ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA ELEKTROTECHNICKÁ

KATEDRA APLIKOVANÉ ELEKTRONIKY A TELEKOMUNIKACÍ

DIPLOMOVÁ PRÁCE

Aplikace softwarového rádia pro zpracování GNSS signálů

Bc. Tomáš Flachs **2018**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2017/2018**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tomáš FLACHS**
Osobní číslo:	**E16N0066P**
Studijní program:	**N2612 Elektrotechnika a informatika**
Studijní obor:	**Telekomunikační a multimediální systémy**
Název tématu:	**Aplikace softwarového rádia pro zpracování GNSS signálů**
Zadávající katedra:	**Katedra aplikované elektroniky a telekomunikací**

Zásady pro vypracování:

1. Prostudujte existující projekty na generování GNSS signálů a realizujte generátor vybraného systému pomocí SDR.
2. Proveďte rozbor opatření, používaných v přijímačích GNSS proti podvržení falešných signálů.
3. Otestujte dostupné GNSS přijímače na schopnost odhalit podvržené signály.

Rozsah grafických prací:	**podle doporučení vedoucího**
Rozsah kvalifikační práce:	**40 - 60 stran**
Forma zpracování diplomové práce:	**tištěná/elektronická**

Seznam odborné literatury:

1. **Dostupné manuály k jednotkám USRP, systému GMU Radio a programovacímu jazyku Python.**
2. **Další vhodnou literaturu si student vyhledá v dostupných pramenech podle doporučení vedoucího práce.**

Vedoucí diplomové práce:	**Ing. Richard Linhart, Ph.D.** Katedra aplikované elektroniky a telekomunikací
Datum zadání diplomové práce:	**10. října 2017**
Termín odevzdání diplomové práce:	**24. května 2018**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Dr. Ing. Vjačeslav Georgiev
vedoucí katedry

V Plzni dne 10. října 2017

Abstrakt

S přibývající dostupností a klesající cenou softwarově definovaných vysílačů roste také možnost využití pro útoky na přijímače pro určení polohy ze signálů globálních satelitních navigačních systémů (GNSS). Tato diplomová práce se zabývá problematikou aplikace softwarově definovaného rádia pro zpracování GNSS signálů se zaměřením na zabezpečení GNSS přijímačů. Cílem práce bylo otestovat schopnost vybraných GNSS přijímačů odhalit podvržené signály vygenerované pomocí softwarově definovaného rádia. V této práci je nejprve prostudována technologie satelitních navigačních systémů s důrazem na globální navigační systém GPS a jejich zranitelnost. Dále se tato práce zabývá rozborem opatření, zajišťujících odolnost zařízení proti podvrženým signálům. V další části práce jsou shrnuty možnosti generování GNSS signálů pomocí komerčních a volně dostupných generátorů a následně je realizován generátor GPS signálu. Na základě poznatků o zranitelnosti byly navrženy a realizovány dva testovací postupy simulující středně obtížný útok. Dostupné GPS přijímače byly testovány na schopnost odhalit útok pomocí podvrženého signálu. V závěru práce jsou výsledky diskutovány a přijímače porovnány s ohledem na jejich schopnost detekovat příjem podvrženého signálu.

Klíčová slova

GNSS, GPS, softwarově definované rádio, zranitelnost, podvržení navigačních rádiových signálů

Abstract

With decreasing cost and increasing availability of the Software Definated Radio transmitters increases the possibility of using the attacks to the Global Navigation Satellite System (GNSS) receivers. This master thesis deals with the application of software-defined radio for processing of GNSS signals. Specifically, with focus on secure of GNSS receivers. The aim of this master thesis was to test the ability of selected GNSS receivers to detect fake signals generated by software-defined-radio. In this thesis we first study the technology of satellite navigation systems with focus on American GPS and their vulnerability. Further, this thesis deals with analysis of the measures that ensure the resistance of the device against the fake signals. The next part of thesis summarizes the possibilities of generating GNSS signals using commercial and freely available generators and after that, GPS signal generator is implemented. In the final part of this thesis, based on knowledge of vulnerability, two test procedures simulating medium-heavy attacks are realizated. Varied GPS receivers of varied generations are tested for ability to detect a spoofing attack. At the end of the thesis are the results discussed and the GPS receivers are compared with respect to their ability to detect fake signals.

Key words

GNSS, GPS, SDR, vulnerability, spoofing

Prohlášení

Předkládám tímto k posouzení a obhajobě diplomovou práci, zpracovanou na závěr studia na Fakultě elektrotechnické Západočeské univerzity v Plzni.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této diplomové práce, je legální.

.....

podpis

V Plzni dne 23.5.2018 Tomáš Flachs

Poděkování

Tato práce vznikla za podpory projektu SGS-2015-002.

Obsah

Úvod ... 1
1 Principy družicových navigačních systémů ... 2
1.1 Úhloměrná metoda ... 2
1.2 Dopplerovská metoda ... 2
1.3 Interferenční metoda ... 4
1.3.1 Interferometrické měření na nosné ... 4
1.4 Dálkoměrná metoda ... 4
1.4.1 Algoritmy určení pozice uživatele ... 6
2 Přehled globálních navigačních systémů ... 9
2.1 Globální navigační systém GPS ... 9
2.1.1 Historie systému ... 9
2.1.2 Struktura systému ... 9
2.1.3 Uživatelský segment ... 10
2.1.4 Popis GPS signálu ... 11
2.1.5 Navigační zpráva ... 15
2.1.6 GPS čas ... 17
2.1.7 Souřadnicový systém v GPS ... 17
2.1.8 Určení pozice družice ... 18
2.1.9 Určení pozice uživatele ... 19
2.1.10 Modernizace systému ... 19
2.2 Globální navigační systém GLONASS ... 20
2.2.1 Struktura systému ... 20
2.2.2 Poskytované služby a signály systému ... 20
2.3 Globální navigační systém Galileo ... 21
2.3.1 Struktura systému ... 21

2.3.2 Poskytované služby a signály systému ... 22
2.4 Globální navigační systém BeiDou-2 ... 22
2.4.1 Struktura systému ... 23
2.4.2 Poskytované služby a signály systému ... 23
3 Zranitelnost použití GNSS systémů ... 24
3.1 Cílené rušení GPS signálu ... 24
3.1.1 Charakteristika rušících signálů ... 25
3.1.2 Zaznamenané incidenty ... 26
3.2 Vysílání podvrženého signálu ... 27
3.2.1 Charakteristika spoofing útoků ... 27
3.2.2 Matematický model útoku ... 28
3.2.3 Zaznamenané incidenty ... 30
4 Rozbor opatření proti podvržení falešných signálů ... 32
4.1 Přehled opatření proti podvržení falešných signálů ... 32
4.1.1 Vyhodnocení statistických vlastností signálu ... 32
4.1.2 Sledování parametrů přijímaného signálu ... 33
4.1.3 Asymetrický bezpečnostní mechanismus ... 34
4.1.4 Víceúrovňový bezpečnostní mechanismus ... 35
4.1.5 Zpracování signálu z anténního pole ... 35
4.1.6 Vzájemná korelace vojenských signálů dvou přijímačů ... 36
4.1.7 Vyhodnocení kvality signálu ... 37
4.1.8 Metody RAIM ... 37
4.1.9 Inerciální navigace s implementací RAIM ... 39
4.2 Porovnání opatření proti falešným signálům ... 39
5 Generátory GNSS signálů ... 42
5.1 Komerční ... 42
5.1.1 Hardwarové simulátory ... 42

5.1.2 Softwarové simulátory ... 43
5.2 Nekomerční ... 43
5.3 Zprovoznění GPS-SDR-SIM ... 44
5.3.1 Stažení a kompilace ... 44
5.3.2 BRDC soubor ... 44
5.3.3 Nastavení generování signálu ... 45
5.3.4 Ověření funkčnosti ... 46
6 Návrh metodiky testování GPS přijímačů na schopnost odhalit podvržené signály ... 49
6.1 Postup testování ... 49
6.1.1 Scénář testování středně obtížného útoku ... 50
6.2 Vybavení ... 51
6.2.1 USRP N210 a NI USRP 2920 ... 51
6.2.2 NI USRP-2920 ... 51
6.2.3 PicoSync - II ... 52
6.2.4 Rozvod GPS signálu ... 52
6.3 Realizace středně obtížného útoku ... 53
6.3.1 Schéma zapojení ... 54
6.3.2 Získání platných efemerid dat s použitím GNSS-SDR ... 54
6.3.3 Generování simulovaného signálu s použitím GPS-SDR-SIM ... 56
6.3.4 Implementace signálového zpracování v GNU Radio ... 56
6.3.5 Nastavení výkonových úrovní signálů ... 59
6.4 Testované přijímače ... 59
7 Vyhodnocení testování ... 63
7.1 Metodika vyhodnocení ... 63
7.1.1 Přepočet formátu souřadnic ... 64
7.1.2 Přepočet souřadnic na vzdálenost ... 64
7.2 Výsledky testování scénáře středně obtížného útoku ... 65

7.2.1 AEK-4H 65
7.2.2 EVK-5H 66
7.2.3 EVK-M8N 67
7.2.4 Kouwell KW-9882 68
7.2.5 Garmin nüvi 350 69
7.2.6 Garmin nüvi 775t 70
7.2.7 TomTom Start 25 71
7.2.8 Mini GPS 72
7.2.9 Garmin Dakota 20 73
7.3 Vyhodnocení testování 74
7.3.1 Analýza zdrojů chyb 74
7.3.2 Vyhodnocení testování podvrženým signálem s aktuálními efemeridy 74
7.3.3 Vyhodnocení testování podvrženým signálem s neplatnými efemeridy 75
7.3.4 Celkové shrnutí výsledků 77
Závěr 79
Seznam obrázků 80
Seznam tabulek 82
Seznam literatury a informačních zdrojů 84
Seznam zkratek 91
Seznam symbolů 93
Přílohy i
Příloha A: Obsah navigační zprávy i
Příloha B: Konfigurační soubor GNSS-SDR v
Příloha C: Blokový diagram v GNU Radio vii

Úvod

Tato diplomová práce se zabývá problematikou zranitelnosti globálních družicových navigačních systémů (GNSS), především amerického systému NAVSTAR GPS.

GPS systém v současnosti patří mezi celosvětově nejrozšířenější systém určený ke zjištění polohy, rychlosti a času. Uplatnění nachází v široké oblasti použití, jak v soukromém, tak i ve veřejném sektoru. GPS přijímače můžeme dnes nalézt ve většině mobilních telefonů a v pozemních a námořních dopravních prostředcích. GPS se prosazuje i v letecké dopravě. Určení pozice je taktéž důležitá pro sledování polohy zboží, zvířat a použití v územním plánování a podobně. Na přesném času GPS systému závisí synchronizace telekomunikačních sítí, energetických sítí, finančních a dalších systémů.

