu založené na SDR jsou v současné době využívány spíše v rámci výzkumných prací různých univerzit a amatérských projektů. I přes obrovský potenciál – převážně z důvodu nízkých nákladů – tento typ simulátoru nenalézá uplatnění v profesionální podnikatelské sféře, jako například u velkých společností testující GNSS přijímače. Téma implementace GNSS SDR simulátoru lze nalézt v jednotkách až desítkách odborných publikací. Zde je uveden popis některých z nich.

Článek z pekingské univerzity publikovaný roku 2019 pojednává o generátoru vytvořeném na základě SDR USRP N210 s možností generovat GPS L1. Autor zde používá vlastní postup k vytvoření binárního navigačního souboru s využitím efemerid ve formátu RINEX. Tento soubor je vysílán zařízením USRP za účasti 40 dB zesilovače a následně zpracován samostatným GPS přijímačem. Schéma celé aparatury lze zhlédnout na Obrázku 19. Výsledkem měření, které zahrnovalo spoofing statické polohy a dynamické trajektorie, bylo úspěšné zaměnění autentických dat za falešná pocházející z generátoru [66].



Obrázek 19: Schéma experimentu s USRP [66]

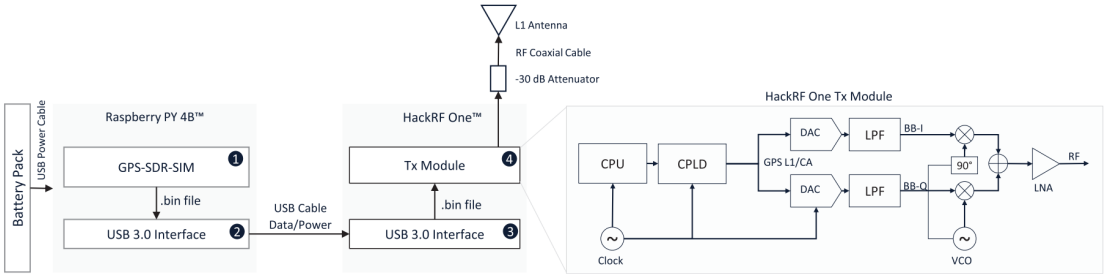
Vlastní SW využili také autoři článku z roku 2018 z padovské univerzity jejichž cílem byl výzkum bezpečnosti mobilních telefonů a jejich odolnosti vůči spoofingu. V rámci práce bylo podrobeno celkem 25 různých telefonů (značek Apple, Huawei, LG, Samsung, Xiaomi a další) vlivům soupravy bladeRF se softwarem sepsaným v jazyce C++, jak lze částečně vidět na Obrázku 20. Výsledkem byl úspěšný spoofing 23 zařízení s různými naměřenými časy od zahájení simulace po fixaci na falešnou polohu. Následně byly provedeny experimenty s vysíláním nepravé časové informace a spoofing dynamické trajektorie, kdy oba dopadly opět u většiny zařízení úspěšným ovlivněním těchto parametrů [67].



Obrázek 20: Testovací souprava bladeRF (A) a mobilní telefony [67]

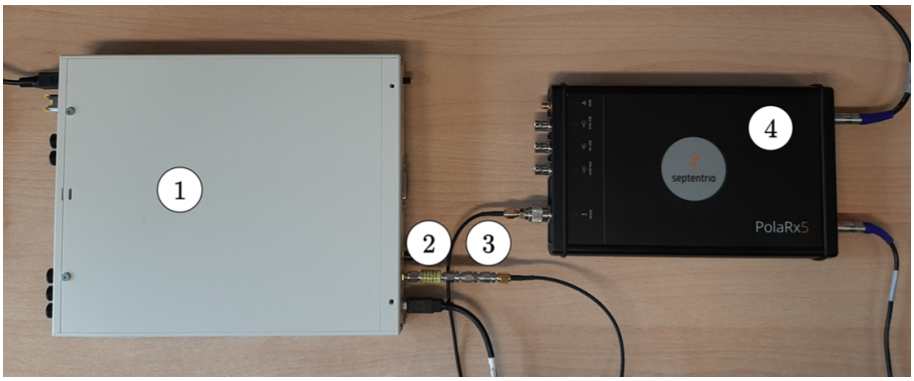
Na rozdíl od výše zmíněných článků byly provedeny také experimenty s použitím open-access programu jako například projekt od čínské obchodní společnosti Alibaba Group. V této studii byla použita zařízení HackRF a bladeRF s implementací nejpopulárnějšího volně dostupného kódu pro generování GPS signálu „gps-sdr-sim“. Po spuštění simulace došlo k úspěšnému spoofingu statické polohy mobilních telefonů Apple a Android a časové informace hodinek Apple Watch [68].

Aparaturu HackRF + SW „gps-sdr-sim“ využili také autoři italských článků z roku 2020 a 2023. V jejich experimentech byl program spuštěn na zařízení Raspberry PY 4B, jež vygeneroval binární soubor, který byl následně odeslán do SDR. Diagram této soustavy zařízení je znázorněn na Obrázku 21. V obou případech byla otestována různá mobilní zařízení. V prvním experimentu bylo u většiny zařízení dosaženo spíše efektu podobnému jammingu a nedošlo k fixu na neautentický signál. To mohlo být způsobeno dalšími funkcemi přijímačů, které umožňují určit polohu nezávisle na GNSS (např. Wi-Fi, mobilní data či Bluetooth). V druhém experimentu, s komplexnější analýzou výsledků, již došlo k úspěšnému spoofingu polohy [69, 70].



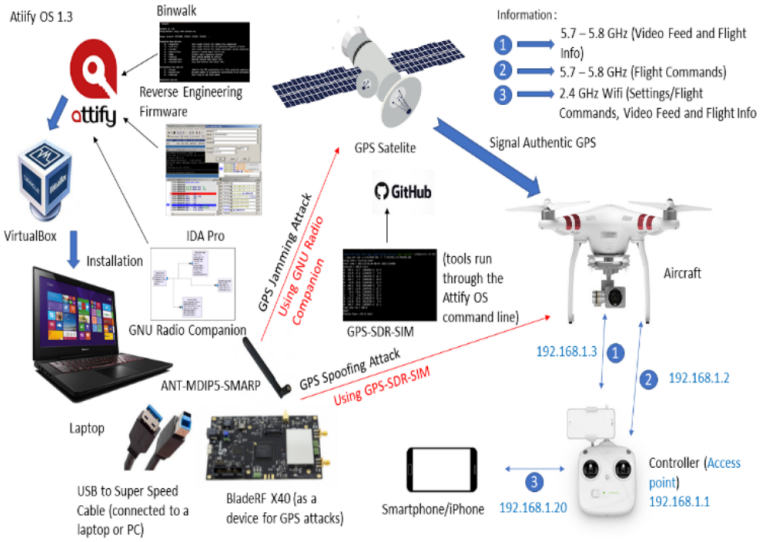
Obrázek 21: Schéma experimentu s HackRF [70]

Zajímavý přístup zvolila skupina vědců z Itálie a Nizozemska, která se ve svém článku z roku 2022 zabývá otázkou, zdali je možné rozlišit data, která bude přijímač zobrazovat při spoofingu a při příjmu autentického signálu. Výzkumný tým použil SDR USRP X300 a komerční SW QA707 pro generování signálu od firmy Qascom. Dle závěru práce byl experiment úspěšný a data z přijímače Septentrio PolaRx5 bylo možné odlišit. Použité přístroje jsou vyobrazeny na Obrázku 22 [71].



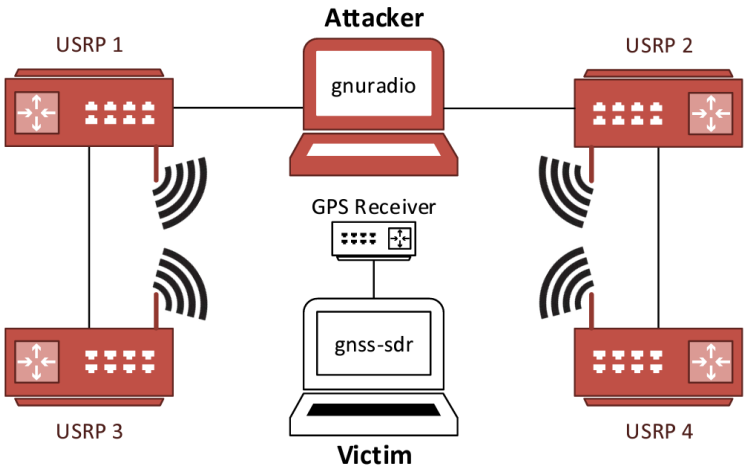
Obrázek 22: Testovací souprava SDR USRP (1) a přijímače Septentrio (4) [71]

Mimo testování GNSS SDR simulátorů na profesionálních přijímačích a mobilních telefonech lze zmínit i experimenty se spoofingem dronů. O takovém výzkumu pojednává například indonéský článek vydaný roku 2020, v němž došlo k úspěšnému spoofingu dronu DJI Phantom 3. Ke scénáři, který byl proveden uvnitř i venku, bylo použito SDR bladeRF a opětovně SW „gps-sdr-sim“. Komplexní schéma celého testu lze zhlédnout na Obrázku 23 [72].



Obrázek 23: Schéma experimentu s bladeRF a dronem DJI [72]

Se zajímavou hypotézou přichází článek z roku 2017 od autorů z univerzit v Bochumu a Abu Dhabi. Práce pojednává o tzv. multi-device útoku, při kterém je použito více SDR najednou. Každé zařízení poté vysílá signál jednoho satelitu. Konkrétně byl experiment proveden se čtyřmi kusy USRP N210 ovládanými skrze PC a softwarem „gps-sdr-sim“. Celá síť byla propojena skrze aplikaci GNU Radio a signál byl přijímán zařízením, které opět tvořilo USRP N210. Test se soupravou na Obrázku 24 proběhl s úspěšnými výsledky, které spočívaly v dosažení fixu na falešný signál již po 50 sekundách. V závěru práce autoři označují současné metody testování odolnosti zařízení vůči spoofingu jedním přístrojem (tzv. single-device) jako zastaralé a zdůrazňují nutnost jejich inovace [73].



Obrázek 24: Schéma multi-device spoofingu s využitím čtyř SDR [73]

4 Sestrojení GNSS simulátoru pomocí SDR

Podstatou praktické části této bakalářské práce je sestrojení GNSS simulátoru s pomocí softwarově definovaného rádia a open-source kódů. V GNSS aplikacích lze v současnosti nalézt použití SDR převážně v pozici přijímače, zatímco jeho využití ke generování GNSS signálu se setkává pouze s malým zájmem, a to i přes mnohé benefity, které tato možnost přináší. Motivací k sestavení takového přístroje je využití širokého potenciálu tohoto druhu simulace, jež přináší obsáhlé možnosti využití nejen na Fakultě dopravní (zkr. FD), ale také v rámci dalších institucí zabývající se problematikou testování GNSS signálu.

Na základě Kapitoly 2.2 byla vyloučena možnost pořízení profesionálního simulátoru z důvodu vysokých nákladů. Provedením rešerše dostupného technického a programového vybavení v Kapitole 3 byly poskytnuty podklady pro realizaci sestavení vlastního GNSS generátoru. Tato kapitola popisuje celý proces od výběru vhodného skriptu a zvolení SDR, přes podrobný popis sestrojení a ovládání zařízení, až po příklady simulačních příkazů.

4.1 Výběr vhodného kódu

Vzhledem k rozsáhlému množství dostupných typů SDR a jejich podobným charakteristikám, které implikují obtížný výběr ideálního modelu, bylo při tvorbě simulátoru v prvním kroku přistoupeno k volbě vhodného softwaru, který výběr vhodných SDR pravděpodobně zúží. Požadavkem byl bezplatně dostupný skript pro generování GNSS signálu, tj. open-access skript. Jak naznačuje Kapitola 3.3, takových kódů neexistuje mnoho, konkrétně tři. V rámci rešerše byly nalezeny projekty, jež umožňují rozlišné funkce simulace, jsou podporovány různými SDR a které se odlišují hodnocením uživatelů platformy GitHub. Veškeré nalezené skripty jsou omezeny na generování signálu GPS L1.

Na základě průzkumu byl výběr primárně zacílen na nejlépe hodnocený kód “gps-sdr-sim”. Bylo odstoupeno od kódů s nízkým hodnocením, a to převážně z důvodu nedostatečné zpětné vazby uživatelů o funkčnosti a malé odezvy autora a komunity na řešené problémy (tj. skripty „gps-sdr-sim-realtime“ a „multi-sdr-gps-sim“). Mimo provedenou rešerši bylo uvažováno o použití dalších populárních kódů „GNSS-SDRLIB“ a „GNSS-matlab“, u kterých bylo ovšem zjištěno, že generují pouze PRN sekvenci, a nikoliv též navigační zprávu. Tento nedostatek by znemožnil plnohodnotnou simulaci a bylo tak od jejich použití upuštěno [74, 75, 63, 65].

Z uvedených důvodů byl pro realizaci GNSS simulátoru zvolen již zmíněný kód “gps-sdr-sim” od autora Takuji Ebinuma. Oproti již zmíněným skriptům disponuje aktivní podporou jak od dalších uživatelů, tak od samotného autora. Kladně lze také hodnotit seznam kompatibilních SDR, která jsou snadno dostupná a jejichž funkčnost v roli vysílače byla úspěšně demonstrována, jak uvádí Kapitola 3.4. Omezujícím kritériem je u tohoto projektu pouze možnost vysílání jediného typu signálu, a to GPS na frekvenci L1 [62].