To dělá z GPS systému lákavý cíl pro možný útok. Zásadní nevýhodou systému je extrémně slabý navigační signál, obdobně jako u dalších GNSS systémů. Takto slabý signál lze účinně rušit pro velké oblasti rušivým signálem o malém vysílacím výkonu.

Civilní navigační signál, který používají všechny výše uvedené systémy, má veřejně známou strukturu a chybějící zabezpečení proti jeho podvržení. To vede k největšímu riziku, které představuje podvržení signálů, kdy přijímači podvrhneme rozdílné souřadnice a čas oproti skutečnému. S rostoucí dostupností technologie softwarově definovaných rádií umožňujících vysílání libovolného signálu dělá z tohoto typu útoku stále aktuálnější hrozbu.

V poslední době se intenzivně pracuje na vývoji různých opatření proti těmto typům útokům. Především pak na detekci a varování uživatele a zmírnění vlivu těchto útoků.

Cílem této práce je seznámit se s problematikou zranitelnosti GNSS systémů, ověřit možnosti útoků proti přijímači signálů z globálních navigačních systému a udělat rozbor opatření na obranu přijímače. Vybrané možnosti útoků realizovat, porovnat rozdílné přijímače s ohledem na jejich odolnost a schopnost rozpoznat tyto útoky a pro tyto účely prostudovat existující projekty na generování GNSS signálu, a realizovat generátor vybraného systému pomocí softwarově definovaného rádia.

1 Principy družicových navigačních systémů

Pro získání polohy uživatele pomocí zpracování družicových signálů je možné použít několik metod:

- Úhloměrná
- Dopplerovská
- Interferenční
- Dálkoměrná

První tři metody budou popsány zběžně. Dálkoměrná metoda bude rozebrána podrobněji, protože ji využívají všechny moderní GNSS systémy jako například GPS, či Galileo.

1.1 Úhloměrná metoda

Pro určení polohy je nutné změřit elevační úhel dvou družic ve stejném čase nebo elevační úhel jedné družice v různých časech pomocí směrové antény. Geometrickým místem se stejným elevačním úhlem si určíme kužely s vrcholem v místě družic, kde průsečnice obou kuželů s povrchem Země je poloha měřeného bodu [1].

Tato metoda patří mezi první použité pro družicovou navigaci. Pro svoji technickou náročnost na přesné měření elevačního úhlu a malou přesnost se nepoužívá.

1.2 Dopplerovská metoda

V této metodě pro určení polohy měří velikost Dopplerova posuvu. Předpoklad pro určení pozice je družice pohybující se po oběžné dráze vysílající signál o stabilní frekvenci f_v, který přenáší časové značky s konstantním časovým intervalem.

Vlivem Dopplerova jevu je přijímaná frekvence rovna f_p, která je odlišná od původní frekvence f_v. Přijímaný signál je v přijímači dále směšován se signálem z místního oscilátoru o frekvenci f_0, Výstupem je signál s rozdílovou frekvencí $f_0 - f_p$. Čítač počítá počty period N_i tohoto signálu. Pokud by se vzdálenost mezi družicí a uživatelem neměnila, byl by počet period:

$$N_i = T(f_0 - f_p). \tag{1.1}$$

Kde:

T konstantní časový interval mezi odvysílanými časovými značkami $t_{i+1} - t_i$

Při měření pohybující se družice, se vzdálenost mezi dvěma časovými značkami změní z hodnoty d_i na hodnotu d_{i+1}. Časová značka je přijata v okamžiku $t_i + \Delta_i$, kde $\Delta_i = d_i/c$ a odpovídá době pro přenos signálu na vzdálenost d_i mezi družicí a přijímačem. Čítač měřící periody signálu měří změnu fáze signálu mezi dvěma přijatými časovými značkami:

$$N_i = \int_{t_i-\Delta_i}^{t_{i+1}+\Delta_{i+1}} (f_0 - f_p)\, dt = Tf_0 + (d_{i+1} - d_i)\frac{f_0}{c} - Tf_v. \tag{1.2}$$

Dopplerovský posun se projeví i v časové oblasti, proto předpokládáme, že počet period signálu vysílaného mezi dvěma značkami je roven počtu period signálu přijatého mezi dvěma značkami:

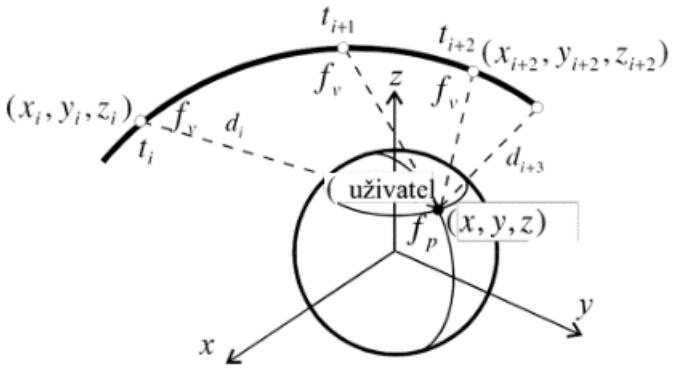
$$f_v(t_{i+1} - t_i) = f_p[t_{i+1} + \Delta_{i+1} - (t_i + \Delta_i)] = f_vT. \tag{1.3}$$

Pokud označíme $F = f_0 - f_p$, a souřadnice družice v čase t_i jako x_i, y_i, a z_i a souřadnice přijímače jako x_u, y_u a z_u, získáme následující rovnici:

$$\begin{aligned} N_i = TF + \frac{f_0}{c}\Big[&\sqrt{(x_{i+1} - x)^2 + (y_{i+1} - y)^2 + (z_{i+1} - z)^2} \\ &- \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}\Big] \end{aligned} \tag{1.4}$$

Pokud provedeme minimálně tři měření N_i, N_{i+1}, N_{i+2} a známe-li souřadnice družice v době měření t_i, t_{i+1}, t_{i+2} získáme soustavu tří rovnic o třech neznámých, kterými jsou souřadnice pozice přijímače x_u, y_u, z_u [5].

Aktuální poloha družice se určí z obdržené navigační zprávy, kterou družice vysílá. Tato navigační zpráva obsahuje aktuální keplerovské parametry orbity družice tak, aby byla chyba určení polohy v okamžicích t_i, t_{i+1}, t_{i+2} co nejmenší.



Obr. 1.1: Doppletova metoda. Převzato z [1].

Dopplerovská metoda se dříve používala jako primární metoda satelitní navigace např. u systému Transit. Nyní slouží spíše jako podpůrná metoda k dálkoměrné metodě určení polohy [1].

1.3 Interferenční metoda

Pro tyto systémy se též používá označení diferenciální. Přijímač má dvě antény na společné základně a jsou od sebe vzdálené na vzdálenost *d*. První anténou měříme zdánlivou vzdálenost D_{1i} k *i*-té družici a zároveň druhá anténa měří zdánlivou vzdálenost D_{2i} ke stejné *i*-té družici. Potom lze určit úhel ϑ_i, který svírá základna se spojnicí střed základny – družice a které pro antény umístěné ve stejné výšce představuje elevační úhel:

$$\vartheta_i = arccos\left(\frac{D_{2i} - D_{1i}}{d}\right) \tag{1.5}$$

Pomocí znalosti elevačního úhlu k družici a polohy družice pak můžeme aplikovat úhloměrnou metodu určení polohy (viz kapitola 2.1.1). Se znalostí tří takto stanovených úhlů a poloh ke třem družicím lze určit orientaci základny v prostoru [1,5].

1.3.1 Interferometrické měření na nosné

Přijímač měří rozdíly fází nosné vlny signálů přijímaných od jedné družice dvěma anténami umístěnými opět na společné základně, kde jsou od sebe vzdálené na vzdálenost *d*. Metoda je totožná jako předchozí, ale měříme jinou veličinu a to fázi. Celý počet *n* period nosné musíme určit jinou metodou, kterou měření inicializujeme. Je možnost změny pracovní frekvence nebo lze použít rozdílovou frekvenci dvou majákových signálů, kterým se zajistí, aby fázové zpoždění mezi signály nepřesáhlo 360°. Úhel, který svírá základna se směrem k družici je dán vztahem:

$$\vartheta_i = arccos\left(\frac{\lambda}{d}\left(n + \frac{\Delta\Phi}{360}\right)\right). \tag{1.6}$$

Měření se vyznačuje značnou přesností než v předchozím případě, protože eliminuje chyby způsobené družicí a šířením signálů a dále na krátkých vlnových délkách odpovídá malé změně vzdáleností velká změna fáze nosné, kterou lze následně přesně změřit [1,5].

1.4 Dálkoměrná metoda

Základní princip určení polohy dálkoměrnou metodou při zanedbání fyzikálních jevů spojených se šířením signálů, pohybem, či pohybem přijímače probíhá měřením vzdálenosti

mezi přijímačem a družicí. Pro měření vzdáleností se využívá měření doby šíření signálu od družice k přijímači:

$$r_k = \tau_{di} c = \left(t_{r,k} - t_{t,k}\right) c. \tag{1.7}$$

Kde:

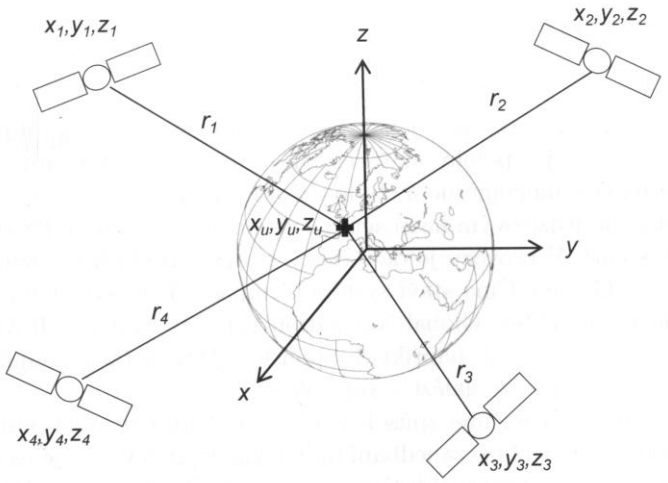
r_k vzdálenost mezi i-tou družicí a přijímačem;

τ_{di} doba šíření signálu na trase d_i;

$t_{r,k}$ čas odvysílání časové značky k-tou družicí;

$t_{t,k}$ doba příjmu časové značky k-té družice;

c rychlost šíření signálu.



Obr. 1.2: Dálkoměrná metoda. Převzato z [3].

Doba šíření signálu, pokud známe kartézské souřadnice i-té družice (x_i, y_i, z_i), můžeme určit polohu uživatele v daném kartézském souřadném systému (x_u, y_u, z_u) jako řešení soustavy tří rovnic pro tři neznámé [1].

$$\sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} = r_k \tag{1.8}$$

Přesně určit dobu τ_{di} je možné pouze za předpokladu přesné synchronizace časové základny družice a uživatelova přijímače navigačních signálů, což je z technického hlediska složité obtížně zajistit. V přijímačích se často používají méně přesné krystalové oscilátory a proto musíme počítat s tím, že časová základna přijímače je posunuta o neznámý časový interval τ_C, který se může měnit v čase. Při započítání neznámého časového posuvu τ_C není výraz

$r_k = \tau_{di} c$ roven vzdálenosti r_k, ale tzv. zdánlivé vzdálenosti ρ_k též nazývané pseudovzdáleností, anglicky pseudorange. Skutečná vzdálenost družice od přijímače se vypočte následovně:

$$r_k = \left(t_{r,k} - t_{t,k} + \tau_c\right)c. \tag{1.9}$$

K rovnici o třech neznámých (1.8), které tvoří souřadnice uživatele přibývá další neznámá τ_C, tedy chyba časové základny přijímače. Pro výpočet neznámých a určení polohy je potřeba zpracovat signál z minimálně čtyř družic [3,5].

$$r_k = \left(t_{r,k} - t_{t,k} + \tau_c\right)c = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} \tag{1.10}$$

1.4.1 Algoritmy určení pozice uživatele

Pro řešení soustavy rovnic (1.10) lze použít jednorázový algoritmus, kdy předchozí poloha uživatele nemá vliv na výpočet aktuální polohy. Taktéž se v družicové navigaci používají predikční algoritmy, které při výpočtu aktuální polohy využívají znalosti předchozí polohy. Mezi tyto algoritmy patří Kalmanův filtr. Tato kapitola čerpá své informace z [3].

Soustavu rovnic je možné řešit buď algebraicky pomocí Bancroftovy metody nebo numericky s použitím aproximace s rozvojem do Taylorovy řady pro vhodně zvolený přibližný odhad řešení. Obvyklé řešení je právě níže popsané numerické řešení.

Pro řešení je potřeba zaprvé upravit rovnici (1.10) do následujícího tvaru:

$$\rho_k = \sqrt{(x_u - x_k)^2 + (y_u - y_k)^2 + (z_u - z_k)^2} - \tau_c c, k = 1, 2, \ldots, \tag{1.11}$$

Kde:

ρ_k změřené pseudovzdálenosti k navigačním družicím.

Pro řešení rovnici linearizujeme v bodě předpokládané polohy uživatele $(\hat{x}_u, \hat{y}_u, \hat{z}_u)$ a časového posunu $\hat{\tau}_c$. Skutečná poloha se bude lišit o $(\Delta x_u, \Delta y_u, \Delta z_u, \Delta\tau_c)$, tedy:

$$\hat{\rho}_k = \sqrt{(\hat{x}_u - x_k)^2 + (\hat{y}_u - y_k)^2 + (\hat{z}_u - z_k)^2} - \hat{\tau}_c c = f(\hat{x}_u, \hat{y}_u, \hat{z}_u, \hat{\tau}_c), \tag{1.12}$$

$$f(x_u, y_u, z_u, \tau_c) = f(\hat{x}_u + \Delta x_u, \hat{y}_u + \Delta y_u, \hat{z}_u + \Delta z_u, \hat{\tau}_c + \Delta\tau_c). \tag{1.13}$$

Závislost lze poté rozvinout do Taylorovy řady:

$$f(x_u, y_u, z_u, \tau_c) = f(\hat{x}_u + \Delta x_u, \hat{y}_u + \Delta y_u, \hat{z}_u + \Delta z_u, \hat{\tau}_c + \Delta\tau_c) =$$
$$= f(\hat{x}_u, \hat{y}_u, \hat{z}_u) + \frac{\partial f(\hat{x}_u, \hat{y}_u, \hat{z}_u)}{\partial \hat{x}_u}\Delta x_u + \frac{\partial f(\hat{x}_u, \hat{y}_u, \hat{z}_u)}{\partial \hat{y}_u}\Delta y_u$$
$$+ \frac{\partial f(\hat{x}_u, \hat{y}_u, \hat{z}_u)}{\partial \hat{z}_u}\Delta z_u + \frac{\partial f(\hat{x}_u, \hat{y}_u, \hat{z}_u)}{\partial \hat{\tau}_c}\Delta\tau_c + \cdots \tag{1.14}$$

Dílčí parciální derivace získáme derivací (1.12).

$$\frac{\partial f(\hat{x}_u, \hat{y}_u, \hat{z}_u, \hat{\tau}_c)}{\partial \hat{x}_u} = \frac{\hat{x}_u - x_k}{\hat{r}_k} = a_{x,k},$$

$$\frac{\partial f(\hat{x}_u, \hat{y}_u, \hat{z}_u, \hat{\tau}_c)}{\partial \hat{y}_u} = \frac{\hat{y}_u - y_k}{\hat{r}_k} = a_{y,k},$$

$$\frac{\partial f(\hat{x}_u, \hat{y}_u, \hat{z}_u, \hat{\tau}_c)}{\partial \hat{z}_u} = \frac{\hat{z}_u - z_k}{\hat{r}_k} = a_{z,k},$$

$$\frac{\partial f(\hat{x}_u, \hat{y}_u, \hat{z}_u, \hat{\tau}_c)}{\partial \hat{\tau}_c} = -c. \tag{1.15}$$

Výsledné koeficienty $a_{x,k}, a_{y,k}, a_{z,k}$, jsou směrové kosiny jednotkového vektoru s počátkem v poloze uživatele, který směruje ke k-té družici. Úpravou rovnice (1.14) získáme:

$$\Delta\rho_k = \rho_k - \hat{\rho}_k = a_{x,k}\Delta x_u + a_{y,k}\Delta y_u + a_{z,k}\Delta z_u + c\Delta\tau_c. \tag{1.16}$$

Soustavu rovnic (1.16) převedeme do maticového zápisu:

$$\mathbf{\Delta\rho} = \mathbf{H}\mathbf{\Delta x}, \tag{1.17}$$

kde:

$$\mathbf{\Delta\rho} = \begin{bmatrix}\Delta\rho_1\\ \Delta\rho_2\\ \vdots\\ \Delta\rho_n\end{bmatrix}, \mathbf{H} = \begin{bmatrix}a_{x,1} & a_{y,1} & a_{z,1} & 1\\ a_{x,2} & a_{y,2} & a_{z,2} & 1\\ \vdots & \vdots & \vdots & \vdots\\ a_{x,n} & a_{y,n} & a_{z,n} & 1\end{bmatrix}, = \begin{bmatrix}\Delta x_u\\ \Delta y_u\\ \Delta z_u\\ -c\Delta\tau_c\end{bmatrix}. \tag{1.18}$$

Δρ je vektor odchylek pseudovzdáleností, **H** je matice směrových kosinů. **Δx** je vektor neznámých, který je cílem řešení. Řešit lze v případě čtyř družic, tedy $n = 4$, přímou metodou:

$$\mathbf{\Delta x} = \mathbf{H^{-1}}\mathbf{\Delta\rho}. \tag{1.19}$$

Pokud je soustava přeurčená, tedy $n > 4$, je možné soustavu řešit metodou nejmenších čtverců nebo váhovou metodou nejmenších čtverců.

Metoda nejmenších čtverců:

$$\mathbf{\Delta x} = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{\Delta\rho}. \tag{1.20}$$

Váhová metoda nejmenších čtverců:

$$\mathbf{\Delta x} = (\mathbf{H}^T\,\mathbf{W}\,\mathbf{H})^{-1}\mathbf{H}^T\,\mathbf{W}\,\mathbf{\Delta\rho}, \tag{1.21}$$

kde matice $\mathbf{W}$ je diagonální matice, jejíž diagonální prvky jsou rovny vahám měření k jednotlivým družicím.

Výše uvedeným postupem lze polohu spočítat, pokud se počítaná poloha uživatele nachází v bezprostřední blízkosti předpokládané polohy $(\hat{x}_u, \hat{y}_u, \hat{z}_u)$. Jinak je potřeba pokračovat iteračním procesem, kdy po výpočtu odchylek $\mathbf{\Delta\rho}$ je přičteme k odhadu předpokládané polohy a tím vytvoříme nový odhad polohy. Celý proces se opakuje, dokud není vektor odchylek dostatečně malý. Počet iterací závisí na přesnosti odhadu předpokládané polohy.

Jako předpokládaná poloha uživatele se používá buď poloha určená v předchozím výpočtu nebo pokud je poloha neznámá se doporučuje nastavit souřadnice na střed Země $(\hat{x}_u, \hat{y}_u, \hat{z}_u, \hat{\tau}_c) = (0,0,0,0)$.

2 Přehled globálních navigačních systémů

2.1 Globální navigační systém GPS

Jedná se globální družicový navigační systém taktéž známý pod názvem NAVSTAR GPS (NAVigation Signal Timing And Ranging Global Positioning System), který provozuje a financuje Ministerstvo obrany Spojených států amerických. V současné době se jedná o jediný systém v plně operačním stavu. Poskytuje svým uživatelům informace o poloze, aktuálním času s vysokou přesností a celosvětové pokrytí.

2.1.1 Historie systému

Projekt družicového navigačního sytému GPS vznikl v roce 1973 v období studené války. GPS je výsledkem sloučení stávajících projektů námořnictva TIMATION, který byl určen pro přesné určení času a Transit s projektem letectva 621B pro určení polohy a projektu SECOR pro geodetické měření armády Spojených států amerických. Projekt byl pojmenován DNSS (Defense Navigation Satellite System) a později byl přejmenován na NAVSTAR Global Position System. Nyní je obecně známo jak GPS [6].

První družice byla vypuštěna v únoru 1978. Do roku 1986 bylo vypuštěno celkem 18 družic. Roku 1993 bylo dosaženo počátečního operačního stavu IOC (Initial Operational Capability) – zajištění minimálního počtu družic pro určení polohy kdekoli na Zemi. V roce 1995 se systém dočkal potřebných 24 družic na oběžné dráze a uvedení do plného operačního stavu FOC (Final Operation Capability).

2. května 2000 provozovatel rozhodl o vypnutí „Selective Availability“ (S/A), což umožnilo civilním uživatelům přijímat plnohodnotný signál bez vnášené chyby pro zhoršení přesnosti [7].

2.1.2 Struktura systému

Systém GPS se skládá ze tří segmentů:

- Kosmický segment,
- řídící segment,
- uživatelský segment.

2.1.2.1 Kosmický segment

Kosmický segment je tvořen konstelací navigačních družic. Původně byl projektován pro 24 družic, ale nyní pracuje s 31 aktivními družicemi. Družice obíhají na střední oběžné dráze v přibližné výšce 20 200 km nad Zemí s dobou oběhu 11 hodin 58 minut. Na přibližně kruhové dráze v šesti orbitálních rovinách o inklinaci 55° jsou rozmístěny pozice pro družice. Konečný počet družic v konstelaci je nyní 32.

Konstelace GPS systému je kombinace starých a nových družic, které se průběžně obměňují. Tab. 2.1 shrnuje současné a budoucí generace GPS družic.