4.2 Výběr vhodného SDR

Na základě předešlého výběru skriptu pro generování GNSS signálu byla volba vhodného SDR limitována následujícím seznamem doporučených zařízení od autora projektu „gps-sdr-sim“ [62]:

- ADALM-PLUTO
- bladeRF
- HackRF
- USRP

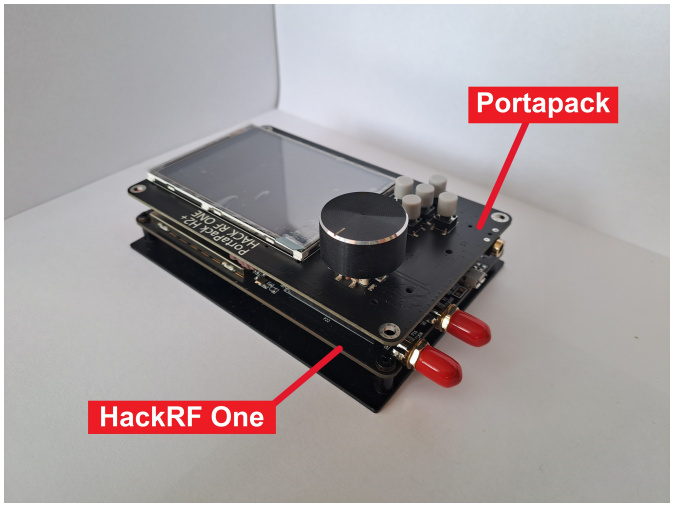
Po přihlédnutí k rešerši provedené v Kapitole 3.2 bylo vyloučeno zařízení USRP, jelikož jeho pořizovací náklady výrazně převyšovaly ceny alternativ. Ze zbývajících tří typů SDR by bylo pravděpodobně zvoleno bladeRF z důvodu přípustné ceny a vynikajících parametrů, kterými jsou rozsah frekvencí a hodnoty vzorkování, jak uvádí Tabulka 5. Vzhledem k dostupnosti jiného HW a časovému omezení byla ovšem provedena realizace GNSS simulátoru na SDR HackRF, které pro účely této práce zapůjčil bývalý student Fakulty dopravní.

Ke zvolení HackRF také přispěl fakt, že zařízení bylo k dispozici v konfiguraci HackRF One + Portapack, což je standalone varianta standardního řešení. Díky tomuto rozšíření je možné SDR ovládat přes ovládací prvky přímo na zařízení prostřednictvím SW Mayhem, bez nutnosti jej připojovat k PC [76].

Varianta HackRF One + Portapack byla dodána i s dalším příslušenstvím, jako například napájecí kabel, SMA koaxiální kabel, 20 dB zesilovač či množství různých antén. Kompletní zapůjčenou soupravu včetně popisků lze zhlédnout na Obrázku 25. Pro pochopení ovládání tohoto produktu bylo využito GitHub adresáře „portapack-mayhem“ [76, 77].

Obrázek 25: Balíček HackRF One + Portapack s příslušenstvím [76]

Konkrétní zapůjčená souprava se skládá ze zařízení HackRF One, které je typu half-duplex s frekvenčním rozsahem 1 MHz až 6 GHz a 8bitovým vzorkováním s rychlostí až 20 MSPS. To je spojeno s nástavbovou deskou Portapack, jež disponuje softwarem Mayhem. Celé zařízení je vyobrazeno na Obrázku 26. SDR disponuje vstupy pro napájecí microUSB kabel, microSD kartu a třemi SMA-female konektory (dva pro externí hodiny, jeden pro anténu). Ovládání probíhá přes dotykovou obrazovku či pomocí ovládacích prvků níže. Podrobný postup ovládání rádia je uveden v Kapitole 4.3.3 [51, 76].



Obrázek 26: Souprava HackRF One + Portapack bez pouzdra

4.3 Postup sestrojení simulátoru a ovládání

Tato kapitola obsahuje podrobný návod ke spuštění simulace od vytvoření aplikace pro generování potřebných souborů, přes jejich vložení do SDR, až po ovládání samotného přístroje. Postup je aplikován na OS Windows, ovšem existuje také rozšířený GitHub projekt pro prostředí Linux [65]. V následujících krocích bylo postupováno v souladu s návody k softwaru „gps-sdr-sim“ a k zařízení HackRF + Portapack na stránkách GitHub [62, 77].

4.3.1 Kompilace „gps-sdr-sim“ aplikace

Prvním krokem nezbytným pro úspěšné spuštění simulace je kompilace samotné aplikace, která umožňuje generování souborů s GNSS signálem. Pro tyto účely slouží vybraný software z GitHubu „gps-sdr-sim“ [62].

Krok 1

V prvním kroku je nutné do počítače stáhnout adresář souborů z GitHub projektu a bezplatnou aplikaci Visual Studio od společnosti Microsoft. Po instalaci a spuštění Visual Studia je postup následující:

1) V pravé části okna Visual Studio zvolit *Create New Project*
2) Vpravo nahoře místo *All languages* vybrat *C++*
3) Ze seznamu zvolit *Console App* $\rightarrow$ *Next*

Při výběru typu projektu je důležité zkontrolovat zvolený programovací jazyk, jelikož typ *Console App* se zde nachází vícekrát. Následně je nutné aplikaci pojmenovat a vybrat její umístění. Poté se kliknutím na tlačítko *Create* soubor vytvoří a spustí se editační okno.

Krok 2

V dalším kroku je zapotřebí nalézt v pravém okně s názvem *Solution Explorer* složku *Source Files* (standardně poslední položka) a přesunout sem soubory s názvy ***getopt.c*** a ***gpssim.c*** ze staženého GitHub adresáře. To je možné provést přímým přetažením myší, či pravým kliknutím na složku *Source Files* $\rightarrow$ *Add* $\rightarrow$ *Existing Item*.

Z umístění *Source Files* je také nutné smazat položku s koncovkou *.cpp*, která má název totožný s pojmenováním celého projektu. Pro úplnost kódu je možné do adresáře *Header Files*

(standardně nad *Source Files*) vložit soubory *getopt.h* a *gpssim.h*. Tento krok je volitelný a neovlivňuje funkčnost výsledné aplikace.

Krok 3

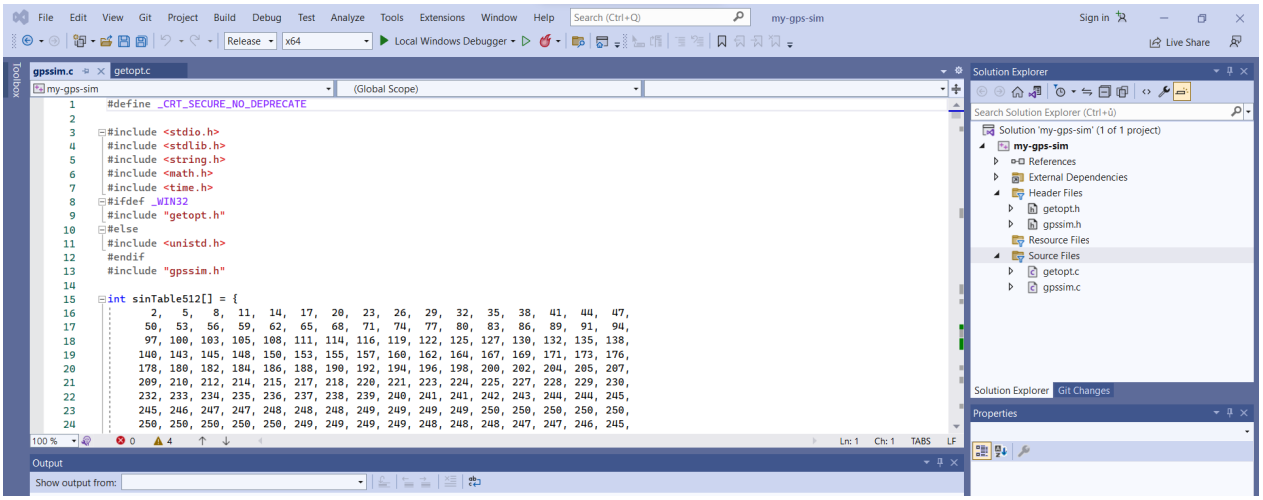
V tuto chvíli je již možné provést kompilaci aplikace pomocí tlačítka v horní liště *Build* → *Build Solution*. Následně je nutné provést debug programu:

1) Pod tlačítkem *Build* vybrat ze seznamu místo *Debug* možnost *Release*

2) Ve vedlejším seznamu vybrat možnost *x64*

3) Spustit debug pomocí tlačítka *Local Windows Debugger*

Finální náhled ve Visual Studiu by měl vypadat tak, jak naznačuje Obrázek 27. Úspěšným debugem je proces kompilace aplikace ukončen, projekt lze uložit a Visual Studio zavřít. Soubor je nyní umístěn na námi zvoleném úložišti. Ve složce se nachází samotné řešení projektu s příponou *.sln*, po jehož otevření se lze navrátit k editaci skriptu. Samotná aplikace (*název.exe*) se zde nachází v adresáři *x64* → *Release*.



Obrázek 27: Náhled finálního skriptu ve Visual Studiu

4.3.2 Generování simulačního souboru

Před použitím vytvořeného programu je ke spuštění simulace zapotřebí stažení aktuálních efemerid, které je zapotřebí dodat do simulátoru externě. Efemeridy všech světových konstelací jsou volně dostupnými soubory, které lze stáhnout například z webové databáze CDDIS od

americké společnosti NASA. Po bezplatné registraci je v archivu databáze vybráno umístění *gnss* → *data* → *daily*. Zde je vybrán aktuální rok a den (dny jsou číslovány postupně od začátku roku). V tomto adresáři se nachází složky pro jednotlivé konstelace. Jelikož v tomto případě se jedná o simulaci GPS signálu, odpovídající složka má název **YYn** (kde YY odpovídá posledním dvou číslicím zvoleného roku). Lze zde nalézt i data pro ostatní konstelace dle klíče: YYf pro BeiDou, YYl pro Galileo a YYg pro GLONASS. Z této složky je poté nutné stáhnout tzv. broadcast soubor s názvem **brdcDDD0.YYn.gz** (kde DDD odpovídá číslu vybraného dne). Po stažení je z archivu vybrán soubor s příponou *.YYn* a vložen do úložiště, kde se nachází aplikace kompilovaná v Kapitole 4.3.1 (přípona *.exe*) [78].

Ovládání samotné simulační aplikace probíhá skrze příkazový řádek. Nejprve je nezbytné nasměrovat konzoli do umístění aplikace pomocí příkazu *cd*. Například *cd Documents\...\Simulator\...\my-gps-sim\x64\Release*.

Příkaz pro zahájení generování souboru se vždy skládá z názvu aplikace a atributů simulace. Typ atributu je označený pomlčkou a písmenem, za kterým následuje mezera a požadovaná hodnota. Celkem je nutné zadat alespoň tři atributy. Pro HackRF One je základní syntaxe příkazu:

```
*NÁZEV_APLIKACE* -e *NÁZEV_SOUBORU_EFEMERID* *DALŠÍ_ATRIBUTY*
-b 8 -o *NÁZEV_VÝSLEDNÉHO_SOUBORU*.c8
```

Názorný příkaz pro název aplikace „my-gps-sim“ by vypadal následovně:

```
my-gps-sim -e brdcDDD0.YYn *DALŠÍ_ATRIBUTY* -b 8 -o simulace01.c8
```

V případě vepsání pouze názvu aplikace se zobrazí nápověda pro všechny dostupné atributy, jak zobrazuje Obrázek 28. Základním atributem je **-e**, jehož hodnota odkazuje na název broadcast souboru efemerid, který slouží přístroji jako vstup pro tvorbu navigační zprávy. Další nezbytný atribut je **-b**, který určuje formát I/Q dat v bitech a **-o**, za nímž je vložen požadovaný název výsledného souboru a jeho přípona. Atribut -b musí být pro HackRF nastaven na hodnotu 8 bitů. Dle oficiálního návodu je také nutné využít specifickou příponu výsledného souboru *.c8*. Pro jiné typy SDR se mohou tyto dva parametry lišit.

Pro simulaci statické polohy je zapotřebí použít atribut **-l**, za kterým jsou vloženy souřadnice polohy v pořadí zeměpisná šířka, zeměpisná délka a výška (LLH). Druhou možností je použití atributu **-c** a zadání polohy ve formátu ECEF x, y, z v metrech. Jednotlivé údaje jsou odděleny čárkou bez mezery a jako desetinný oddělovač je použita tečka.

V případě simulace dynamické trajektorie lze využít celkem 3 možnosti. Atribut **-x** požaduje data o trajektorii s použitím LLH, zatímco atribut **-u** zpracovává trasu ve formátu ECEF. Oba pracují se soubory formátu CSV. Třetí variantou je atribut **-g**, k němuž jsou připojena data o trajektorii ve formátu NMEA s příponou *.txt*.

Software dále umožňuje měnit čas začátku scénáře (atributy **-t** a **-T**) či délku jeho trvání (atribut **-d**). Je-li požadován čas začátku simulace nacházející se v druhé polovině dne (tj. 12:01 až 23:59), je nutné využít argument -T. Vzorkovací frekvence simulace je defaultně nastavena na 2,6 MHz, ovšem lze ji upravit za pomoci atributu **-s**. Konfiguraci simulace umožňují také atributy **-i**, pro eliminaci zpoždění signálu v ionosféře, a **-v** pro zobrazení více detailů o simulovaných kanálech.