Tab. 2.1: Přehled navigačních družic. Převzato a upraveno z [8]

Blok	Signál						V provozu	Plánovaná životnost	Zavedení
	L1 C/A	L1 P(Y)	L2 P(Y)	L2C	L5	L1C			
IIA	X	X	X				0	7,5 let	1990-1996
IIR	X	X	X				12	7,5 let	1997-2004
IIR-M	X	X	X	X			7	7,5 let	2005-2009
IIF	X	X	X	X	X		12	12 let	2010-2016
III/IIIF	X	X	x	X	X	X	V přípravě	12 let	2018-

2.1.2.2 Řídící segment

Řídící segment se skládá z celosvětové sítě pozemních stanic, které monitorují stav vesmírného segmentu a provádí jeho údržbu. Hlavním úkolem řídícího segmentu je přesné sledování dráhy družic a atomových hodin monitorovacími stanicemi. Dále zajišťuje generování obsahu navigační zprávy, generování systémového času, synchronizace na systémový čas, monitorování správné činnosti družice, údržbu konstelace, řízení systémů a nahrávání aktuální navigační zprávy [3].

Řídící segment dělíme:

- řídící středisko (Master Control Station MSC)
- 3 nahrávací stanice (Ground Antenna)
- 18 monitorujících stanic (Monitor Stations)

2.1.3 Uživatelský segment

Uživatelský segment se skládá ze samotných přijímačů, které umožňují zpracovávat GPS signál.

Přijímače se obvykle skládají z antény s nízkošumovým zesilovačem, procesoru přijímače a zdrojem přesného hodinového signálu. U přijímačů se často uvádí počet kanálů. Počet kanálů určuje maximální počet zpracovávaných družic [4].

Uživatele lze dělit podle využívané služby GPS:

- **Standardní služba navigace SPS (Standard Position Service)** je určena bezplatně všem uživatelům, tj. neautorizovaným uživatelům, kteří disponují GPS přijímačem. Šíří se C/A kódem na frekvenci L1.
- **Přesná služba navigace PPS (Precision Position Service)** je určena pro armádu spojených států a některých dalších spojeneckých armád, tj. autorizovaní uživatelé. Šíří se P(Y) kódem na frekvencích L1 a L2. Od Standardní služby se liší zaručenou vyšší přesností.
- **Služba kritická z hlediska bezpečnosti SoL (Safety of Life Service)** je služba určená pro kritické aplikace jako je přesné přiblížení letadel pro přistání. Je vysílán na frekvenci L5, která je mezinárodně chráněna pro leteckou navigaci. Signál je vysílán z nově nasazených družic při obnově konstelace systému.

2.1.4 Popis GPS signálu

Každá družice vysílá několik typů navigačních signálů podle poskytované služby. Frekvence navigačních signálů jsou:

Tab. 2.2: Přehled frekvencí signálů GPS

Pásmo	Frekvence [MHz]	Použití
L1	1575,42	služba SPS, služba PPS
L2	1227,6	služba PPS
L3	1381,05	detekce jaderných testů
L4	1841,4	Měření ionosférické interference
L5	1176,46	Služba kritická z hlediska bezpečnosti

Frekvence signálů jsou odvozené ze základní frekvence atomového standardu 10,32 MHz. Signály určené pro navigaci L1 a L2 lze popsat následujícím vztahem:

$$s(t) = C(t)D(t)\sin(2\pi L_1 t) + P(t)D(t) + P(t)D(t)\cos(2\pi L_2 t). \qquad (2.1)$$

Kde:

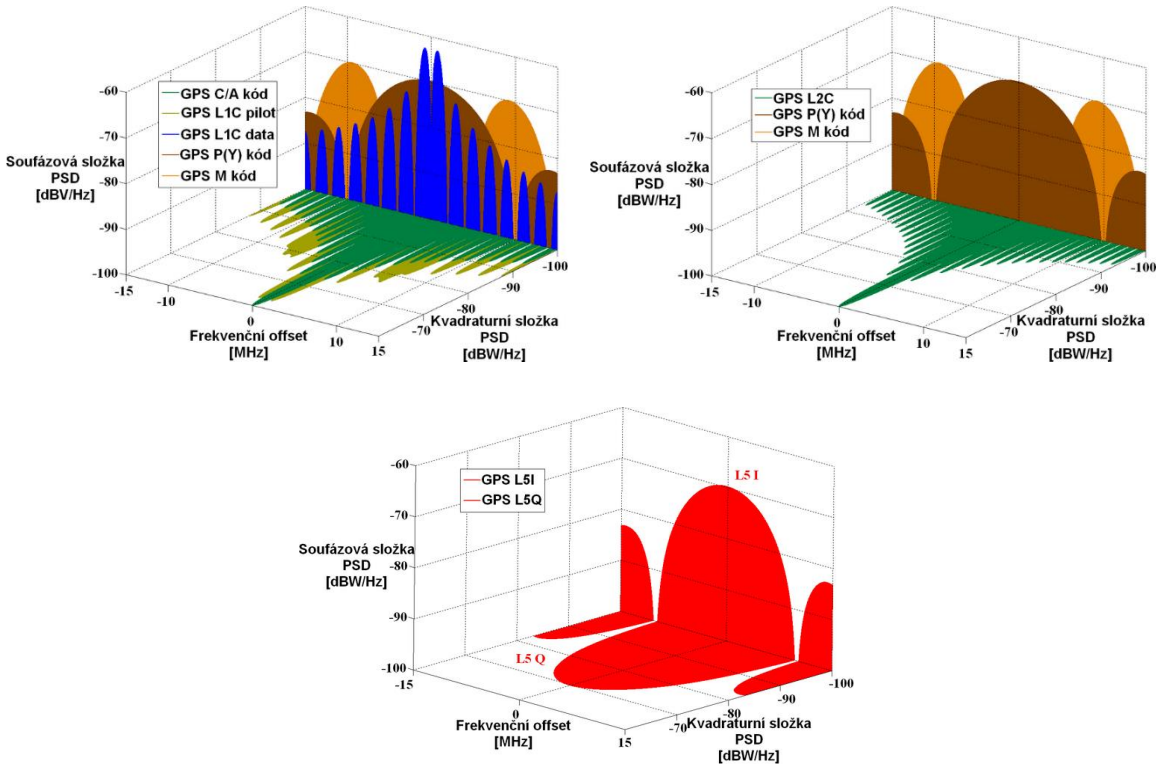
C(t) civilní C/A kód,

P(t) autorizovaný P(Y) kód,

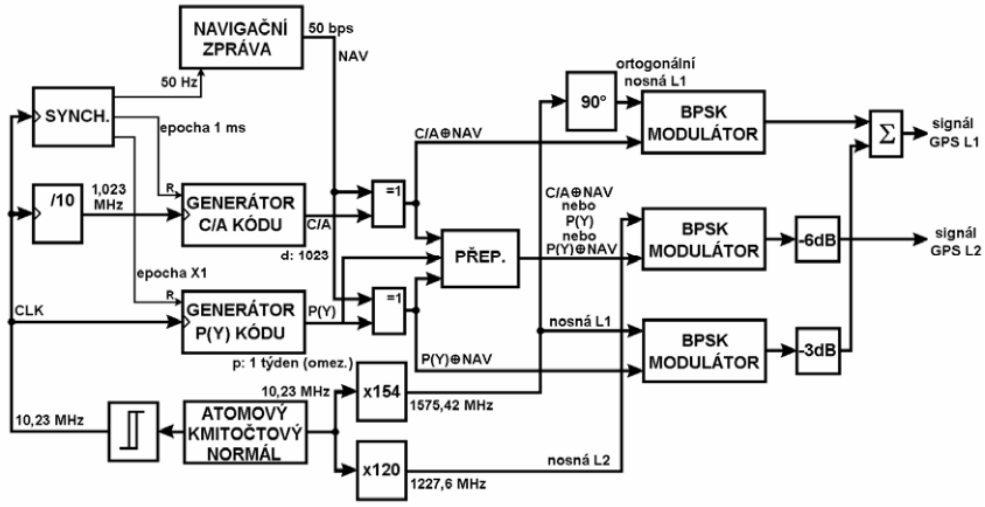
D(t) navigační zpráva družice.

Přenos navigační zprávy D(t) je zajištěn BPSK modulací. Kódy C(t) a P(t) umožňují měření vzdáleností mezi uživatelem a družicí a vzájemné oddělení signálů jednotlivých družic.

Signály C/A P(Y) používají stejné pásmo L1 a stejnou techniku rozprostření spektra, jejichž oddělení je zajištěno ortogonálním modulováním signálů na nosnou. Modulační signály C/A P(Y) jsou navzájem posunuty o 90°, kompozitní signál představuje QPSK. I-složka je modulována C/A modulačním signálem Q-složka je modulována signálem P(Y). Schéma způsobu generování C/A P(Y) signálu v pásmech L1 a L2 je na obrázku Obr. 2.2 [1].



Obr. 2.1: Frekvenční spektrum GPS signálů. Převzato ä upraveno z [9].



Obr. 2.2: Blokové schéma generování signálu v pásmech L1 a L2. Převzato z [1].

2.1.4.1 C/A kód

Dálkoměrný C/A (Coarse/Acquisition) kód je určen pro standardní službu navigace SPS. Slouží k určení pseudovzdálenosti mezi uživatelem a družicí, zajištění kódového multiplexu CDMA pro jednotlivé družice a jejich jednoznačnou identifikaci.

V systému GPS se pseudovzdálenost určí korelací přijímaného signálu s replikou pseudonáhodného PRN (Pseudo Random Noise) kódu příslušné družice. Pro C/A kód se využívá předností Goldovy posloupnosti. Ta se vyznačuje ostrým maximem autokorelační funkce a velmi malou hodnotou vzájemné korelační funkce mezi jednotlivými C/A kódy ostatních družic. To zajišťuje vzájemné oddělení signálů z různých družic.

Goldovy posloupnosti jsou v C/A získány jako binární modulo součet dvou nezávislých posloupností G1 a G2 o stejné délce, kde pseudonáhodná posloupnost G2 je pro daný C/A kód zpožděna o *k* bitů. Každá dílčí posloupnost se skládá z posuvného registru o velikosti *R*. Pro C/A kód je *R=10*, délka kódu je:

$$L_{G1} = L_{G2} = 2^R - 1 = 2^{10} - 1 = 1023. \tag{2.2}$$

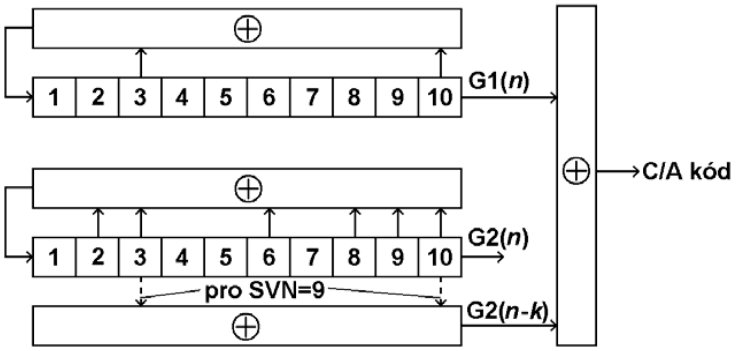
Tvar generujícího polynomu pseudonáhodné posloupnosti G1 je:

$$G1 = 1 + X^3 + X^{10}, \tag{2.3}$$

pro pseudonáhodnou posloupnost G2 je tvar generujícího polynomu:

$$G2 = 1 + X^2 + X^3 + X^6 + X^8 + X^9 + X^{10}. \tag{2.4}$$

Zpoždění posloupnosti G2 o *k* bitů je možné realizovat binárním modulo součtem vhodných buněk posuvného registru pro G2. Schéma generátoru C/A kódů pro GPS družice je znázorněn na Obr. 2.3. V tabulce Tab. 2.3 jsou pro jednotlivé družice identifikované svým SVN (Space vehicle Number) číslem přiřazené příslušné zpoždění G2 oproti G1 a k nim odpovídající buňky posuvného registru G2 pro modulo součet. Iniciace posloupností G1 a G2, tedy počátek kódu, který je časově synchronní s počátkem bitu navigační zprávy je roven vektorům o deseti jedničkách [1].



Obr. 2.3: Generování C/A kódu pro GPS družice. Převzato a upraveno z [5].

Tab. 2.3: Generování Goldovy posloupnosti. Převzato z [5]

SVN	Zpoždění k [bit]	Buňky G2	SVN	Zpoždění k [bit]	Buňky G2	SVN	Zpoždění k [bit]	Buňky G2
1	5	2 ⊕ 6	14	256	7 ⊕ 8	27	515	7 ⊕ 9
2	6	3 ⊕ 7	15	257	8 ⊕ 9	28	516	8 ⊕ 10
3	7	4 ⊕ 8	16	258	9 ⊕ 10	29	859	1 ⊕ 6
4	8	5 ⊕ 9	17	467	1 ⊕ 4	30	860	2 ⊕ 7
5	17	1 ⊕ 9	18	470	2 ⊕ 5	31	861	3 ⊕ 8
6	18	2 ⊕ 10	19	471	3 ⊕ 6	32	862	4 ⊕ 9
7	139	1 ⊕ 8	20	472	4 ⊕ 7	R-33	863	5 ⊕ 10
8	140	2 ⊕ 9	21	473	5 ⊕ 8	R-34	950	4 ⊕ 10
9	141	3 ⊕ 10	22	474	6 ⊕ 9	R-35	947	1 ⊕ 7
10	251	2 ⊕ 3	23	509	1 ⊕ 3	R-36	948	2 ⊕ 8
11	252	3 ⊕ 4	24	512	4 ⊕ 6	R-37	950	4 ⊕ 10
12	254	5 ⊕ 6	25	513	5 ⊕ 7			
13	255	6 ⊕ 7	26	514	6 ⊕ 8			

Kódy označené písmenem R se nepoužívají pro použití družicemi, ale jsou určeny pro specializované pozemní aplikace [10].

2.1.4.2 P(Y) kód

Dálkoměrný P(Y) (Precision, česky přesný) kód je určen pro přesnou službu navigace PPS určenou pro licencované uživatele.

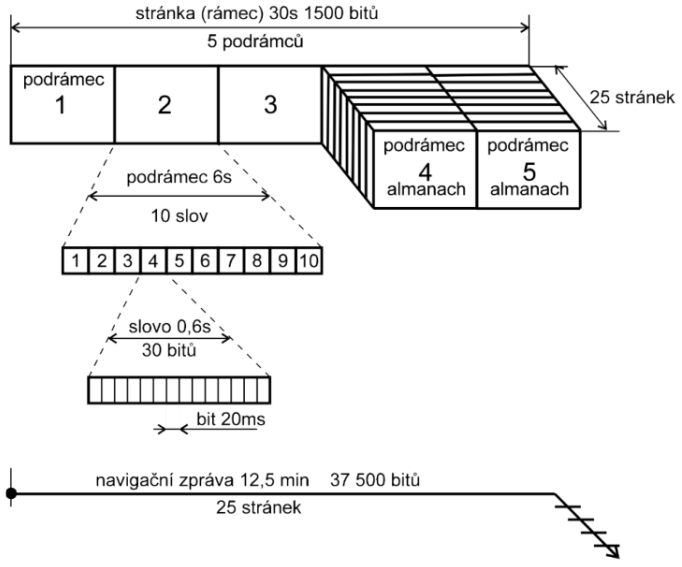
P kód je pseudonáhodná posloupnost maximální délky s celkovou periodou přibližně 266 dní, kdy obdobně jako u C/A kódu má každá družice svůj P kód. V praxi se používá sedmidenní část. P kód umožňuje měření pseudovzdálenosti přesněji než C/A kód z důvodů použití rychlejšího a delšího kódu, čímž dochází k většímu frekvenčnímu rozprostření signálu a zvýšení přesnosti měření. Přístup k P kódu je omezen zavedením šifrování pomocí Y kódu. Tento režim se označuje jako Anti-Spoofing (A-S) a jeho zavedením se též ověřuje pravost přijímaného signálu z družice.

Podrobný popis generování P kódu lze najít v [11].

2.1.5 Navigační zpráva

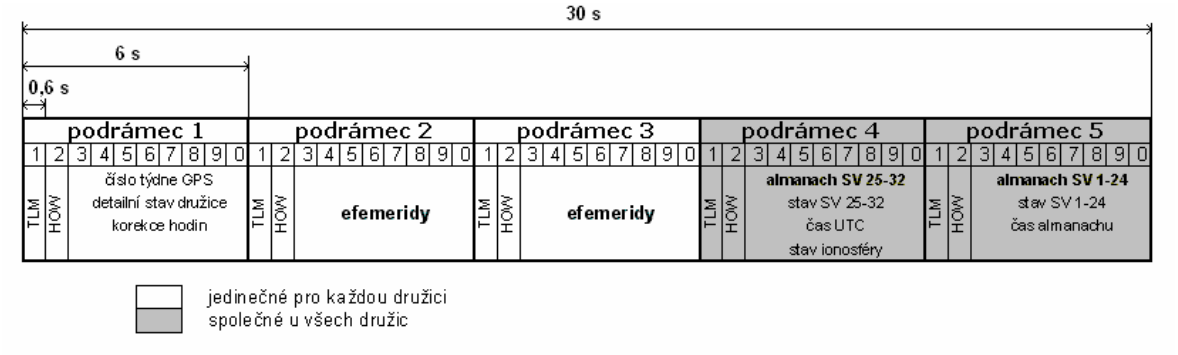
Jak je uvedeno v kapitole 2.1.4, kódy C/A P(Y) jsou modulovány daty s rychlostí 50 bit/s. Tato data obsahují navigační zprávu, která obsahuje informace nutné k určení pozice družice.

Navigační zpráva je rozdělena do 25 rámců, kde každý rámec se skládá z 5 podrámců. Podrámce se skládají z 10 slov o délce 30 bitů, z nichž je 24 datových a 6 bitů slouží k zabezpečení přenosu pomocí Hammingova kódu. Struktura navigační zprávy je na Obr. 2.4. Při bitové rychlosti 50 bit/s trvá odeslání rámce 30 sekund a odeslání celé navigační zprávy 12,5 minut.



Obr. 2.4: Struktura navigační zprávy. Převzato z [5].

První dvě slova podrámce jsou stejná pro každý podrámec. První slovo obsahuje telemetrická data (TLM). Prvních osm bitů je synchronizační slovo 1001011, kterým se určuje začátek podrámce. Dalších 14 bitů je vyhrazeno pro diagnostickou zprávu od řídícího segmentu. Předávací (HOW) slovo obsahuje na prvních 17 bitech informaci o pořadí podrámce v aktuálním týdnu GPS (viz kapitola 2.1.6). Taktéž obsahuje příznakové bity, první indikuje že Anti-Spoofing byl aktivován (viz kapitola 2.1.4.2). Druhý příznakový bit v případě nenulové hodnoty varuje, že přesnost signálu družice je nízká a jeho zpracování je na uživatelovo vlastní nebezpečí [11]. HOW slovo také obsahuje na bitech 20 až 22 informací o číslu podrámce.



Obr. 2.5: Obecný popis navigační zprávy GPS. Převzato z [1].

První podrámec obsahuje informace o aktuálním číslu GPS týdne, detailní informace o stavu družice a korekce atomového času. Přenášené parametry jsou v příloze A v tabulce A.1. Výpočet odchylky časové základny družice podle standartního algoritmu lze nalézt v [5] nebo v [11].

Druhý a třetí podrámec obsahují parametry efemerid, tedy přesných parametrů dráhy dané družice, pomocí kterých je možné vypočítat její polohu i údaje pro korekce. Popis přenášených parametrů je v příloze A v tabulce A.2.

Čtvrtý a pátý podrámec obsahují parametry ionosférického modelu a almanach, tedy přibližné parametry dráhy všech družic nutné k určení jejich přibližné polohy. Konkrétně čtvrtý podrámec obsahuje:

- Strany 2 až 10 obsahují almanach pro družice 25 až 32.
- Strana 17 obsahuje speciální zprávy od řídícího segmentu.
- Strana 18 zahrnuje ionosférické korekce.
- Strana 25 obsahuje příznakové bity o stavu jednotlivých družic.

Pátý podrámec zahrnuje:

- Na stranách 1 až 24 obsahuje almanach pro družice 1 až 24;
- Strana 25 obsahuje příznakové bity o stavu družic, referenční čas a referenční číslo týdne almanachu.

Popis přenášených parametrů almanachu je v příloze A v tabulce A.3 [1,3].

2.1.6 GPS čas

GPS si generuje svůj vlastní, kontinuálně běžící, čas GPST. Je řízen atomovými hodinami řídícího segmentu a atomovými hodinami na palubě družic.

Začátek GPST času nastal o půlnoci mezi 5. a 6. lednem 1980. GPS používá týden jako největší časovou jednotku, která se počítá od počátku GPST času. Čas se skládá ze dvou hodnot, pořadové číslo GPS týdne a počet sekund od počátku týdne. Navigační zpráva, ve které se pořadové číslo GPS týdne vysílá (viz. 2.1.5), má pro tento parametr omezenou délku, takže maximální počet pořadového čísla GPS týdne 1023. Při dosažení nastává tzv. rollover a počítá se opět od nuly. První rollover nastal 22. srpna 1999. Příští nastane v dubnu roku 2019.

Čas generovaný atomovými hodinami na palubě navigačních družic je monitorován a korigován řídícím segmentem, aby rozdíl nebyl větší než 1 μs [13] Zpráva zahrnuje koeficienty korekce mezi GPST časem vysílaný družicí a skutečným GPST časem (viz. kapitola 2.1.5).

2.1.7 Souřadnicový systém v GPS

Pro určení polohy je potřeba v prvním případě definovat příslušný referenční souřadnicový systém. Z popisu struktury systému GPS (viz 2.1.2) vyplývá, že se skládá se dvou pozemních segmentů a jednoho segmentu umístěného ve vesmíru. Z toho vychází i požadavek na použití dvou odlišných referenčních souřadnicových systémů:

- Souřadnicový systém pevně spjatý se zemským povrchem s počátkem ve středu země ECEF (Earth centered, Earth fixed),
- Inerciální souřadnicový systém s počátkem ve středu země ECI (Earth-centered inertial), který je fixován k jarnímu bodu.