Po spuštění simulace dojde ke generování fiktivního signálu, jehož trvání je ve výchozím nastavení 300 sekund. Poté je v adresáři aplikace vytvořen soubor se zadanou koncovkou, v případě HackRF *.c8*.

```
Usage: gps-sdr-sim [options]
Options:
  -e <gps_nav>     RINEX navigation file for GPS ephemerides (required)
  -u <user_motion> User motion file in ECEF x, y, z format (dynamic mode)
  -x <user_motion> User motion file in lat, lon, height format (dynamic mode)
  -g <nmea_gga>    NMEA GGA stream (dynamic mode)
  -c <location>    ECEF X,Y,Z in meters (static mode) e.g. 3967283.15,1022538.18,4872414.48
  -l <location>    Lat,Lon,Hgt (static mode) e.g. 30.286502,120.032669,100
  -t <date,time>   Scenario start time YYYY/MM/DD,hh:mm:ss
  -T <date,time>   Overwrite TOC and TOE to scenario start time
  -d <duration>    Duration [sec] (dynamic mode max: 300 static mode max: 86400)
  -o <output>      I/Q sampling data file (default: gpssim.bin ; use - for stdout)
  -s <frequency>   Sampling frequency [Hz] (default: 2600000)
  -b <iq_bits>     I/Q data format [1/8/16] (default: 16)
  -i               Disable ionospheric delay for spacecraft scenario
  -v               Show details about simulated channels
```

Obrázek 28: Seznam dostupných atributů aplikace [62]

4.3.3 Transfer souboru do SDR a ovládání simulace

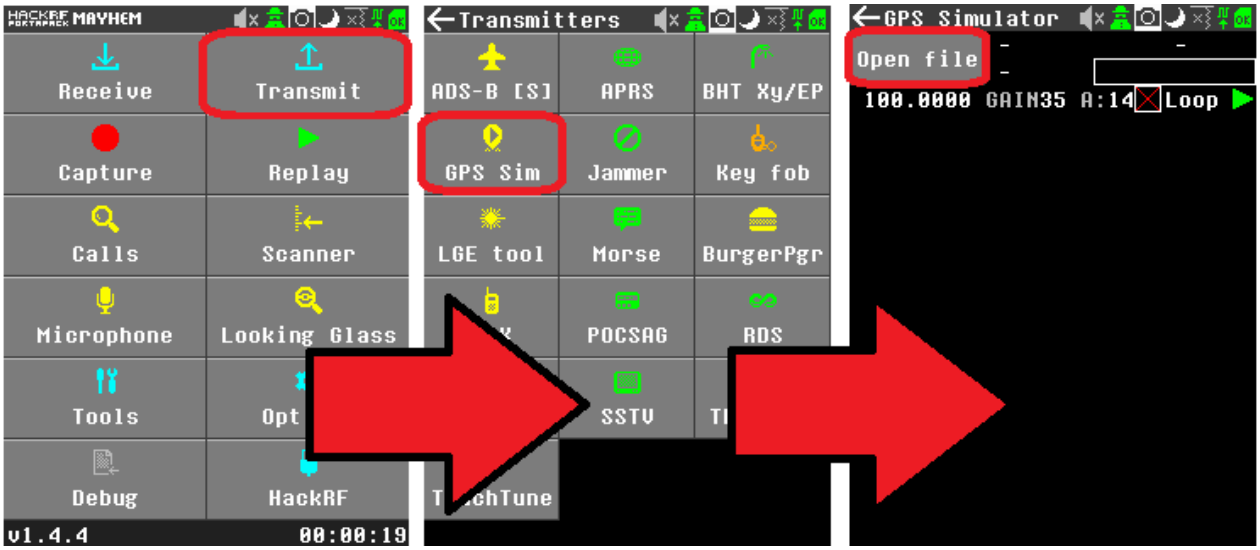
Pro spuštění simulace na zařízení HackRF je dále nezbytné vytvořit textový soubor s názvem totožným jako je pojmenování souboru C8. Zde je nutné vypsat dva parametry simulace - středovou frekvenci a vzorkovací frekvenci v jednotkách Hz. Středová frekvence musí být 1575,42 MHz (tj. GPS L1). Vzorkování je dle návodu možné nastavit na 2,6 MHz, 2,5 MHz či 1,25 MHz. Z výsledků testování zařízení lze nejlepších výsledků dosáhnout při hodnotě 2,6 MHz, což je pravděpodobně zapříčiněno shodou s defaultní hodnotou vzorkovací frekvence softwaru „gps-sdr-sim“. Textový soubor tedy musí obsahovat tyto dva řádky:

sample_rate=2600000
center_frequency=1575420000

Jelikož HackRF + Portapack funguje jako standalone zařízení, je transfer souborů prováděn pomocí microSD karty. Na kartu se nahraje simulační soubor C8 a příslušný textový soubor. Po vložení karty do SDR je zařízení připraveno k simulaci.

Zapnutí SDR probíhá stisknutím levého otočného kolečka, vypnutí jeho dvojitým stisknutím. Pohyby v nabídce lze vykonávat otáčením levého kolečka či prostřednictvím čtyř tlačítek napravo. Potvrzení probíhá stisknutím kolečka nebo středového tlačítka v pravé části přístroje. Po spuštění SDR je vhodné vypnout funkci automatického vypnutí displeje po 5 sekundách. To je provedeno v hlavním menu *Options* → *Interface* → *Backlight off after: 5 seconds.*

Po návratu do menu je zvolena položka *Transmit* → *GPS Sim*. V tuto chvíli přístroj zobrazuje hlavní obrazovku GPS simulátoru. Postup jednotlivými nabídkami v SW Mayhem je vyznačen na Obrázku 29. Vlevo nahoře je pomocí tlačítka *Open file* nutné nahrát připravený C8 soubor. Po jeho načtení lze upřesnit parametry simulace, jako například vysílací výkon v položce *GAIN* (hodnota 1 až 47, bezrozměrná jednotka). Dále je možné přepínat mezi jednorázovým a opakovaným vysíláním v sekci označené *LOOP*. Simulace je spuštěna zeleným tlačítkem napravo se symbolem ▶.



Obrázek 29: Jednotlivé obrazovky při spouštění simulace

Vysílání simulovaného GPS signálu lze realizovat přímým spojením s přijímačem přes koaxiální kabel skrze SMA konektor. Druhou variantou je bezdrátové vysílání prostřednictvím antény. Je možné použít některou z dodaných v balíčku Portapack, pokud její rozsah pokrývá i frekvenci GPS L1. Úspěšné simulace lze na základě testování lépe dosáhnout při použití antén určených pro GPS vysílání, které jsou vyráběny přímo pro frekvenci 1575,42 MHz.

4.4 Příklady simulace

Pro účely této práce byla aplikace vytvořená podle Kapitoly 4.3.1 pojmenována „my-gps-sim“ a umístěná na úložiště *D:\Dokumenty\FD ČVUT\BP\VisualStudio-c8_gen\my-gps-sim\x64\Release*. Nejprve tedy bylo nutné přesměrovat konzoli následujícími příkazy:

D: → *Enter*
cd Dokumenty\FD ČVUT\BP\VisualStudio-c8_gen\my-gps-sim\x64\Release → *Enter*

Pro příkladovou simulaci uvažujeme datum 1. 5. 2023. Z toho důvodu byly do složky s aplikací staženy efemeridy s názvem *brdc1210.23n* (121. den v roce). Za těchto vstupních podmínek by byl syntax příkazů pro různé typy simulace následovný:

Generování statické polohy

1) Simulace statické polohy, Barcelona, LLH souřadnice

```
my-gps-sim -e brdc1210.23n -l 41.390205,2.154007,100 -b 8 -o barcelona.C8
```

2) Simulace statické polohy po dobu 10 min., New York, LLH souřadnice

```
my-gps-sim -e brdc1210.23n -l 40.730610,-73.935242,100 -d 600 -b 8 -o ny.C8
```

3) Simulace statické polohy, New York, ECEF souřadnice, vzorkování 1,25 MHz

```
my-gps-sim -e brdc1210.23n -c 1339408,-4651226,4139864 -s 1250000 -b 8 -o ny.C8
```

Generování dynamické trajektorie

Pro provedení dynamické simulace je zapotřebí vytvořit soubor s daty trajektorie v úložišti aplikace. To lze provést pomocí různých online nástrojů, jak zmiňuje GitHub návod od uživatele *emlyons2014*. Jednoduché řešení nabízí např. Google Mapy, které umí definovanou trasu exportovat ve formátu KML. Tento soubor lze pak snadno transformovat do NMEA formátu v podobě textového souboru např. prostřednictvím aplikace SatGen. Dále je možná konverze KML souboru do formátu CSV. Pro další příklady simulace jsou uvažovány soubory s fiktivní trajektorií nazvané *trasa.csv* a *trasa.txt* [79, 80].

4) Simulace dynamické trajektorie, formát NMEA

```
my-gps-sim -e brdc1210.23n -g trasa.txt -b 8 -o dynsim.C8
```

5) Simulace dynamické trajektorie, formát CSV, LLH souřadnice, začátek 1. 2. 2023 10:00

```
my-gps-sim -e brdc1210.23n -x trasa.csv -t 2023/02/01,10:00:00 -b 8 -o dynsim.C8
```

6) Simulace dynamické trajektorie, formát CSV, ECEF souřadnice, vypnutí ionosférického zpoždění

```
my-gps-sim -e brdc1210.23n -u trasa.csv -i -b 8 -o dynsim.C8
```

5 Testování sestaveného zařízení

Dle kroků uvedených v Kapitole 4 byl simulátor úspěšně sestaven. Pro ověření funkčnosti sestrojeného zařízení byly uskutečněny tři různé testy. V této kapitole je u každého z nich zmíněna jeho metodika a popsány naměřené výsledky. Ve většině případů se jednalo o experimenty spočívající v generování statické polohy a sledování reakcí různých přijímačů. Ve všech případech byl použit simulátor v konfiguraci HackRF One + Portapack se softwarem „gps-sdr-sim“. Sestava zahrnující tento přístroj, napájecí kabel, powerbanku a microSD kartu je dále označována souhrnným pojmem „simulátor“. Kapitolu uzavírá diskuze dosažených výsledků.

5.1 Test 1 – mobilní telefony

5.1.1 Metodika měření

Datum a místo provedení: prosinec 2022 – červen 2023, Říčany, ČR

Vybavení:

- Simulátor
- Aktivní anténa GPS L1 2J7C01MC3F plochá, 1575,42 MHz (dále jen anténa 01)
- Aktivní anténa GPS L1 2J0801b tyčová, 1575,42 MHz (dále jen anténa 02)
- Univerzální anténa tyčová stříbrná, rozsah 40-6000 MHz (dále jen anténa 04)
- Testované mobilní telefony (viz Tabulka 6)
- Stopky

První testy byly provedené na snadno dostupných zařízeních, kterými jsou mobilní telefony. Ty jsou v současné době téměř vždy vybaveny GNSS přijímačem, který často využívá více než jeden typ konstelace. Před jednotlivými experimenty byly staženy GPS efemeridy ze dne měření a byla vybrána lokace pro generování statické polohy (typicky velké město). Po vytvoření potřebných souborů a jejich přesunu do simulátoru bylo realizováno samotné měření.

V **první fázi** (prosinec 2022 až březen 2023) byla k testům použita teleskopická anténa 04, která byla dodána jako součást balíčku HackRF + Portapack. Důvodem byl odpovídající frekvenční rozsah i předchozí úspěšné výsledky jiných uživatelů [77]. S touto anténou byl testován mobilní telefon Samsung Galaxy A33 (v Tabulce 6 ID 1) s nainstalovanými aplikacemi *GPSTest* [24] a *Google Mapy*. První zmíněná aplikace byla využita k přehlednému zobrazení všech GNSS satelitů,

jejichž signál je aktuálně přijímán a zároveň k ověření, zda byla vypočítána poloha zařízení. Druhá aplikace zobrazovala polohu na mapovém podkladu. Simulována byla nejčastěji lokace města Londýn, zatímco mobil se nacházel ve městě Říčany. Testování proběhlo mimo budovu i uvnitř.

Moderní mobilní telefony využívají k určení polohy i různé sekundární služby jako například připojení k internetu (Wi-Fi či mobilní data) či funkci Bluetooth. Na základě doporučení z návodů byly tyto služby před vykonáním testů vypnuty, a to spuštěním *Režimu letadlo*. Tím bylo zajištěno určování polohy pouze na základě příjmu signálu z GNSS. Po tomto procesu byl mobil umístěn do těsné blízkosti antény (0 – 2 cm) a vysílání bylo spuštěno.

V pozdějších etapách bylo zjištěno, že lepších výsledků lze dosáhnout restartováním telefonu po spuštění generování signálu (spoofingu). Příčinou je pravděpodobně proces, při kterém si některé modely ukládají dříve přijaté navigační zprávy do mezipaměti (angl. cache) a tím mohou negativně ovlivnit průběh výpočtu polohy. Obsah této paměti je restartem vymazán. V této fázi testování bylo sledovaným parametrem pouze nabytí generované polohy. Měření bylo prováděno pro jednotlivé tři vzorkovací frekvence, které byly doporučeny návodem (viz Kapitola 4.3.3).

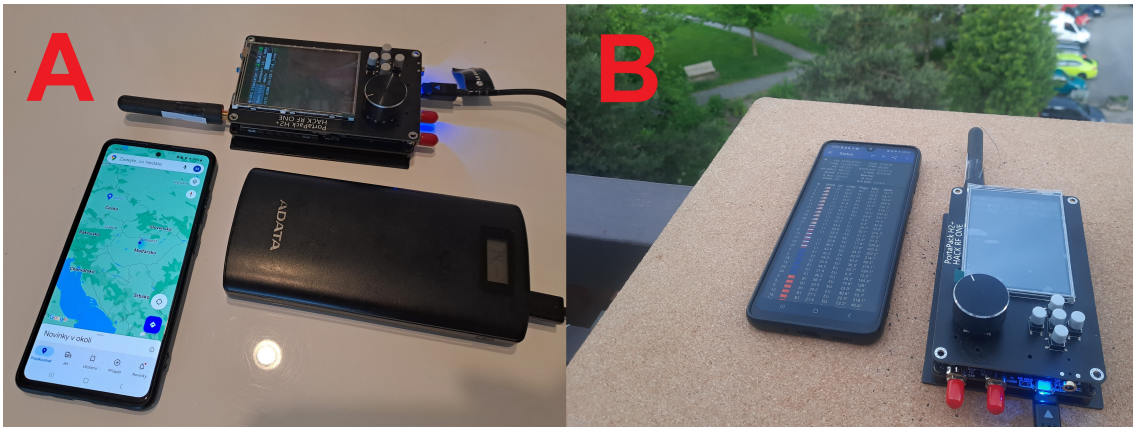
Ve **druhé fázi** (duben až červen 2023) byly Ústavem letecké dopravy zakoupeny profesionální GPS antény 01 a 02, jež jsou určeny pro příjem či vysílání na frekvenci GPS L1, tj. 1575,42 MHz. Současně došlo také ke změně vzorkovací frekvence na hodnotu 2,6 MHz, za účelem sladění s výchozím nastavením vzorkování softwaru. Při této konfiguraci došlo k otestování celkem pěti různých mobilních zařízení. Byly jimi čtyři mobilní přístroje Samsung Galaxy a jeden telefon značky Apple iPhone. Seznam zařízení včetně roku jejich výroby a podporovaných konstelací zobrazuje Tabulka 6 (poslední sloupec obsahuje využívané regionální konstelace).

Tabulka 6: Seznam testovaných zařízení v testu 1

ID	Výrobce	Typ	Rok	Podporované konstelace				
				GPS	GLONASS	Galileo	BeiDou	Reg.
1	Samsung	Galaxy A33	2022	**ANO**	**ANO**	**ANO**	**ANO**	NE
2	Samsung	Galaxy A51	2019	**ANO**	**ANO**	**ANO**	**ANO**	NE
3	Samsung	Galaxy A8	2018	**ANO**	**ANO**	NE	**ANO**	NE
4	Samsung	Galaxy J4+	2018	**ANO**	**ANO**	NE	**ANO**	NE
5	Apple	iPhone 12 mini	2020	**ANO**	**ANO**	**ANO**	NE	**QZSS**

Podmínky testů byly stejné jako v první fázi (tj. zapnutí *Režimu letadlo* a restart po spuštění vysílání). Mezi sledované parametry byl zařazen také čas pro nabytí fiktivní lokace (pokud k tomu došlo) a čas, který byl zapotřebí k opětovnému zobrazení autentické polohy. Došlo-li k úspěšnému spoofingu, pokračovalo vysílání cca další minutu a poté byl simulátor vypnut.

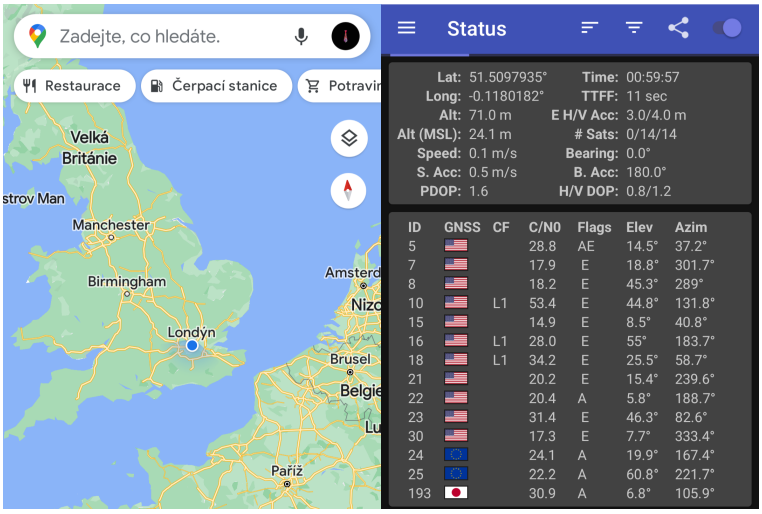
Po předchozích zkušenostech byl experiment nadále prováděn pouze s anténou 02, která dosahovala lepších výsledků. Testy probíhaly ve dvou scénářích. Scénář 1 se uskutečnil uvnitř budovy a pro simulaci byla zvolena statická lokace města Budapešť. Scénář 2 obsahoval totožný test se všemi zařízeními, ovšem mimo budovu a s vybranou lokací města Bruggy. Předpokladem byly rozdílné výsledky z důvodu snazšího příjmu autentického GNSS signálu na otevřeném prostranství. Testovací soupravy lze zhlédnout na Obrázku 30.



Obrázek 30: Vybavení k testu 1 pro druhou fázi, scénář 1 (A) a scénář 2 (B)

5.1.2 Výsledky měření

První fáze testování se potýkala s velkým počtem neúspěšných pokusů. Nezávisle na zvoleném prostředí se častým jevem namísto zamýšleného spoofingu stával jamming, při kterém mobilní zařízení Galaxy A33 ztratilo signál z autentických satelitů. Tento jev se opakoval i při změně simulované lokace, místa experimentu, vzdálenosti od simulátoru či intenzity vysílání. K prvnímu úspěšnému spoofingu došlo v prosinci 2022, kdy telefon získal falešnou polohovou informaci s lokací ve městě Londýn. Snímky obrazovky z aplikací při tomto testu jsou vyobrazeny na Obrázku 31. Tento experiment se ovšem v rámci první fáze nepodařilo zopakovat.



Obrázek 31: Snímky obrazovky z první fáze testování

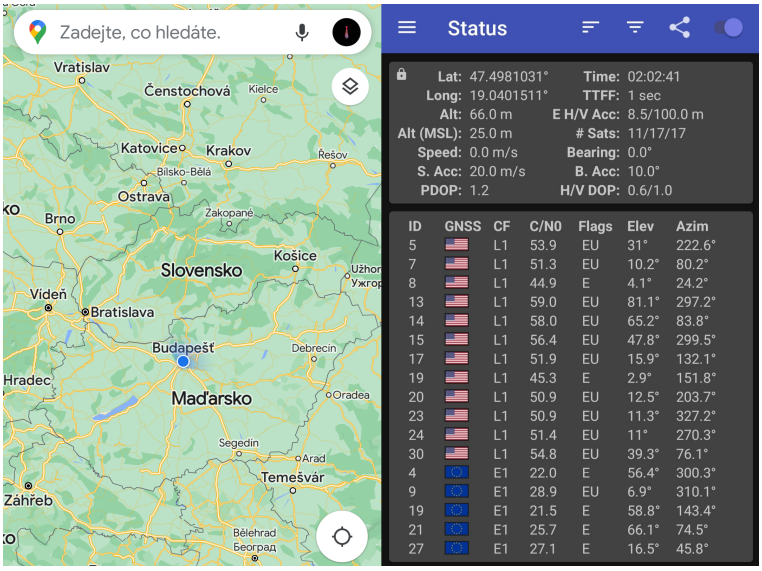
Druhá fáze již dosahovala lepších výsledků. U celkem čtyř z pěti testovaných zařízení byl proveden úspěšný spoofing a telefony tak zobrazovaly polohu na fiktivní lokaci ve městě Budapešť, respektive Bruggy, i přesto, že se ve skutečnosti nacházely v obci Říčany. Zobrazení falešného umístění bylo docíleno pouze u přístrojů výrobce Samsung, a to v obou scénářích. U zařízení Apple iPhone byl spoofing neúspěšný – vysílání se projevilo jako jamming.

Tabulka 7 zobrazuje informace, zdali byl spoofing úspěšný (položka „Fix“) a celkem dva časové údaje pro každý scénář ve formátu minuty:sekundy. Sloupec „Čas fix“ obsahuje dobu od zapnutí telefonu (konkrétně od výzvy pro zadání PIN kódu či zámku obrazovky) po zobrazení zafixování fiktivní polohy v aplikaci *GPSTest*. Údaj „Čas rec“ (z angl. recovery) zobrazuje čas od vypnutí simulátoru po nabytí autentické polohové informace (tj. zobrazení skutečné lokace v aplikaci *GPSTest*). Pokud tato doba překročila 15 minut, je v tabulce uvedeno „15+“.

Tabulka 7: Shrnutí výsledků testu 1, druhá fáze

ID	Zařízení	Scénář 1 – Budapešť IN			Scénář 2 - Bruggy OUT		
		Fix	Čas fix	Čas rec	Fix	Čas fix	Čas rec
1	Galaxy A33	ANO	1:22	15+	ANO	1:44	15+
2	Galaxy A51	ANO	0:51	15+	ANO	1:20	1:26
3	Galaxy A8	ANO	1:31	15+	ANO	1:37	15+
4	Galaxy J4+	ANO	1:57	15+	ANO	1:01	3:29
5	iPhone 12 mini	NE	jamm.	0:45	NE	jamm.	15+

Mimo zařízení ID 5 se „Čas fix“ nacházel vždy v intervalu 50 sekund až 2 minuty. U tří zařízení ze čtyř byly tyto časy vyšší pro scénář 2 – tj. mimo budovu. „Čas rec“ byl při testování uvnitř budovy vždy vyšší než 15 minut s výjimkou zařízení ID 5, které se ovšem zotavovalo pouze z vlivů jammingu. Při experimentech mimo budovu bylo u tohoto času dosaženo hodnoty menší než 15 minut u zařízení ID 2 a 4. Pro příklad jsou na Obrázku 32 uvedeny snímky obrazovky z aplikací *GPSTest* a *Google Mapy* při testování scénáře 1.



Obrázek 32: Snímky obrazovky z druhé fáze testování, scénář 1

Pro přehlednost je uveden seznam podmínek, které vedly k nejlepším výsledkům:

- Vzorkovací frekvence v textovém souboru: 2600000
- Použití GPS L1 antény 2J0801b
- Před zahájením vysílání vypnutí Wi-Fi, mobilních dat, Bluetooth (ideální *Režim letadlo*)
- Po spuštění vysílání restartování telefonu
- Umístění telefonu velmi blízko k anténě simulátoru (0 – 2 cm)
- Výchozí nastavení intenzity vysílání na SDR (tj. GAIN = 35)

V průběhu druhé fáze testování byl také vyzkoušen dynamický spoofing. Fiktivní trajektorie, nacházející se v centru Prahy, byla skrze *Google Mapy* a software *SatGen* exportována v textovém formátu NMEA a vložena do programu „gps-sdr-sim“. Vysílání bylo následně provedeno se zařízením ID 1 Samsung Galaxy A33. Výsledná lokace se sice měnila, ale pouze skokově a v určitých chvílích setrvávala pozice nehybně na jednom místě po dobu několika minut.

5.2 Test 2 – spektrální analyzátor

5.2.1 Metodika měření

Datum a místo provedení: 11. 4. 2023, Praha 1 – Staré Město, ČR

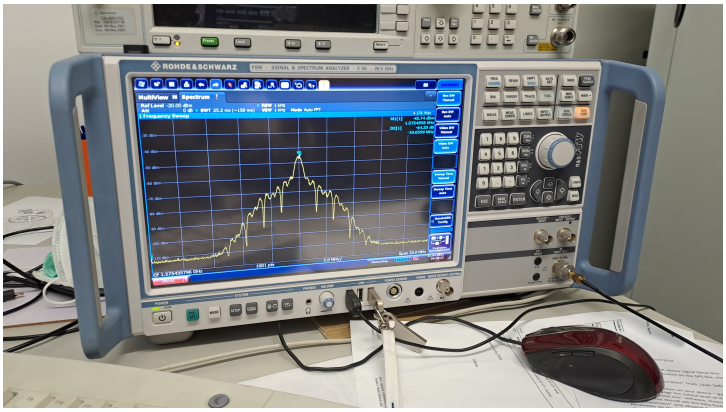
Vybavení:

- Simulátor, SMA redukce, kabeláž
- Aktivní anténa GPS L1 2J7C01MC3F plochá, 1575,42 MHz (dále jen anténa 01)
- Aktivní anténa GPS L1 2J0801b tyčová, 1575,42 MHz (dále jen anténa 02)
- Pasivní anténa GPS L1 2J4D01MP plochá, 1575,42 MHz (dále jen anténa 03)
- Faradayova klec ETS Lindgren 5230-36
- Rohde & Schwarz FSW signální a spektrální analyzátor

Druhý test spočíval v rozboru simulovaného signálu na spektrálním analyzátoru. Jedná se o zařízení, jež umožňuje zobrazit různé parametry elektromagnetického signálu v závislosti na jeho nastavení. Jelikož takovým přístrojem disponuje laboratoř speciálních projektů na FD ČVUT v Praze, bylo pro experiment využito toto pracoviště. Mimo analyzátor byla také použita Faradayova klec (také bezodrazová komora), jejíž funkcí je pohlcení rušivých signálů při bezdrátovém měření. Důvodem měření bylo ověření funkčnosti nově dodaných GPS antén (především antén 01 a 02) a také potřeba stanovení přesných hodnot intenzit, které lze nastavit pomocí parametru GAIN v softwaru Mayhem. Testované antény jsou vyobrazeny na Obrázku 33 [81].

Obrázek 33: Vybavení k testu 2 – simulátor, anténa 01 (A), anténa 02 (B), anténa 03 (C)

Měření bylo provedeno ve 3 odlišných scénářích za použití efemerid pro den testování. U všech byl pomocí simulačního softwaru opět vytvořen soubor s fiktivní statickou lokací a vložen na SDR. V jednotlivých případech bylo nutné nastavit parametry zobrazení na spektrálním analyzátoru. Jednalo o středovou frekvenci (center frequency), jejíž hodnota vždy odpovídala 1575,42 MHz, dále pak šířku zobrazovaného rozsahu pásma (span), která byla určena na 20 MHz nebo 5 MHz, a nakonec také rozlišovací šířku pásma (resolution bandwidth), jež byla použita na doporučení přítomných techniků v hodnotě 1 kHz. Na přístroji bylo nastaveno zobrazení grafu tzv. výkonového spektra (angl. power spectral density, zkr. PSD), jež byl následně hlavním výstupem tohoto experimentu. Konkrétní použité zařízení lze zhlédnout na Obrázku 34.

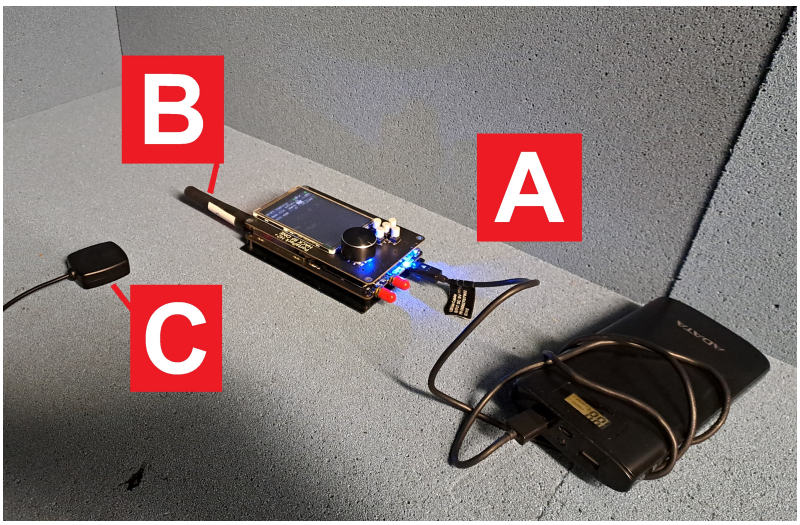


Obrázek 34: Spektrální analyzátor v laboratoři speciálních projektů FD ČVUT

Ve **scénáři 1** byl simulátor se spektrálním analyzátorem přímo propojen pomocí SMA kabelu a potřebných redukcí. Ve **scénářích 2 a 3** byl simulátor vložen do bezodrazové komory, uvnitř které se nacházela anténa 03 určená pro příjem signálu. Ta byla následně propojena kabeláží s analyzátorem. Ve scénáři 2 byla využita anténa 01 a měření proběhlo ve dvou různých vzdálenostech od přijímací antény – nejprve cca 80 cm, poté v těsné blízkosti. Ve scénáři 3 byla použita anténa 02 a test byl proveden pouze v těsné blízkosti, jak je možné vidět na Obrázku 35.

U výše uvedených scénářů byla provedena analýza pro celkem 6 hodnot intenzity signálu – nastavení GAIN = 1, 10, 20, 30, 40 a 47. Pro každou z těchto hodnot byl exportován PSD graf. Jedná se o grafickou reprezentaci signálu, která zobrazuje závislost vysílacího výkonu na frekvenci. Výsledná křivka je poté vyhlazena hodnotou rozlišovací frekvence. Také byla zaznamenána maximální hodnota výkonu (angl. nazývaná peak) [82].

Sekundárním výstupem byly NMEA zprávy, jejichž příjem a zpracování zprostředkovali přítomní pracovníci laboratoře nad rámec plánovaného měření. K tomuto účelu posloužil specializovaný software pracoviště, který umožnil export těchto dat v textovém formátu.