GPS systém používá pro určení polohy uživatele ECEF geodetický souřadnicový systém, který používá pro aproximaci zemského povrchu referenční elipsoid WGS-84

s uvedené v tabulce Tab. 2.4. Poloha je dána trojicí kartézských souřadnic (x, y, z) (zkráceně XYZ, kde osa x prochází nultým poledníkem a osa z je osa rotace Země nebo může být dána použitím geodetických souřadnic: zeměpisná šířka, zeměpisná délka a výška (zkráceně LLA).

Tab. 2.4: Parametry WGS-84 souřadnicového systému. Převzato a upraveno z [3]

Parametr	Označení	Hodnota	Veličina
Délka hlavní poloosy	a	6 378 137,0	m
Délka vedlejší poloosy	b	6 356 752,314 2	m
Reciproká hodnota zpoždění	$1/f$	298,257 223 563	-
Kvadrát excentricity	e^2	$8{,}181\ 919\ 084\ 2622 \cdot 10^{-2}$	-
Úhlová rychlost zemské rotace	ω_E	$7\ 292\ 115{,}0 \cdot 10^{-11}$	rad/s
Geocentrická gravitační konstanta	GM	$3{,}986\ 004\ 42 \cdot 10^{14}$	m^3/s^2
Rychlost světla ve vakuu	c	$2{,}997\ 924\ 58 \cdot 10^{8}$	m/s

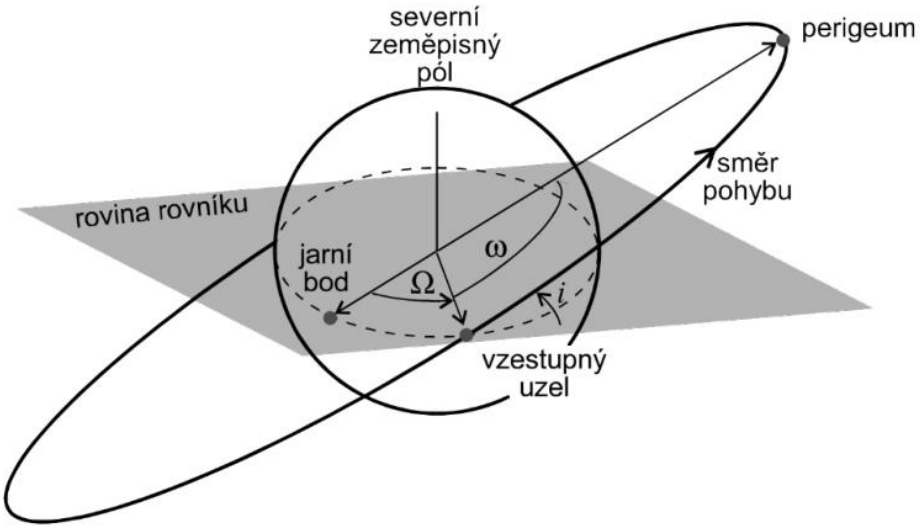
GPS systém používá inerciální souřadnicový systém ECI pro zjednodušení výpočtu určení pozice družice na dráze, protože v tomto systému platí Newtonovy pohybové zákony a je zde definována rychlost světla a tím i skupinové zpoždění šíření signálu [3]. Transformační vztahy pro převod LLA souřadnic na XYZ souřadnice a transformační vztahy pro převod ECI na ECEF lze nalézt např. v [3].

2.1.8 Určení pozice družice

Pro určení pozice družice se musí vypočítat její eliptická oběžná dráha, viz Obr. 2.6, kde v jednom z ohnisek je těžiště Země. Pro charakterizaci dráhy družice se používají keplerovské parametry. Keplerovské parametry popisují tvar dráhy družice v oběžné rovině a orientaci oběžné roviny vůči Zemi. Tyto parametry jsou:

- délka hlavní poloosy oběžné dráhy a,
- excentricita oběžné dráhy e,
- čas průchodu perigeem t_p,
- inklinace oběžné dráhy družice i,
- délka vzestupného uzlu – rektascenze Ω,
- argument perigea ω.

Keplerovské parametry jsou vysílány družicemi v navigační zprávě, která byla podrobně popsána v kapitole 2.1.5. Kromě přesných keplerovských parametrů v efemeridách dané družice a přibližných parametrů celého systému, obsahuje navigační zpráva také harmonické korekce dráhy družice, které korigují výpočet pozice dráhy družice o vlivy dalších hmotných těles sluneční soustavy, pohybovým odporem zbytků atmosféry a nehomogenity Země [1].



Obr. 2.6: Eliptická dráha družice. Převzato z [3].

Standardní algoritmus výpočtu pozice družice je uveden například v [11]. Stejný algoritmus používá i evropský systém Galileo. Rozdíly jsou v některých konstantách, v čase a v systému souřadnic, protože Galileo používá systém GTRF (Galileo Terrestrial Reference Frame) místo WGS84 [3].

2.1.9 Určení pozice uživatele

Systém GPS, stejně jako další globální navigační systémy používají pro určení pozice uživatele dálkoměrnou polohu popsanou v kapitole 1.4. Standartní algoritmy pro výpočty pozice uživatele jsou popsány v podkapitole 1.4.1.

2.1.10 Modernizace systému

Práci na modernizaci GPS systému probíhá na několika úrovních:

- modernizace vesmírného segmentu,
- modernizace řídícího segmentu,
- zavádění nových civilních signálů a modernizované civilní navigační zprávy.

Kosmický segment je průběžně doplňován družicemi z nových bloků z důvodů omezené životnosti družic. Nový blok družic používá vylepšené technologie a rozšiřují systém o nové navigační signály. Přehled jednotlivých bloků navigačních družic a vysílaných signálů je v tabulce Tab. 2.1.

V případě modernizace řídícího segmentu je od roku 2008 implementován Next Generation Operational Control System (OCX). OCX bude řídit všechny modernizované i starší navigační družice, spravovat veškeré civilní a vojenské navigační signály a bude zajišťovat vylepšenou bezpečnost a odolnost systému.

Modernizace se týká také vysílaných navigačních signálů. Celkem se plánuje rozšířit systém o tři civilní navigační signály: L2C, L5 a L1C a vojenské navigační signály M v pásmu L1 a L2. Součástí modernizace je také zavedení nového formátu navigační zprávy pro nové civilní navigační signály.

Podrobné informace o modernizaci systému GPS jsou k dispozici na [14].

2.2 Globální navigační systém GLONASS

GLONASS (Global'naya Navigatsionnaya Sputnikovaya Sistema) je globální navigační systém provozovaný armádou Ruské federace. Vývoj systému začal v roce 1970 v tehdejším Sovětském svazu a navazuje na navigační systémy Tsikada a Parus používající dopplerovskou metodu. První testovací družice byla vypuštěna v roce 1982. Od roku 2011 se společně s americkým GPS jedná o systém v plném celosvětovém operačním stavu.

2.2.1 Struktura systému

Strukturu systému lze rozdělit na tři segmenty.

- **Kosmický segment –** Konstelace systému je navržena pro 24 družic, které se pohybují ve výšce 19100 km na třech drahách o inklinaci 64,8°. V současné době se ve vesmírném segmentu nachází 25 navigačních družic, z nich 23 je v operačním stavu [15].
- **Řídící segment**
- **Uživatelský segment**

2.2.2 Poskytované služby a signály systému

Obdobně jako u GPS, uživatele můžeme rozdělit dle používané služby. Armádní a státní sektor využívá službu se zaručenou vyšší přesností HP (High Positioning), civilní uživatelé používají službu SP (Standard Positioning).

Aktuálně využívá systém GLONASS dvě frekvenční pásma, L1 a L2. Na rozdíl od systémů GPS a Galileo používá k rozlišení signálu z jednotlivých družic kmitočtově dělení FDMA místo kódového CDMA. Nosný kmitočet pro jednotlivé kanály lze spočítat:

$$f_{k,L1} = 1602{,}0 + 0{,}5625\ k\ [MHz],$$

$$f_{k,L2} = 1201{,}0 + 0{,}4375\ k\ [MHz]. \tag{2.5}$$

Rozsah kanálů je k = -7, …, +6. Na obou kmitočtech se vysílá civilní i vojenský navigační signál.

Použití FDMA patří mezi hlavní nedostatek systému GLONASS. Způsobuje interference mezi kanály, širší zabrané kmitočtové pásmo a složitější přijímače, než pro systémy používají CDMA. Tyto nedostatky se řeší v probíhající modernizaci, kdy budou přidány signály:

- L3 (1197–1217 MHz) – frekvenční dělení, šíření vojenského a civilního signálu,
- L1CR (1575,42 MHz) – kódové dělení, zajištěná interoperabilita s dalšími GNSS službami,
- L5 (1176,45 MHz) – Kódové dělení, signál typu Safety of life se zajištěnou interoperabilitou s dalšími GNSS systémy.

Podrobnosti o signálech, použitých kódech a formátu navigačních zpráv lze nalézt v [17].

2.3 Globální navigační systém Galileo

Galileo je společný projekt členských států Evropské unie, jehož cílem je vytvořit globální navigační systém v plném civilním řízení. Řízení zajišťuje Evropská kosmická agentura (ESA). V roce 1999 byl představen projekt Galileo pro zajištění nezávislosti na americkém systému GPS. V roce 2011 byla vynesena první navigační družice. Od prosince 2016 je systém v počátečním operačním stavu. Plný operační stav se předpokládá v roce 2020.

2.3.1 Struktura systému

Obdobně jako u dalších navigačních systémů lze strukturu systému rozdělit do segmentů.

- **Kosmický segment –** Konstelace systému je navržena pro 30 družic, které se pohybují ve výšce 23 222 km na třech drahách o inklinaci 56°. V současné době je v operačním stavu 14 navigačních družic [16]. 2.3 Navigační systém
- **Řídící segment**
- **Uživatelský segment**

2.3.2 Poskytované služby a signály systému

Systém Galileo bude nabízet v plném celosvětovém operačním stavu čtyři typy služeb:

- **Základní služba OS (Open Service) –** Bezplatná služba určena veřejnosti.
- **Služba kritická z hlediska bezpečnosti SoL (Safety of Life Service)** – Základní služba rozšířená o varování uživatele v případě, že není garantována přesnost nebo integrita systému.
- **Komerční služba CS (Commercial Service) –** Zpoplatněná služba pro profesionální aplikace, s přidanou hodnotou v oblasti přesnosti, spolehlivosti a zabezpečení signálu.
- **Veřejně regulovaná služba PRS (Public Regulated Service) –** Služba určená pro vládní využití členských států, především pro bezpečností složky. Služba disponuje vyšší přesností a spolehlivostí a mechanismy proti rušení a podvržení signálu.
- **Vyhledávací a záchranná služba SAR (Search and Rescue service) –** Služba nouzové lokalizace v rámci mezinárodního pátracího a záchranného systému COSPAS-SARSAT. Umožněna bude taktéž obousměrná komunikace.