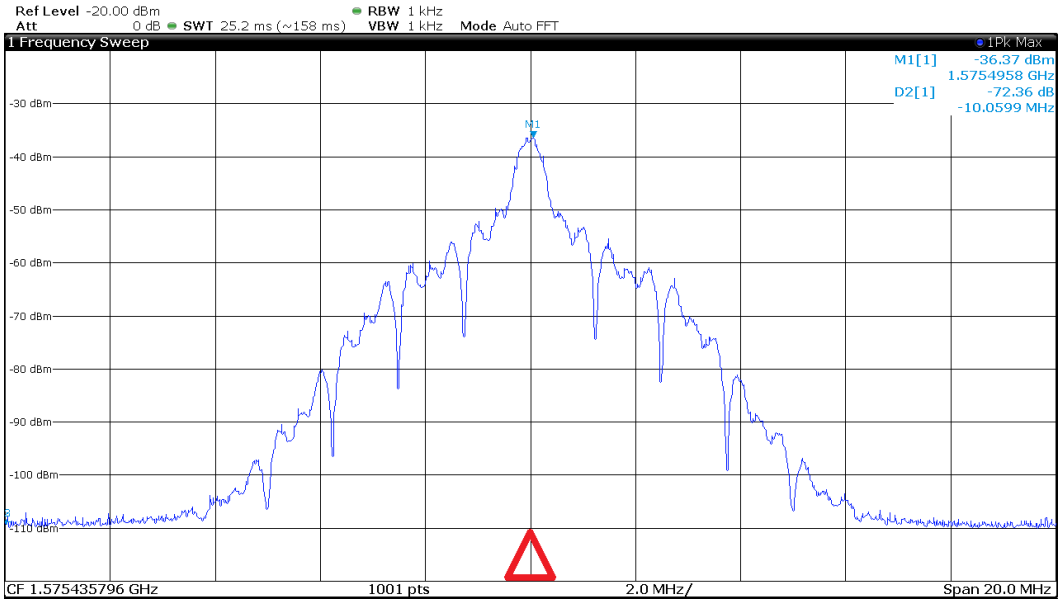
Obrázek 35: Testovací souprava pro scénář 3 - (A) simulátor, (B) anténa 02, (C) anténa 03

5.2.2 Výsledky měření

Základním výstupem měření byly PSD grafy ze spektrálního analyzátoru. Ty zobrazují na svislé ose výkon signálu v jednotkách dBm (logaritmická jednotka vztažené k hodnotě 1 mW) a na vodorovné ose frekvenci v jednotkách Hz. Jelikož na horizontální ose nejsou vyznačeny jednotlivé hodnoty, je v Obrázcích 36 až 38 vždy zvýrazněna středová frekvence (1575,42 MHz) červeným trojúhelníkem. Pro určení maximální hodnoty výkonu byla použita funkce markerů. Na grafech je tato hodnota vždy vyznačena markerem M1 a odpovídající výkon je uveden v pravém horním rohu.

Scénář 1, který spočíval v drátovém propojení, dosahoval nejvýraznějších zobrazení peaků. Ty byly pozorovány u veškerých nastavení položky GAIN (tj. 1 – 47) a jejich tvar se podobal typickému spektru autentického signálu GPS L1, jak naznačuje například Obrázek 36.

Čím nižší byla hodnota GAIN, tím nižší byl peak a tím pádem i maximální hodnota výkonu. Tímto byla potvrzena závislost vysílacího výkonu na nastavení parametru na SDR. Hodnoty výkonů lze zhlédnout v Tabulce 8.



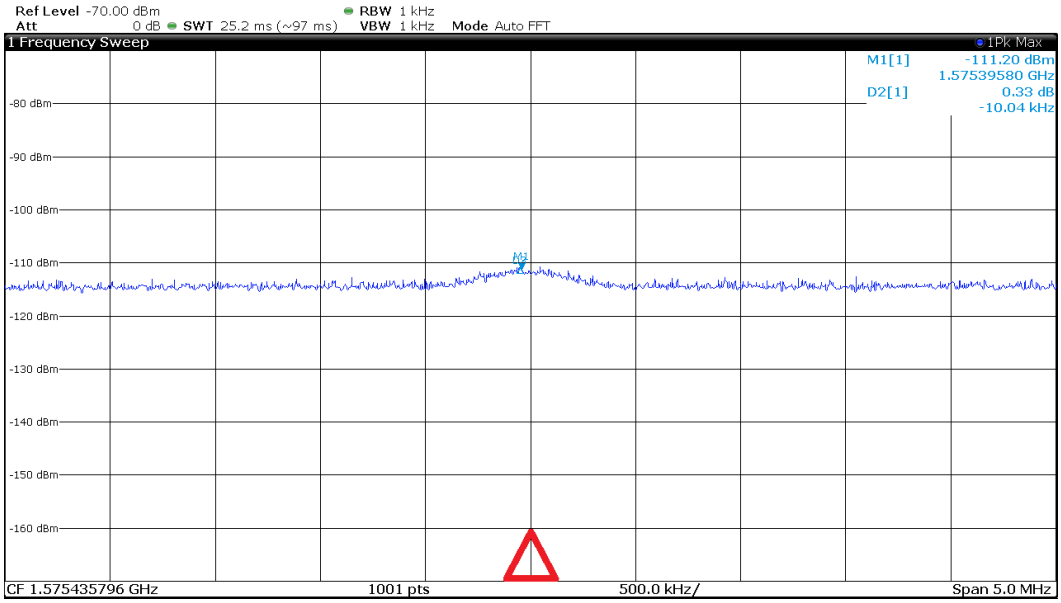
Obrázek 36: PSD graf, scénář 1, GAIN = 30

Tabulka 8: Změřené maximální výkony pro scénář 1

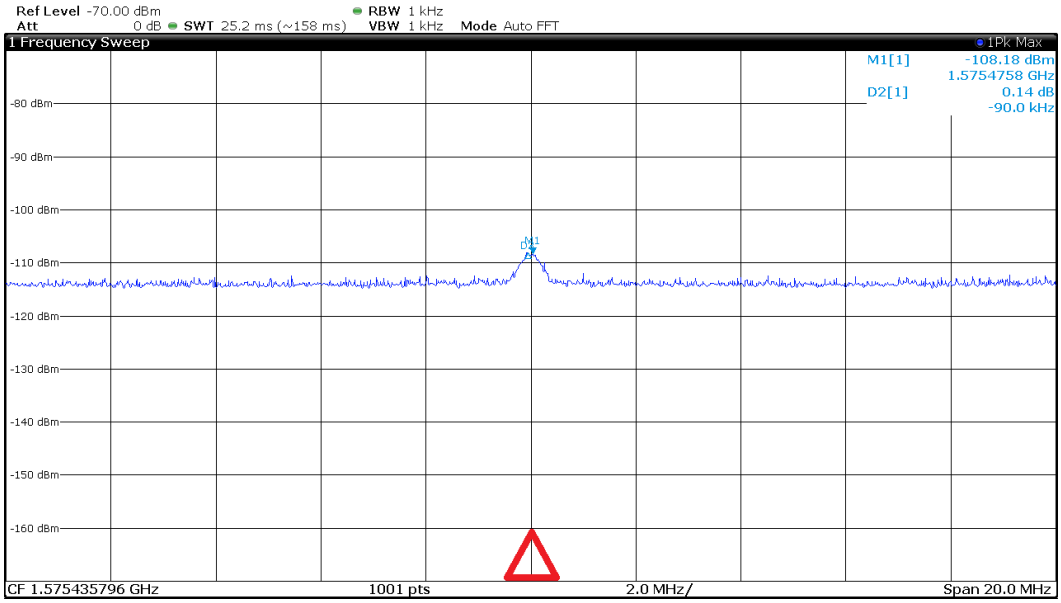
Výkon na SDR – GAIN [-]	1	10	20	30	40	47
Max. výkon na analyzátoru – M1 [dBm]	-65,51	-54,16	-45,71	-36,37	-29,91	-29,21
Přibližná hladina šumu [dBm]	-115	-113	-112	-109	-106	-105

V rámci **scénáře 2** při měření na vzdálenost 80 cm nebyl při žádné z hodnot GAINu zaznamenán typický peak. Grafy tak zobrazovaly pouze šum, který se během tohoto měření pohyboval kolem hodnoty -114 dBm. Po umístění antén do těsné blízkosti a nastavení GAIN = 47 byl již peak pozorován, a to s výkonem -111,2 dBm, jak ukazuje Obrázek 37. Rozdíl mezi ním a hladinou šumu tak činil pouze cca 3 dBm. Při snižování výkonu na SDR se intenzita signálu také snižovala a cca při hodnotě GAIN = 40 byl peak ztracen pod šumem.

U měření dle **scénáře 3** bylo pozorováno podobné chování jako v předchozím případě. Hladina šumu zůstala na hodnotě přibližně -114 dBm. Při maximálním nastavení GAIN byla hodnota výkonu signálu -108,18 dBm, jak interpretuje Obrázek 38. Peak tudíž vzrostl oproti scénáři 2 na výšku cca 6 dBm. Lepších výsledků dosahovala tato varianta i při snižování výkonu, kdy maximum zaniklo pod hladinu šumu při hodnotě GAIN = 35, tj. o 5 jednotek později.



Obrázek 37: PSD graf, scénář 2, GAIN = 47



Obrázek 38: PSD graf, scénář 3, GAIN = 47

Pro měření s anténou 02, která dosahovala lepších výsledků, byly také po dobu cca 5 minut nahrávány přijaté NMEA zprávy pomocí MATLAB skriptu poskytnutým v laboratoři. Z NMEA zpráv byly získány následující informace: identifikace, datum a čas zprávy, počet satelitů v používání (*NumSatInUse*), vypočítaná poloha, chyba polohy, počet viditelných satelitů (*NumSatInView*), azimut, elevace a další podrobnosti.

V naprosté většině se parametr *NumSatInView* pohyboval v rozmezí 14 – 16 satelitů, nejčastěji šlo o hodnotu 16. Takový počet se shodoval s informací, kolik satelitů by měl generovat kód „gps-sdr-sim“ dle jeho autora. Oproti tomu se parametr *NumSatInUse* v celém záznamu rovnal číslu 0. Z toho lze vyvodit, že přijímač fiktivní satelity rozpoznal, ovšem nepoužil je pro výpočet polohy, která tak zůstala neznámá. V určitých intervalech byla u některých satelitů dostupná také hodnota azimutu a elevace.

5.3 Test 3 – profesionální u-blox přijímače

5.3.1 Metodika měření

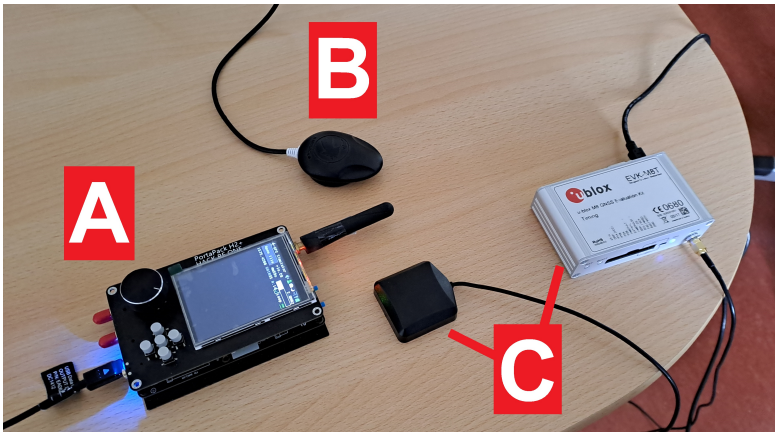
Datum a místo provedení: 21. 6. 2023, Praha 2 – Nové Město, ČR

Vybavení:

- Simulátor
- Aktivní anténa GPS L1 2J0801b tyčová, 1575,42 MHz
- Přijímač u-blox 8 UBX-M8030-KT od společnosti Navilock (dále jen přijímač Navilock)
- Přijímač u-blox EVK-M8T zapůjčený společností ŘLP (dále jen přijímač EVK)
- PC se softwarem *u-center*

Cílem třetího testu bylo zjištění účinků simulátoru na přijímače, které se – na rozdíl od zařízení v prvních testech – používají čistě pro příjem GNSS signálu a poskytují více výstupních parametrů. K takovému měření byly zajištěny dva přístroje. Prvním byl multikonstelační GNSS přijímač od německé firmy Navilock využívající hardware u-blox 8 UBX-M8030-KT. Dle výrobce je schopen přijímat signály ze všech globálních konstelací i regionální QZSS. Přijímač Navilock pracuje na jednotné frekvenci ekvivalentní k GPS L1 a byl poskytnut Ústavem letecké dopravy FD [83].

Druhým přístrojem byl také multikonstelační přijímač, model u-blox EVK-M8T, který ze svého inventáře poskytlo Řízení letového provozu ČR (zkr. ŘLP). EVK-M8T umožňuje příjem z konstelací GPS a GLONASS a pracuje na stejné frekvenci jako předchozí přístroj. Na rozdíl od prvního přijímače, který představuje integrované řešení řídící jednotky a antény, jsou u tohoto zařízení jednotlivé části odděleny, jak interpretuje Obrázek 39 [84].



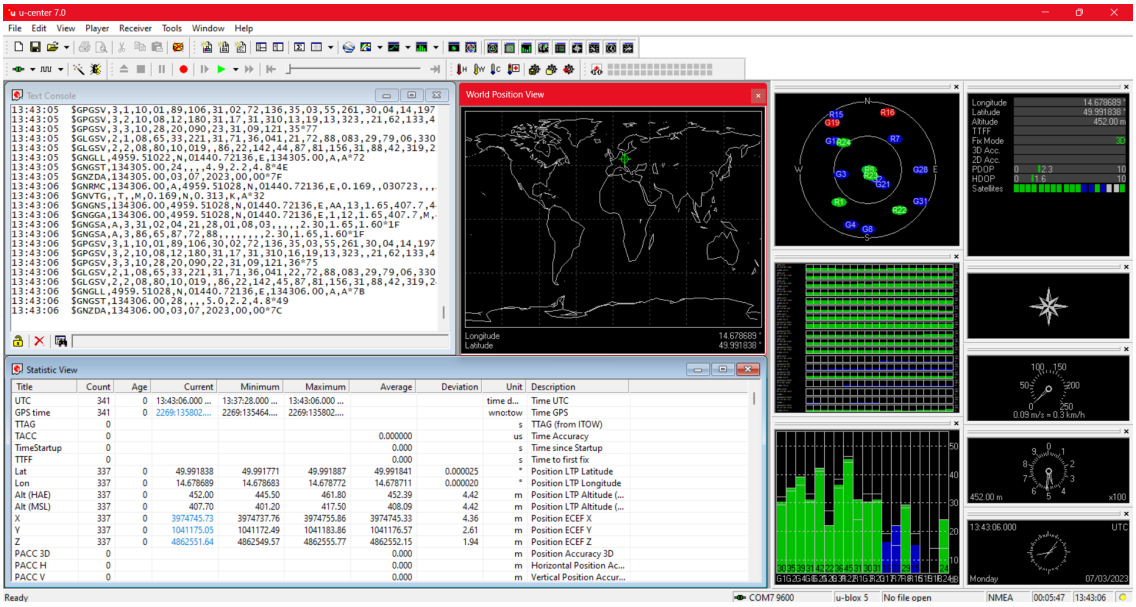
Obrázek 39: Vybavení k testu 3 – simulátor (A), přijímač Navilock (B), přijímač EVK (C)

Oba zmíněné přijímače využívají hardware od výrobce u-blox. Jedná se o švýcarskou společnost, která se zaměřuje na vývoj komunikačních zařízení, GNSS modulů, a bezdrátových polovodičů. Prostřednictvím USB kabelů byly tyto přístroje připojeny k PC, na němž probíhalo jejich ovládání pomocí softwaru *u-center*, rovněž od firmy u-blox. Tento program umožnuje zobrazit veškerá přijímaná data z GNSS satelitů. Po spárování s přijímačem se v pravé části aplikace zobrazí základní informace jako např. vypočítaná poloha, údaje o přesnosti, čas, výška, rychlost, poloha satelitů a výkonové poměry přijímaných signálů $C/N0$. Zobrazení dalších oken záleží na volbě uživatele. Užitečným nástrojem je konzole, která umožňuje prohlížení přijatých zpráv v textovém či NMEA formátu. Často využívanými funkcemi jsou také statistická zobrazení, náhledy různých grafů či histogramů a znázornění polohy na mapovém podkladu. Příklad rozvržení programu se zapnutou NMEA konzolí a statistickým zobrazením lze zhlédnout na Obrázku 40 [85].

Mimo těchto funkcí disponuje *u-center* také řadou ovládacích prvků. Mezi ně lze zařadit například volbu nahrávání, která umožňuje celé měření uložit a zpětně jej přehrát. Dále lze v aplikaci provést celkem tři druhy restartů zařízení [85]:

- „Hotstart“ – zachová informace o poloze, času, efemeridy a almanach
- „Warmstart“ – zachová informace o poloze, času a almanach, vymaže efemeridy
- „Coldstart“ – vymaže veškeré informace

Součástí přípravy testu bylo jako v předchozích případech vytvoření souboru se simulovaným signálem, tentokrát s polohou města Rio de Janeiro. Při měření byly antény obou přijímačů umístěny v těsné blízkosti simulátoru. Na zařízení HackRF bylo po celou dobu nastavení GAIN = 1 a vysílání zajišťovala tyčová anténa 2J0801b (v předchozích testech označovaná anténa 02).

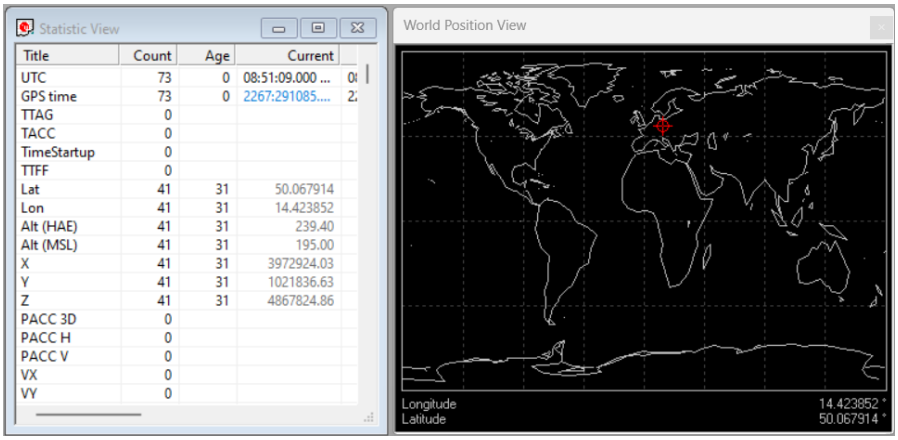


Obrázek 40: Prostředí programu u-center

Přístroje byly nejprve ponechány po určitou dobu při příjmu autentického signálu. Experiment byl dále rozdělen do dvou částí. První byl proveden **scénář 1**, při kterém byly oba přijímače bez další konfigurace vystavěny simulovanému signálu. Mohly tedy přijímat signál z více konstelací na jedné frekvenci. Následně byl testován **scénář 2**, u kterého byly omezeny přijímané konstelace pouze na GPS. Této varianty se účastnil pouze přijímač EVK, jelikož přijímač Navilock toto omezení nastavit neumožnuje. Dle potřeby bylo poté přistupováno k určitým druhům restartů. V obou případech probíhal dohled nad testy prostřednictvím softwaru *u-center*, ve kterém byly scénáře nahrány a uloženy.

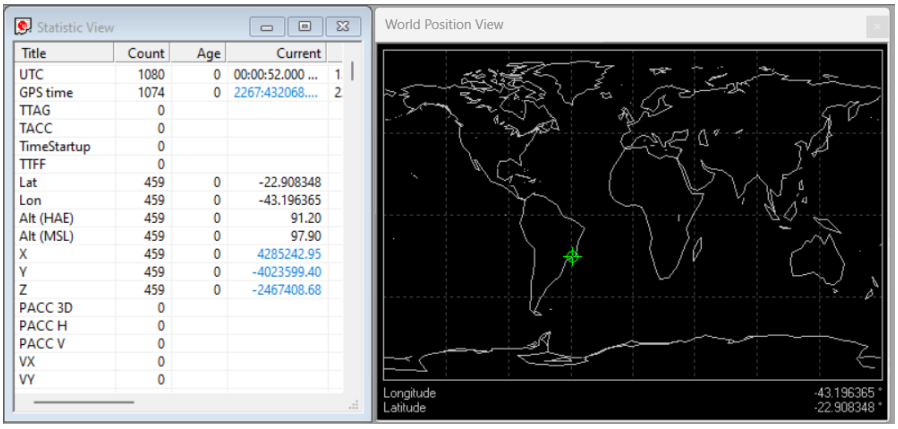
5.3.2 Výsledky měření

Výsledky měření **scénáře 1** byly následovné. Přijímač Navilock ihned po spuštění vysílání ztratil autentický signál. V tomto stavu byl ponechán několik minut a ani po delší době nedošlo k fixaci na autentickou či fiktivní polohu, jak naznačuje snímek obrazovky na Obrázku 41. Dle softwaru *u-center* přístroj po celou zpracovával pouze signál z konstelací GPS a GLONASS, i přestože měl být podle popisu schopen přijímat také Galileo a BeiDou.



Obrázek 41: Ztráta polohy v u-center, scénář 1

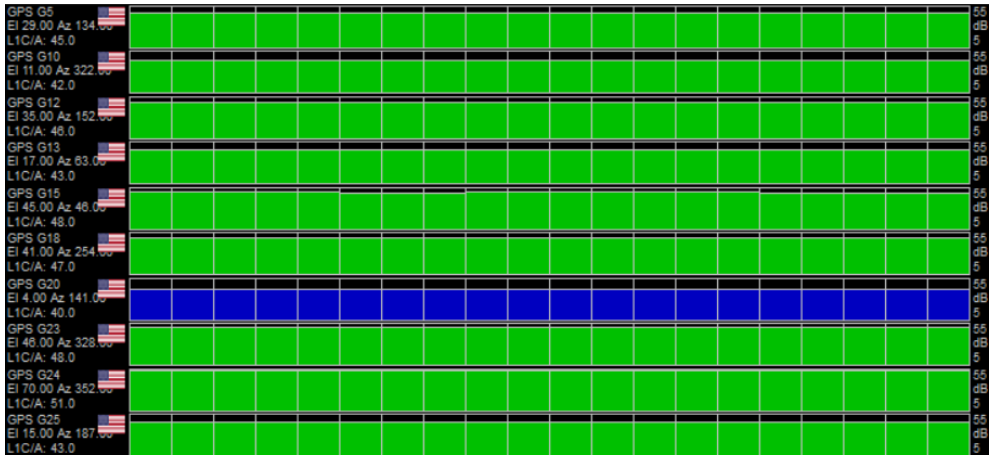
Poté bylo přistoupeno k „hotstartu“. Ani ten ovšem stav přijímače nezměnil. Dalším krokem bylo spuštění „warmstartu“, po kterém zařízení cca minutu vyhledávalo signál a následně se úspěšně zafixovalo na simulovanou lokaci ve městě Rio, jak je vyznačeno na Obrázku 42. V tuto chvíli se vyrovnaly poměry $C/N0$ u veškerých satelitů a fixace setrvávala až do ukončení vysílání. Stejný experiment byl zopakován o pár dní později, kdy došlo k přemístění na fiktivní polohu až po zvolení možnosti „coldstart“.



Obrázek 42: Fixace na polohu v u-center, scénář 1

Pro totožný scénář bylo u přijímače EVK pozorováno odlišné chování, kdy po spuštění vysílání neztratil autentickou polohu ihned. Po určitém čase začalo zařízení skokově měnit stavy mezi ztrátou signálu a fixací na pravou lokaci. Následně bylo opět přistoupeno k procesům „hotstart“ a „warmstart“. Ani jeden ovšem situaci nezměnil a byl tak spuštěn „coldstart“. Cca po půl minutě se přístroj zafixoval na simulovanou lokaci.

Scénáře 2 se účastnil přijímač EVK, u kterého byly konstelace omezeny pouze na GPS L1, kterou je schopen generovat simulátor. Po zapnutí SDR došlo k jammingu a zařízení ztratilo informaci o poloze. Rušení pokračovalo přibližně 5 minut a poté se přijímač zafixoval na lokaci v Riu, a to bez nutnosti jakéhokoliv restartu. V tuto chvíli se opět vyrovnaly poměry $C/N0$, jak je možné vidět na Obrázku 43. Čas 5 minut, jež byl zapotřebí k fixaci pozice, odpovídá hodnotě 300 sekund, pro kterou byl vygenerován soubor pomocí softwaru „gps-sdr-sim“.



Obrázek 43: Poměry $C/N0$ po fixaci pro scénář 2

Vybrané parametry výše uvedených simulací byly aritmeticky zprůměrovány a shrnuty do Tabulky 9. První sloupec popisuje, o jaký scénář se jednalo a jaký přijímač byl použit. Dále je uvedena informace, zdali byl k určení polohy potřeba určitý druh restartu a poté další veličiny změřené při příjmu autentického signálu a následně po fixaci na simulovaný signál. Sloupce „Tracked“ obsahují počet všech zaměřených satelitů a sloupce „Used“ uvádí počet satelitů použitých k výpočtu polohy. Na závěr jsou vypsány průměrné hodnoty poměru $C/N0$ pro veškeré signály přijaté z jednotlivých satelitů.

Tabulka 9: Základní parametry testu 3

Scénář	Restart	Autentický signál - FIX			Simulovaný signál - FIX		
		Tracked	Used	$C/N0$ [dB-Hz]	Tracked	Used	$C/N0$ [dB-Hz]
1 - Navilock	Warm / Cold	19	5	25	38	9	42
1 - EVK	Cold	21	9	22	33	9	42,5
2 - EVK	-	9	5	19	24	9	45

Nad rámec plánovaných scénářů byla provedena také simulace časové informace. Test proběhl úspěšně a po fixaci na polohu se zadaný čas zobrazil v *u-center*. Dále bylo zjištěno, že pokud nedojde k upřesnění času, vysílá simulátor signál defaultně ve smyčce od 23:59 do 00:04 UTC (v případě výchozí délky vysílání 300 sekund).

5.4 Diskuze výsledků

Celkem byly provedeny tři testy sestaveného GPS simulátoru. Cílem těchto experimentů bylo ověřit, zdali zařízení správně funguje a splňuje veškeré požadavky, za jejichž účelem bylo sestrojeno. Tyto požadavky zahrnovaly převážně vysílání GPS signálu zahrnující PRN i navigační zprávu, které by umožnilo testování odolnosti dalších zařízení vůči spoofingu. Během zmíněných testů bylo prostřednictvím různých přijímačů a dalších přístrojů pozorováno, jakou charakteristiku má vysílaný signál a zdali došlo k úspěšnému spoofingu či nikoliv. Testům předcházela zdárná kompilace simulační aplikace a spuštění vysílání na SDR simulátoru.

Součástí testu 1 bylo podrobení různých mobilních telefonů vlivům vysílání simulátoru. V první fázi docházelo k opakovaným neúspěchům, kdy vysílaný signál způsoboval na telefonech spíše jamming, ovšem nedošlo k výpočtu jakékoliv polohy. Později bylo usouzeno, že hlavní příčinou takových výsledků mohlo být použití stříbrné tyčové antény s příliš širokým rozsahem (40 - 6000 MHz). To ovšem vyvrátily další experimenty, při kterých již byly použity antény speciálně upravené pro signál GPS L1. I po této modifikaci docházelo převážně k neúspěšným testům a namísto spoofingu převažovaly vlivy jammingu.

Posléze bylo přistoupeno k úvaze, že důvodem je nesprávné nastavení vzorkovací frekvence v textovém souboru, jež byl na SDR nahráván spolu se samotným C8 souborem. Po přepsání této veličiny na hodnotu 2,6 MHz a použití GPS L1 antény docházelo téměř pouze k úspěšným měřením, při kterých přijímače sledovaly simulované družice a zobrazovaly generovanou polohovou informaci. Tento obrat zapříčinilo pravděpodobně sladění vzorkovací frekvence s hodnotou, při které software „gps-sdr-sim“ defaultně vytváří své soubory. Při této konfiguraci byly testy opakovány a opět s kladnými výsledky.

Ve výsledcích shrnutých v Tabulce 7 lze pozorovat, že časy v položce „Čas fix“ (doba od počátku vysílání do chvíle, kdy přijímač začal sledovat generovaný signál) jsou pro scénář 2 zpravidla větší než pro scénář 1. Pravděpodobným důvodem tohoto chování bylo konání druhého scénáře venku,

kde mobilní telefony přijímaly autentický signál z více satelitů, s větší intenzitou signálu a bylo tak obtížnější je zaspoofovat. Naproti tomu některé časy v položce „Čas rec“ (doba od vypnutí simulátoru po fixaci na autentický signál) byly větší ve scénáři 1. To bylo nejspíše zapříčiněno vnitřním prostředím, kdy v budově bylo pro mobily náročnější opětovně se zafixovat na autentický GNSS signál.