Systém Galileo bude používat celkem deset navigačních signálů šířených na čtyřech nosných kmitočtech, popsané v tabulce Tab. 2.5.

Tab. 2.5: Přehled používaných kmitočtů systému Galileo

Označení	Kmitočet [MHz]	Služby
E1	1575,420	OS, SoL, PRS
E6	1278,750	CS, PRS
E5a	1176,450	OS, SoL
E5b	1207,140	OS, SoL

Signály systému Galileo jsou velmi komplexní, používají speciální typy modulace z důvodu omezení interferencí s dalšími družicovými navigačními systémy, především GPS. Příklad použité modulace je BOC (1,1). Podrobnosti o signálech, použitých kódech a formátu navigačních zpráv lze nalézt v [18].

2.4 Globální navigační systém BeiDou-2

Projekt BeiDou je realizován Čínskou lidovou republikou. Jeho cílem je realizovat globální navigační systém, nezávislý na americkém systému GPS. Čína provozuje od roku 2003 regionální navigační systém BeiDou, používající geostacionární družice. V roce 2006 se rozhodlo o rozšíření konstelace o navigační družice na střední oběžné dráze (MEO) a poskytnutím celosvětového pokrytí v roce 2020. Druhá verze označení nese název BeiDou–2, alternativně Compass.

2.4.1 Struktura systému

Systém Compass se skládá ze tří segmentů:

- **Kosmický segment** – Konstelace systémů počítá do roku 2020 s 35 družicemi. Pět navigačních družic na geostacionární dráze, 27 navigačních družic na třech středních oběžných drahách o inklinaci 55° obíhajících ve výšce 21 528 km a tři navigační družice obíhající na šikmých geosynchronních drahách (IGSO). V současné době je v operačním stavu celkem 15 navigačních družic [19].
- **Řídící segment**
- **Uživatelský segment**

2.4.2 Poskytované služby a signály systému

Systém po svém dokončení bude poskytovat dva typy globálních služeb a dva typy regionálních služeb.

Mezi globální služby patří bezplatná služba pro běžné uživatele OS (Open Service), která bude nabízet přesnost přibližně deset metrů. Druhá, autorizovaná, globální služba AS (Authorized Service) je určena pro vojenské služby. Bude přesnější než bezplatná služba a bude poskytovat uživateli informaci o stavu systému a možnost použít komunikačních služeb. Regionální služby budou sloužit k šíření ionosférických korekcí a přenosu krátkých zpráv [20].

Systém Compass využívá pro šíření navigačních signálů jednotlivých služeb celkem tři nosné kmitočty uvedené v tabulce Tab. 2.6.

Tab. 2.6: Přehled používaných kmitočtů systému BeiDou - 2

Označení	Kmitočet [MHz]	Služby
B1	1575,42	OS, AS
B2	1191,79	OS
B3	1268,52	AS

Výhodou bude vzájemná interoperabilita s dalšími globálními navigačními systémy používající stejné pásmo jako signál B1. Podrobnosti o signálech, použitých kódech a formátu navigačních zpráv lze nalézt v [21].

3 Zranitelnost použití GNSS systémů

Signál GNSS systémů, především GPS, se používá jako přesný zdroj hodin k synchronizaci v řadě aplikací: finanční systémy a burzy, komunikační sítě, energetické přenosové sítě atd. K těmto účelům slouží standardní služba navigace GPS, která svým navigačním signálem nabízí dostatečnou přesnost hodin a celosvětovou dostupnost.

Navzdory svým výhodám disponuje navigační signál též vlastnostmi, které mohou být použity k útoku na systémy.

- Slabý signál z navigačních družic, který lze snadno zarušit – **Jamming**.
- Chybějící zabezpečení navigačního signálu proti podvržení falešného signálu přijímači – **Spoofing**.

Těmito druhy útoků na přijímače lze znemožnit příjem signálu nebo pozměnit přijímané informace. To může vést v případě úspěšného útoku například na burzovní systémy k velkým finančním ztrátám nebo v případě použití například na autonomních dopravních prostředcích i ke ztrátám na životech [22].

V roce 2016 vydala Resilient Navigation and Timing Foundation publikaci, ve které analyzovala a hodnotila možné hrozby v GPS. Mezi největší hrozby podle [23] patří náhodné zarušení signálu v malém rozsahu a zarušení velkého území buď soupeřícími vojsky nebo teroristickými skupinami.

3.1 Cílené rušení GPS signálu

Problém GPS signálu je, že je velmi slabý. Technické specifikace systému GPS udávají, že minimální přijímaný výkon C/A kódu vysílaného v pásmu L1 je na povrchu Země -160 dBW a pro P(Y) kód v pásmu L2 je přijímaný výkon -161,5 dBW [10], což je pod úrovní šumu pozadí. Takto slabý signál lze velmi snadno rušit dalším, výkonnějším zdrojem rádiového signálu a tím znemožnit zpracování signálu přijímačem. Cílené rušení navigačního signálů se v anglické literatuře nazývá Jamming a zařízení určené k vysílání jamming signálů se nazývá Jammer.

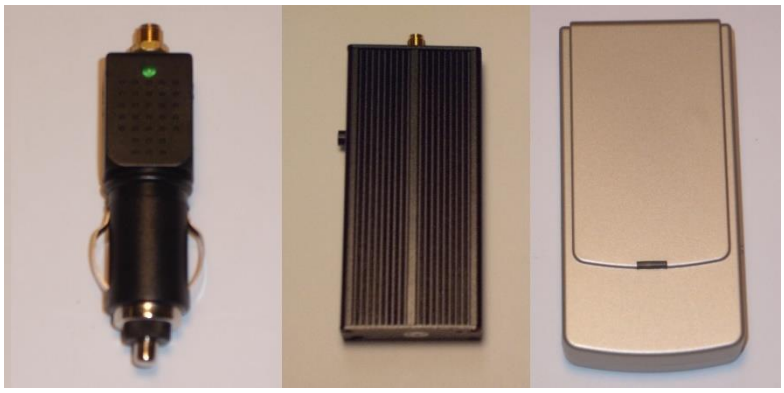
Jamming je definovaný jako „emise vysokofrekvenční energie dostatečného výkonu a takových vlastností, aby se zabránilo přijímači v cílové oblasti používat GPS signál“ [24].

3.1.1 Charakteristika rušících signálů

Vysokofrekvenční rušení (RFI) může být impulsní nebo spojité. Spojité vysokofrekvenční rušení může být dále děleno podle šířky pásma na úzkopásmové a širokopásmové. Toto dělení je relativní i pro GNSS frekvenční pásmo [11] a definuje, že širokopásmové rušení má stejnou nebo větší šířku pásma, než je šířka pásma GNSS (např. 2 MHz pro C/A kód). Úzkopásmové rušení má užší šířku pásma

V roce 2011 proběhl v USA skupinou Ryana H. Mitche průzkum vlastností 18 komerčně dostupných rušiček určených k zarušení civilního signálu systému GPS [25]. Zařízení jsou rozdělena podle zdroje napájení a typu antény na tři kategorie:

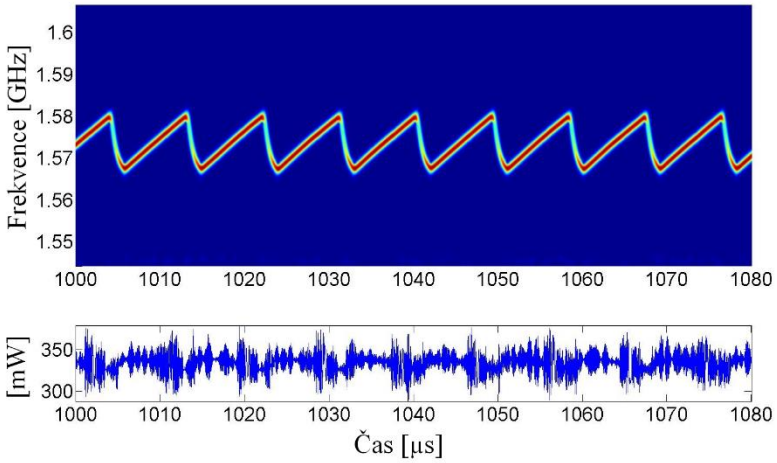
- Rušičky navrhnuty pro připojení k 12 V automobilové zásuvce. Tyto rušičky mají obvykle malý vysílací výkon do 100 mW.
- Rušičky napájené baterií a vybavené externí anténou připojenou přes SMA konektor. Některé typy mohou mít vysílací výkon až 1 W.
- Rušičky zamaskované jako jiné elektronické zařízení, např. mobilní telefon a obvykle používají pilovou frekvenční modulaci.



Obr. 3.1: Příklady možných GPS jammerů. Převzato z [25].

Analýzou těchto rušiček se zjistilo, že všechny Rušičky pracují se šířkou pásma 2 MHz na pokrytí civilního C/A signálu v pásmu. Většina rušiček používá frekvenční modulaci lineárně rozmítané vlny pro generování širokopásmové interference.

Obr. 3.2 zobrazuje výsledek analýzy typického signálu rušiček z první skupiny. Horní graf znázorňuje sérii lineárního rozmítání signálu, kde perioda je 9 μs a pokrývá pásmo o 14 MHz včetně GPS pásma L1. Spodní graf znázorňuje závislost vysílaného výkonu na čase [25].



Obr. 3.2: Signál rušiček z první skupiny. Převzato a upraveno z [25].

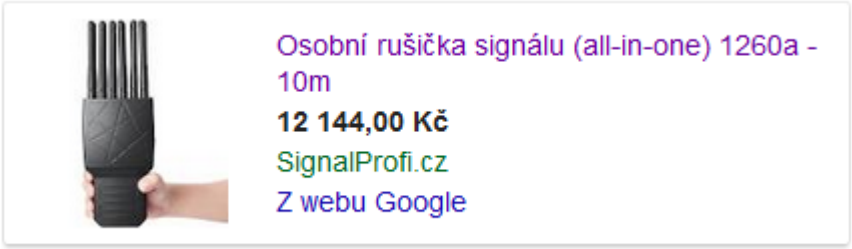
3.1.2 Zaznamenané incidenty

Incidenty spojené s rušením GPS signálu lze rozdělit dle původu rušení na civilní a vojenské rušení.

V krizových situacích může vláda nebo armáda přistoupit k rušení civilního signálu, kde cílem je omezit přístup k systému pro neautorizované uživatele. Mezi zaznamenané incidenty vojenského původu patří:

- Rušení GPS signálu Severní Koreou [26].
- Rušení GPS signálu na severu Norska během cvičení ruské armády [27].
- Rušení GPS signálu a dalších radiokomunikačních systémů během konfliktu na Ukrajině [28].
- Rušení GPS signálu v Sýrii ruskou armádou [29].
- Rušení GPS signálů v Nevadě a Coloradu během leteckého cvičení „Red Flag“ [30].