Test 1 lze závěrem porovnat s tabulkou v GitHub projektu „portapack-mayhem“ (sekce *Wiki* → *Applications* → *Transmitters* → *GPS Sim*) [77]. Autoři zde uvádí úspěšný spoofing u všech tří zmíněných mobilních telefonů Samsung. To souhlasí s výsledky naměřenými v této práci v rámci druhé fáze. Naopak rozporuplná je zmínka autorů o úspěšném zaspoofování zařízení Apple, které se v této práci nezdařilo.

Následoval test 2, který měl za úkol změřit výkonové charakteristiky vysílání simulátoru na spektrálním analyzátoru. Ve všech provedených scénářích lze považovat dosažené výsledky za úspěšné. Obdržené PSD grafy, byly svými tvary velice podobné autentickému signálu GPS L1. Dále byla změřena závislost mezi nastavením GAIN a vysílacím výkonem SDR, kdy se v omezeném rozsahu změna položky GAIN o jednu jednotku zobrazila jako změna intenzity na analyzátoru o 1 dBm.

Součástí výsledků tohoto testu byl také soubor s přijatými NMEA zprávami. V souhrnu data ukazovala, že software přijímal signál ze všech 16 simulovaných satelitů, ovšem žádný nevyužil pro výpočet polohy. Z toho důvodu nebylo dosaženo fiktivní lokace. Příčinu tohoto neúspěchu lze přisoudit faktu, že přijímač nebylo možné restartovat a v paměti tak zůstaly uloženy autentické efemeridy přijaté dříve. Alternativním důvodem mohl být příliš krátký čas, po který byl simulátor spuštěn či ostatní autentické konstelace, ze kterých byl přijímač schopen určit svou polohu.

Nakonec byl proveden test 3 spočívající ve vystavení profesionálních u-blox přijímačů simulovanému signálu. Výsledky experimentu prokázaly, že pokud přístroje nejprve přijímaly autentický signál, bylo zapotřebí je restartovat a až poté došlo k úspěšnému výpočtu fiktivní polohy. To platilo v případě, kdy byly k určení polohy využívány i další konstelace než jen GPS L1. Byl-li příjem omezen na signál GPS L1, nebyl restart nutný a po cca 5 minutách došlo k přechodu na simulovanou polohu. Tento výsledek je pro praktický výzkum práce velmi důležitý, jelikož frekvence L1 je pro mnohé soudobé přijímače v letectví jediným zdrojem polohy z GNSS.

U tohoto testu přineslo zajímavé výsledky také pozorování výkonů signálu. Bylo změřeno, že při příjmu autentického signálu se hodnota $C/N0$ pohybuje v rozmezí 19 – 25 dB-Hz, zatímco při zafixování na simulovaný signál byl poměr v průměru 43 dB-Hz. Z toho lze usoudit, že přijímač by považoval simulovaný signál za reálný snáze, pokud by došlo k nastavení tohoto výkonu mírně nad hladinu autentického GPS L1. Toho lze docílit například za pomoci externích prvků jako jsou atenuátory. Dále byla potvrzena domněnka, že simulátor vždy vysílá signál ze 16 fiktivních satelitů, ovšem přijímač využije pro výpočet polohy pouze ty, které by mohl reálně pozorovat ze simulované lokace (nejčastěji určuje parametr přijímače „elevation mask“).

Obecně lze považovat výsledky celé praktické části za pozitivní. S ohledem na stanovené cíle došlo k jejich naplnění – tj. byla ověřena správná funkčnost sestaveného přístroje a byly provedeny úspěšné testy spoofingu různých zařízení. Zároveň byla stanovena podobnost vysílaného spektra s autentickým signálem. Výsledky experimentů lze pokládat za validní, jelikož byly vykonány na různých zařízeních a za několika odlišných podmínek. Jelikož byly testy 1 a 3 provedeny na vícero přijímačích, lze zároveň připustit zevšeobecnění těchto výsledků.

6 Další uplatnění a rozvoj

Sestavené a otestované zařízení pro simulaci GPS signálu otevírá mnoho možností dalšího uplatnění, zároveň je zde i prostor pro jeho rozvoj a modernizaci. V ohledu budoucího uplatnění se v rámci letectví nabízí testování výkonnosti GNSS přijímačů, které jsou nedílnou součástí každého dopravního letadla a velké části CNS infrastruktury. Tento proces by mohl být doplňkem k live-sky testování a používání klasických simulátorů. Takové testy by mohly být prováděny porovnáním simulované a vypočítané polohy, z čehož lze číselně vyjádřit přesnost určení polohy a statistickou hodnotu chyby přijímače. Za druhou variantu využití lze považovat měření odolnosti přijímačů vůči spoofingu či ověření metodiky takového měření. Obě možnosti uplatnění lze aplikovat i v přehledových leteckých systémech využívající GNSS, mezi které řadíme sekundární radar, multilaterační systémy či ADS-B zprávy. Dále se nabízí testování jakýchkoliv jiných GNSS přijímačů i mimo letecké odvětví.

Současný stav evropských regulací pro letadlové GNSS přijímače vyžaduje podporu pouze frekvencí GPS L1 a GLONASS G1. Na první z těchto frekvencí lze provádět testy se sestrojeným simulátorem. Do budoucna se ovšem v letectví počítá s rozšířením na konstelace BeiDou a Galileo a frekvenci L5 (1176,45 MHz). Kupříkladu pro takové účely lze uvažovat o rozšíření vysílání sestaveného zařízení na další frekvence či globální a regionální konstelace. K této modifikaci však aktuálně neexistuje žádný volně dostupný skript. Dále by mohlo být vhodné pořízení dalšího SDR, a to výkonnějšího pro dosažení lepších výsledků či identického pro realizaci pokročilejších metod rušení, jako např. meaconingu. Pro úpravy vysílacího výkonu lze zvážit rozšíření o specifické hardwarové prvky jako jsou antény, zesilovače a atenuátory [86].

I přes přínosy praktické části této práce a budoucí potenciál sestrojeného zařízení, je nutné mít na mysli možné zneužití dosažených výsledků. Například v letectví je GNSS součást CNS systémů a zajišťuje primární zdroj polohové informace pro většinu letadel. Jelikož letecká navigace spoléhá především na frekvenci GPS L1, bylo by teoreticky možné způsobit zkonstruovaným simulátorem rušení, které by mohlo negativně ovlivnit bezpečnost provozu. Za hrozbu lze považovat i jakékoliv jiné narušení GNSS vysílání pro kritickou i nekritickou infrastrukturu, které je v ČR považováno za protiprávní akt.

Závěr

Tato bakalářská práce rozebírá problematiku simulace GNSS signálu a zaměřuje se na variantu s využitím softwarově definovaného rádia. Úvodní část obsahuje obecný vhled do GNSS systémů se zaměřením na vysvětlení základního principu fungování GNSS a elementárních typů rušení. Dále navazuje kapitola specificky zaměřená na způsoby simulace GNSS signálu s porovnáním dvou základních variant testování GNSS zařízení, kterými jsou live-sky testování a použití GNSS simulátorů. Následně práce podrobně vysvětluje fungování GNSS simulátorů na bázi SDR a sumarizuje vhodná SDR zařízení a volně dostupné skripty pro generování GNSS signálu.

Poslední zmíněná kapitola přichází se znalostními podklady pro praktickou část, ve které dochází k samotnému sestrojení simulátoru s jedním konkrétním typem hardwaru a zvoleným simulačním skriptem. Je popsána kompilace simulační aplikace, postup při vytváření souborů, jejich přesunutí do simulátoru a jeho spuštění a ovládání. Pro demonstraci správné funkčnosti sestaveného přístroje jsou v navazující kapitole provedeny tři různé testy. Ty zahrnují otestování příjmu signálu mobilními telefony, pokročilými u-blox přijímači a podrobení vysílání spektrální analýze ve specializované laboratoři. Práce je zakončena úvahou o dalším uplatnění a rozvoji vytvořeného GPS L1 generátoru.

Přes dosažené úspěchy je nutné mít na paměti, že sestavený simulátor je omezen na frekvenci GPS L1. I přestože pokročilé přijímače využívají k určení polohy více konstelací, respektive frekvencí, v odvětví letecké dopravy lze nalézt velký počet zařízení pracující pouze se signálem GPS L1, popřípadě také s blízkou frekvencí GLONASS G1. S těmito přijímači lze realizovat různá testování, která jsou zmiňována dále. Proces sestrojení simulátoru spočíval v pořízení SDR a implementaci již vytvořeného simulačního programu. I přestože nebyl tento skript upravován, je nutné vzít v úvahu, že i proces samotné implementace byl velmi časově náročný a další vylepšení by překračovaly očekávaný rozsah této práce. Zmíněné limitace jsou též vyváženy snadnou obsluhou zařízení a nízkými pořizovacími náklady.

Díky práci bylo sestrojeno zařízení na základech SDR HackRF umožňující generování GPS L1 signálu včetně PRN a navigační zprávy. Takové řešení přináší levný, rychlý a snadno proveditelný způsob GNSS simulace. Zároveň je zahrnut kompletní postup sestavení, dle něhož je možné, za předpokladu pořízení vlastního SDR, proces zreplikovat. Bylo dokázáno, že mnohé přijímače považují přijatý signál ze simulátoru za autentický a zpravidla po restartu podléhají spoofingu.

Do budoucna lze uvažovat o různých potenciálech sestrojeného zařízení. Z těch nejdůležitějších je možné zmínit testování výkonnosti GNSS přijímačů a měření odolnosti vůči vlivům GNSS rušení, například v rámci laboratoře CNS/ATM systémů na Ústavu letecké dopravy FD ČVUT. Jelikož moderní navigační prostředky nespoléhají pouze na signál GPS L1, lze rozvážit rozšíření simulátoru o další konstelace či frekvence. Další vylepšení by mohly být provedeny pořízením rozlišných antén či implementací dalších hardwarových prvků.

Seznam použité literatury

1. *What is Positioning, Navigation and Timing (PNT)? — US Department of Transportation*. Washington, D.C.: U.S .Department of Transportation, 2017. Dostupné také z: https://www.transportation.gov/pnt/what-positioning-navigation-and-timing-pnt.
2. *Satellite navigation*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné také z: https://en.wikipedia.org/wiki/Satellite_navigation.
3. VOJTEK, David. Globální navigační a polohové systémy - Prednášky pro obor Geoinformatika. In: Ostrava: Hornicko-geologická fakulta VŠB-TU Ostrava, 2014. Dostupné také z: https://geoinformatika-1.vsb.cz/vojtek/content/gnps/files/_source/Ucebni-texty-GNPS-distancni.pdf.
4. *What are the different GNSS Constellations? - everything RF*. everything RF, 2022. Dostupné také z: https://www.everythingrf.com/community/what-are-the-different-gnss-constellations.
5. *Modern civilization would be lost without GPS - SpaceNews*. University Park: SpaceNews, The Pennsylvania State University, 2021. Dostupné také z: https://spacenews.com/modern-civilization-would-be-lost-without-gps/.
6. PLENINGER, Stanislav. Prezentace k předmětu 21ZT: Zabezpečovací letecká technika: Soubor GNSSpart1.pdf. In: Praha: ČVUT v Praze, Fakulta dopravní, Ústav letecké dopravy, 2022.
7. *GPS.gov: GPS Overview*. Washington, [b.r.]. Dostupné také z: https://www.gps.gov/systems/gps/.
8. *Centimeter Precision Positioning GNSS RTK Technology*. Box Hill: Tersus GNSS, [b.r.]. Dostupné také z: https://www.tersus-gnss.com/technology.
9. *GNSS Signal - Navipedia*. Madrid: European Space Agency GSSC, [b.r.]. Dostupné také z: https://gssc.esa.int/navipedia/index.php/GNSS_signal.
10. KOVÁŘ, Pavel. *Družicová navigace: Od teorie k aplikacím v softwarovém přijímači*. Praha: Česká technika - nakladatelství ČVUT, 2016. ISBN 978-80-01-05989-0.

11. YVON, Henri; ATILLA, Matas; BAUMANN, Ingo. RNSS and the ITU Radio Regulations. *InsideGNSS*. 2018. Dostupné také z: https://www.insidegnss.com/auto/janfeb18-LAW.pdf.

12. REIL, Andreas. Receiving BEIDOU, GALILEO and GPS signals with MATLAB® and RS® IQR, RS®TSMW: Application Note. *Rohde Schwarz*. [B.r.]. Dostupné také z: https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma203/1MA203_0e_BeiDouSWReceiver.pdf.

13. *GPS.gov: Space Segment*. Washington, [b.r.]. Dostupné také z: https://www.gps.gov/systems/gps/space/.

14. *GPS.gov: New Civil Signals*. Washington, [b.r.]. Dostupné také z: https://www.gps.gov/systems/gps/modernization/civilsignals/%5C#L2C.

15. *GPS Signal Plan - Navipedia*. Madrid: European Space Agency GSSC, [b.r.]. Dostupné také z: https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan.

16. *GPS signals*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné také z: https://en.wikipedia.org/wiki/GPS_signals.

17. PLENINGER, Stanislav. Prezentace k předmětu 21ZT: Zabezpečovací letecká technika: Soubor GNSSpart2.pdf. In: Praha: ČVUT v Praze, Fakulta dopravní, Ústav letecké dopravy, 2022.

18. *CDMA FDMA Techniques - Navipedia*. Madrid: European Space Agency GSSC, [b.r.]. Dostupné také z: https://gssc.esa.int/navipedia/index.php/CDMA_FDMA_Techniques.

19. *GNSS Receivers General Introduction - Navipedia*. Madrid: European Space Agency GSSC, [b.r.]. Dostupné také z: https://gssc.esa.int/navipedia/index.php/GNSS_Receivers_General_Introduction.

20. BHATTA, Basudeb. *Global Navigation Satellite Systems: New Technologies and Applications*. Second edition. Boca Raton: CRC Press, 2021. ISBN 978-0-367-47408-9.

21. *GNSS Basic Observables - Navipedia*. Madrid: European Space Agency GSSC, [b.r.]. Dostupné také z: https://gssc.esa.int/navipedia/index.php/GNSS_Basic_Observables.

22. ŘEPÍK, Michal. *Keplerova rovnice*. 2014. Dostupné také z: http://www.michalrepik.cz/matematika/keplerova_rovnice.html.

23. *Globální družicový polohový systém: Určování polohy a času*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné také z: https://bit.ly/3JiKzQ2.

24. *GitHub - barbeau/gpstest: The #1 open-source Android GNSS/GPS test program*. GitHub, c2023. Dostupné také z: https://github.com/barbeau/gpstest.

25. POSPÍŠIL, Martin. *Rušení signálu GNSS a dopad na letectví*. Praha, 2019. Bakalářská práce. ČVUT v Praze, Fakulta dopravní, Ústav letecké dopravy.

26. *Why Simulate?: What is a GNSS Simulator? Why should you use one for testing?* Paignton: Spirent, 2010. Dostupné také z: https://www.nottingham.ac.uk/grace/documents/resources/glossariestutorials/aboutgnsssimulator.pdf.

27. VODIČKOVÁ, Kristýna. *Možnosti zavádění technologií na odhalování nezákonného rušení GNSS signálu v ČR*. Praha, 2018. Diplomová práce. ČVUT v Praze, Fakulta dopravní, Ústav letecké dopravy.

28. WALKER, Andy. *Limitations of Live Sky Testing in a Production Environment*. Crawley: Spirent, 2012. Dostupné také z: https://www.spirent.com/blogs/limitations-of-live-sky-testing-in-a-production-environment.

29. STŘELCOVÁ, Kateřina. *Metody certifikace GNSS aplikací v dopravě*. Praha, 2010. Bakalářská práce. ČVUT v Praze, Fakulta dopravní, Ústav dopravní telematiky.

30. KREJČÍ, Jan. *Metody simulace GNSS systémů pro účely testování v dopravní telematice*. Praha, 2010. Bakalářská práce. ČVUT v Praze, Fakulta dopravní, Ústav letecké dopravy.

31. *What is GNSS Simulation?: And how can simulation help reduce your time to market? - Spirent White paper*. Devon: Spirent, 2010. Dostupné také z: https://www.nottingham.ac.uk/grace/documents/resources/glossariestutorials/whatisgnsssimulation.pdf.

32. *Why use a GNSS Simulator — CAST Navigation*. Tewksbury: CAST Navigation, c2020. Dostupné také z: https://castnav.com/why-use-a-gnss-simulator/.

33. *The Future of GNSS Simulation is Software-defined*. Cleveland: GPS World - North Coast Media, c2023. Dostupné také z: https://www.gpsworld.com/sponsoredcontent/the-future-of-gnss-simulation-is-software-defined/.

34. *GSG 5/6 GPS/GNSS Simulators*. Les Ulis: Safran, [b.r.]. Dostupné také z: https://safran-navigation-timing.com/product/gsg-5-6-series-gps-gnss-simulators/.

35. *GSS9000 GNSS Simulator*. Crawley: Spirent, c2023. Dostupné také z: https://www.spirent.com/products/gnss-simulator-gss9000.

36. *What Is Hardware-in-the-Loop?* Austin: NI - Engineer Ambitiously, 2023. Dostupné také z: https://www.ni.com/en/solutions/transportation/hardware-in-the-loop/what-is-hardware-in-the-loop-.html.

37. *RS®SMBV100B vector signal generator*. Columbia: Rohde Schwarz USA, c2023. Dostupné také z: https://www.rohde-schwarz.com/us/products/test-and-measurement/vector-signal-generators/rs-smbv100b-vector-signal-generator_63493-519808.html.

38. *Skydel GSG-7 Advanced GNSS Simulator*. Les Ulis: Safran, [b.r.]. Dostupné také z: https://safran-navigation-timing.com/product/skydel-gsg-7-advanced-gnss-simulator/.

39. *Skydel BroadSim GNSS Simulation Platform*. Les Ulis: Safran, [b.r.]. Dostupné také z: https://safran-navigation-timing.com/product/broadsim-gnss-simulation-platform/.

40. *GSS6300 Multi-GNSS Signal Generator*. Crawley: Spirent, c2023. Dostupné také z: https://www.spirent.com/products/gnss-signal-generator-gss6300.

41. *Srovnání cen elektřiny 2023*. Praha: Ušetřeno.cz, c2010-2023. Dostupné také z: https://www.usetreno.cz/energie-elektrina/cena-za-1-kwh/.

42. *BladeRF Power Consumption Nuand/bladeRF Wiki*. GitHub: Nuand, 2017. Dostupné také z: https://github.com/Nuand/bladeRF/wiki/bladeRF-Power-Consumption.

43. *BladeRF x40 - Nuand*. New York: Nuand, c2023. Dostupné také z: https://www.nuand.com/product/bladerf-x40/.

44. *Software defined radio*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné také z: https://en.wikipedia.org/wiki/Software-defined_radio.

45. *What is a Software Defined Radio? - everything RF*. everything RF: Editorial Team, 2021. Dostupné také z: https://www.everythingrf.com/community/what-is-a-software-defined-radio.

46. *What is a Software Defined Radio? - everything RF*. everything RF: Per Vices, 2021. Dostupné také z: https://www.everythingrf.com/community/what-is-a-software-defined-radio.

47. *Frontend and backend*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné také z: https://en.wikipedia.org/wiki/Frontend_and_backend.

48. *Programovatelné hradlové pole*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné také z: https://cs.wikipedia.org/wiki/Programovateln%5C%C3%5C%A9_hradlov%5C%C3%5C%A9_pole.

49. VE6EY, John. *Introduction to SDR (Software Defined Radio) - Making It Up*. Making It Up, 2015. Dostupné také z: http://play.fallows.ca/wp/radio/software-defined-radio/introduction-to-sdr-software-defined-radio/.

50. *ADALM-PLUTO Evaluation Board — Analog Devices*. Wilmington: Analog Devices, c1995-2023. Dostupné také z: https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html%5C#eb-overview.

51. *HackRF One - Great Scott Gadgets*. Lakewood: Great Scott Gadgets, c2009-2021. Dostupné také z: https://greatscottgadgets.com/hackrf/one/.

52. *LimeSDR Mini - Lime Microsystems*. Guildford: Lime Microsystems, c2020. Dostupné také z: https://limemicro.com/products/boards/limesdr-mini/.

53. *HackRF One*. London: RoboSavvy, c2018. Dostupné také z: https://robosavvy.co.uk/hackrf-one-3.html.

54. *LimeSDR Mini 2.0 — Crowd Supply*. Portland: Crowd Supply, [b.r.]. Dostupné také z: https://www.crowdsupply.com/lime-micro/limesdr-mini-2#products.

55. *RTL-SDR.COM*. RTL-SDR, [b.r.]. Dostupné také z: https://www.rtl-sdr.com/.

56. *SiGe GN3S Sampler v3*. Petach Tikva: Dash, c2009. Dostupné také z: http://www.dash.co.il/index.php?route=product/product&product_id=2636.

57. *SiGe GN3S Sampler v3 - GPS-10981 - SparkFun Electronics*. Niwot: SparkFun Electronics, [b.r.]. Dostupné také z: https://www.sparkfun.com/products/retired/10981.

58. *USRP N210 Software Defined Radio (SDR) - Ettus Research — Ettus Research, a National Instruments Brand — The leader in Software Defined Radio (SDR)*. Austin: Ettus Research™, c2023. Dostupné také z: https://www.ettus.com/all-products/un210-kit/.

59. *Ettus USRP N210: High-bandwidth, High-dynamic Range SDR/Cognitive Radio - Digilent*. Pullman: Digilent, c2023. Dostupné také z: https://digilent.com/shop/ettus-usrp-n210-high-bandwidth-high-dynamic-range-sdr-cognitive-radio/.

60. ŠINDELÁŘ, Radek. *Generátor GNSS signálu*. Praha, 2015. Bakalářská práce. ČVUT v Praze, Fakulta elektrotechnická, Katedra radioelektroniky.

61. *GitHub: Let's build from here · GitHub*. San Francisco: GitHub, c2023. Dostupné také z: https://github.com/.

62. *GitHub - osqzss/gps-sdr-sim: Software-Defined GPS Signal Simulator*. GitHub, c2015-2023. Dostupné také z: https://github.com/osqzss/gps-sdr-sim.

63. *GitHub - gym487/gps-sdr-sim-realtime: Realtime gps-sdr-sim with TCP stream output that can connect to gnuradio or anything else..* GitHub, c2015-2022. Dostupné také z: https://github.com/gym487/gps-sdr-sim-realtime.

64. *Real-time simulace*. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné také z: https://cs.wikipedia.org/wiki/Real-time_simulace.

65. *GitHub - Mictronics/multi-sdr-gps-sim: multi-sdr-gps-sim generates a IQ data stream on-the-fly to simulate a GPS L1 baseband signal using a SDR platform like HackRF or ADLAM-Pluto*. GitHub, c2021. Dostupné také z: https://github.com/Mictronics/multi-sdr-gps-sim.

66. HU, Yaqi. GNSS SDR Signal Generator Implementation Based on USRP N210. *Journal of Physics: Conference Series*. 2019, roč. 1314, č. 1. ISSN 1742-6588. Dostupné z DOI: 10.1088/1742-6596/1314/1/012016.

67. CECCATO, Silvia; FORMAGGIO, Francesco; CAPARRA, Gianluca; LAURENTI, Nicola; TOMASIN, Stefano. Exploiting side-information for resilient GNSS positioning in mobile phones. *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. 2018, s. 1515–1524. ISBN 978-1-5386-1647-5. Dostupné z DOI: 10.1109/PLANS.2018.8373546.

68. WANG, Kang; CHEN, Shuhua; PAN, Aimin. Time and Position Spoofing with Open Source Projects. 2015. Dostupné také z: https://www.blackhat.com/docs/eu-15/materials/eu-15-Kang-Is-Your-Timespace-Safe-Time-And-Position-Spoofing-Opensourcely-wp.pdf.

69. RUSTAMOV, Akmal; GOGOI, Neil; MINETTO, Alex; DOVIS, Fabio. Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices. *2020 International Conference on Localization and GNSS (ICL-GNSS)*. 2020, s. 1–6. ISBN 978-1-7281-6455-7. Dostupné z DOI: 10.1109/ICL-GNSS49876.2020.9115489.

70. RUSTAMOV, Akmal; MINETTO, Alex; DOVIS, Fabio. Improving GNSS Spoofing Awareness in Smartphones via Statistical Processing of Raw Measurements. *IEEE Open Journal of the Communications Society*. 2023, roč. 4, s. 873–891. ISSN 2644-125X. Dostupné z DOI: 10.1109/OJCOMS.2023.3260905.

71. MILJANOVIC, Sanja; ARDIZZON, Francesco; CROSARA, Laura; LAURENTI, Nicola; CANZIAN, Luca; LOVISOTTO, Enrico; MONTINI, Nicola; POZZOBON, Oscar; IOANNIDES, Rigas. Experimental testing and impact analysis of jamming and spoofing attacks on professional GNSS receivers. 2022, s. 1–14. Dostupné také z: https://ceur-ws.org/Vol-3183/paper9.pdf.

72. ARU SAPUTRO, Jabang; EGISTIAN HARTADI, Esa; SYAHRAL, Mohamad. Implementation of GPS Attacks on DJI Phantom 3 Standard Drone as a Security Vulnerability Test. *2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)*. 2020, s. 95–100. ISBN 978-1-7281-8309-1. Dostupné z DOI: 10.1109/ICITAMEE50454.2020.9398386.

73. JANSEN, Kai; PÖPPER, Christina. Advancing attacker models of satellite-based localization systems. *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2017, s. 156–159. ISBN 9781450350846. Dostupné z DOI: 10.1145/3098243.3098270.

74. *GitHub - taroz/GNSS-SDRLIB: An Open Source GNSS Software Defined Radio Library*. GitHub, c2014. Dostupné také z: https://github.com/taroz/GNSS-SDRLIB.

75. *GitHub - danipascual/GNSS-matlab: Matlab codes to generate GNSS PRNs, secondary codes, dataless signals and spectra. Includes real data captures and a theory summary. GPS (L1CA, L2C, L5), Galileo (E1OS, E5), BeiDou-2 (B1I)*. GitHub, c2023. Dostupné také z: https://github.com/danipascual/GNSS-matlab.

76. *HackRF Portapack H2 Mayhem Firmware Flashed + HackRF One 1MHz to 6GHz SDR + 2500mAh Battery + 0.1ppmTCXO—Demo Board—- AliExpress*. Chang-čo: AliExpress - OpenSourceSDR Lab, c2010-2022. Dostupné také z: https://www.aliexpress.com/item/4000247041639.html.

77. *GitHub - eried/portapack-mayhem: Custom firmware for the HackRF+PortaPack H1/H2*. GitHub, c2021. Dostupné také z: https://github.com/eried/portapack-mayhem.

78. *CDDIS*. Washington, DC: NASA, 2023. Dostupné také z: https://cddis.nasa.gov.

79. *GitHub - emlyons2014/gps-sim: Simulate GPS with HackRF*. GitHub, c2015-2018. Dostupné také z: https://github.com/emlyons2014/gps-sim.

80. *SatGen Software*. Buckingham: Racelogic - LabSat, [b.r.]. Dostupné také z: https://www.labsat.co.uk/index.php/en/products/satgen-simulator-software.

81. PAJUREK, René. *Spektrální analyzátory – Co byste o nich měli vědět — Volty*. Frýdek-Místek: Volty.cz, 2020. Dostupné také z: https://www.volty.cz/2020/02/17/spektralni-analyzatory-co-byste-o-nich-meli-vedet/.

82. *What is a Power Spectral Density (PSD)?* Plano: Siemens, 2020. Dostupné také z: https://community.sw.siemens.com/s/article/what-is-a-power-spectral-density-psd.

83. *Navilock Products 62524 Navilock NL-8012U USB 2.0 Multi GNSS Receiver u-blox 8 4.5 m*. Navilock, [b.r.]. Dostupné také z: https://www.navilock.com/produkt/62524/faq.html.

84. *EVK-8/EVK-M8 — u-blox*. Thalwil: u-blox, [b.r.]. Dostupné také z: https://www.u-blox.com/en/product/evk-8evk-m8.

85. *Home — u-blox*. Thalwil: u-blox, [b.r.]. Dostupné také z: https://www.u-blox.com/en.

86. *GNSS milestone achieved as ICAO Council adopts new dual-frequency multi-constellation standards*. Montréal: ICAO, 2023. Dostupné také z: https://www.icao.int/Newsroom/Pages/GNSS-milestone-achieved-as-ICAO-Council-adopts-new-dualfrequency-multiconstellation-standards.aspx.