Civilní rušičky GPS signálu nabývají v poslední době na popularitě a lze je snadno pořídit na internetu i prostřednictvím reklamy, viz Obr. 3.3. Pro uživatele existuje velké množství důvodů, proč tyto zařízení používat.



Obr. 3.3: Reklama na osobní rušičku rušící i GPS systém

Časté je použití u řidičů firemních vozidel pro zachování soukromí před zaměstnavatelem nebo k obejití placení mýtného. Nutno zmínit, že použití těchto rušiček je nejen na území České republiky nezákonné. Mezi zaznamenané incidenty civilního původu patří:

- Rušení pozemního systému monitorujícího integritu (GBAS) na mezinárodním letišti v Newarku, USA způsobené osobní rušičkou v automobilu [31].
- Rušení GPS signálu na letišti ve Philadelphii způsobenou rušičkou v dodávkovém voze poblíž letiště [32].
- 78 zjištěných případů použití GPS rušičkou ve vozidle na dálnici v USA [32].
- Použití GPS rušiček na silnicích ve Velké Británii [33].

3.2 Vysílání podvrženého signálu

Vysílání podvrženého signálu, často používaný anglický termín spoofing, je dle [24] technika, kdy se vysílá falešný GNSS signál GNSS přijímači, který poskytuje falešné informace o poloze, rychlosti a času (PVT). Cílem spoofingu je tajně přinutit GNSS přijímač sledovat falešný signál s cílem poskytnout odlišné řešení polohy od skutečné. I pokud by spoofing nebyl plně úspěšný, spoofing obvykle způsobí významné chyby určení PVT a efektivně zaruší možný příjem GNSS signál.

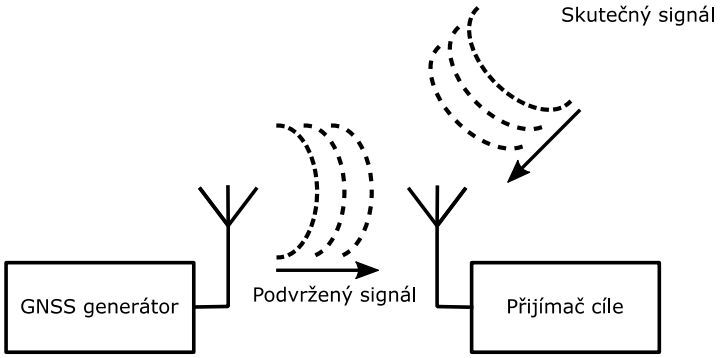
Vysílání podvrženého signálu je mnohem náročnější k realizace než rušení, proto se často zaměřuje proti individuálnímu cíli místo plošného působení. Přesto může spoofing působit jako zdroj rušení pro velké území, protože zdroj podvrženého signálu může vysílat zavádějící data do určené oblasti, PRN signál může působit jako vysoce efektivní zdroj rušení na velké vzdálenosti. Spoofery – zdroje podvržených signál můžou také překonat všechny ochrany proti zarušení.

Do spoofingu se řadí též tzv. „Meaconing“. Meaconing je označení pro typ útoku, kdy se vysílá předem nahraný, zpožděný, signál pro zmatení přijímače cíle útoku [24].

3.2.1 Charakteristika spoofing útoků

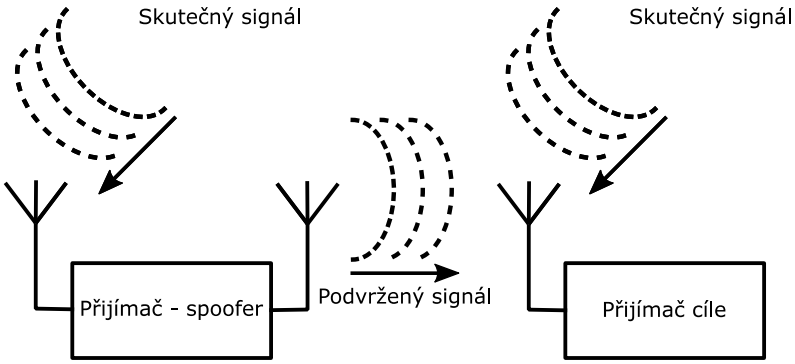
Profesor Humreyse a kolektiv ve své práci [34] zaměřené na vývoj přenosného osobního spooferu rozděluje útoky podvrženým signálem na tři kategorie:

Nesofistikovaný útok – Používá se komerční generátor GNSS signálů pro generování podvrženého signálu pro danou polohu. Výhodou je jednoduchost, kdy není potřeba znát aktuální PVT informace cíle. Nevýhoda je cena a velikost těchto komerčních GNSS generátorů a relativně snadné odhalení útoku.



Obr. 3.4: Princip nesofistikovaného útoku.

Středně obtížný útok – K útoku je nejprve potřeba získat PVT informace cíle a tyto informace použít k vygenerování podobného podvrženého signálu, který je následně vysílán anténou směrem k cíli. K tomuto lze s výhodou použít softwarově definované rádio. Následně se postupně zvyšuje výkon falešného signálu, dokud cílový přijímač nezamkne na falešný signál. Poté může spoofer postupně měnit PVT informace cíle na libovolnou hodnotu. Tento typ útoku je těžké odhalit pomocí běžných algoritmů zpracování signálů v GNSS přijímačích.



Obr. 3.5: Princip středně obtížného útoku.

Sofistikovaný útok – Jedná se o podobný typ útoku jako výše uvedený středně obtížný útok. Používá se několik koordinovaných spooferů, fázově synchronizovaných, současně vysílajících podvržené signály z různých směrů k cíli. Výhoda je obtížné odhalení útoku běžným přijímačem s jednou anténou. Nevýhoda je obtížné provedení tohoto útoku.

3.2.2 Matematický model útoku

Matematický popis přijímaného signálu v případě probíhajícího útoku podvrženými signály lze modelovat pro dva případy:

- Přijímač s jednou anténou
- Přijímač s anténním polem

Přijímač s jednou anténou – GPS C/A kód ve frekvenčním pásmu L1 pod vlivem útoku podvrženými signály může být modelován jako:

$$r(nT_s) = \sum_{m=1}^{N_{au}} \sqrt{p_m^a}\, F_m^a(nT_s) + \eta(nT_s) + \sum_{q=1}^{N_{sp}} \sqrt{p_q^s}\, F_q^s(nT_s) + \eta(nT_s) \tag{3.1}$$

Kde:

$$F_m^a(nT_s) = h_m^a(nT_s - \tau_m^a)c_m^a(nT_s - \tau_m^a)e^{j\phi_m^a + j2\pi f_m^a nT_s}, \tag{3.2}$$

$$F_q^s(nT_s) = h_q^{as}\left(nT_s - \tau_q^s\right)c_q^s\left(nT_s - \tau_q^s\right)e^{j\phi_q^s + j2\pi f_m^s nT_s}, \tag{3.3}$$

N_{au} počet autentických pseudonáhodných signálů,

N_{sp} počet podvržených pseudonáhodných signálů,

T_s vzorkovací perioda,

a,m označení pro autentické signály,

s,q označení pro podvržené signály,

n komplexní přídavný bílý Gaussovský šum s odchylkou σ^2,

$h(nT_s)$ vysílaná data navigační zprávy v okamžiku T_s,

$c(nT_s)$ pseudonáhodná sekvence v okamžiku T_s,

ϕ fáze nosné vlny,

f Dopplerova frekvence nosné vlny,

p přijímaný výkon,

τ časový posun kódu přijímaného signálu.

Přijímač s anténním polem – Předpokládá se N – prvkové anténní pole, kde jedna z antén je zvolena jako referenční. Dále se předpokládá, že zdroj podvržených signálů je vysílač s jednou anténou, která vysílá odlišné pseudonáhodné signály ze stejné lokality. Proto je možné komplexní reprezentaci N přijatých prostorově oddělených vzorků autentických a podvržených signálů zapsat ve formě vektoru:

$$\boldsymbol{r}(nT_s) = \begin{bmatrix} r_1(nT_s) \\ \vdots \\ r_N(nT_s) \end{bmatrix} = \sum_{m=1}^{N_{au}} \boldsymbol{a}_m \sqrt{p_m^a}\, F_m^a(nT_s) + \boldsymbol{b} \sum_{q=1}^{N_{sp}} \sqrt{p_q^s}\, F_q^s(nT_s) + \boldsymbol{\eta}(nT_s). \quad (3.4)$$

Kde:

$\boldsymbol{\eta}$ Nx1 komplexní přídavný bílý Gaussovský šum, s kovarianční maticí $\sigma^2\boldsymbol{I}$, kde $\boldsymbol{I}$ reprezentuje N x N jednotkovou matici,

$\boldsymbol{a}_m$, $\boldsymbol{b}$ řídící vektory zahrnující prostorové charakteristiky anténního pole pro autentický a podvržený signál.

Řídící vektory lze popsat následovně:

$$\boldsymbol{b} = \begin{bmatrix} 1 \\ b_2 \\ \vdots \\ b_N \end{bmatrix} = \begin{bmatrix} e^{-j(\frac{2\pi \boldsymbol{d}_{11}^{ant} \cdot \widehat{\boldsymbol{d}}^{sp}}{\lambda})} \\ e^{-j(\frac{2\pi \boldsymbol{d}_{21}^{ant} \cdot \widehat{\boldsymbol{d}}^{sp}}{\lambda})} \\ \vdots \\ e^{-j(\frac{2\pi \boldsymbol{d}_{N1}^{ant} \cdot \widehat{\boldsymbol{d}}^{sp}}{\lambda})} \end{bmatrix}, \quad (3.5)$$

$$\boldsymbol{a}_m = \begin{bmatrix} 1 \\ (a_m)_2 \\ \vdots \\ (a_m)_N \end{bmatrix} = \begin{bmatrix} e^{-j(\frac{2\pi \boldsymbol{d}_{11}^{ant} \cdot \widehat{\boldsymbol{d}}_m^{au}}{\lambda})} \\ e^{-j(\frac{2\pi \boldsymbol{d}_{21}^{ant} \cdot \widehat{\boldsymbol{d}}_m^{au}}{\lambda})} \\ \vdots \\ e^{-j(\frac{2\pi \boldsymbol{d}_{N1}^{ant} \cdot \widehat{\boldsymbol{d}}_m^{au}}{\lambda})} \end{bmatrix}. \quad (3.6)$$

Kde:

$\boldsymbol{d}_{i1}^{ant}$ reprezentuje směrový vektor z počátku (fázový centrum referenční antény) k fázovému středu *i*-té antény.

$\widehat{\boldsymbol{d}}^{sp}$ reprezentuje směrový jednotkový vektor z počátku ke zdroji podvržených signálů

$\widehat{\boldsymbol{d}}_m^{au}$ reprezentuje směrový jednotkový vektor z počátku ke k *m*-té navigační družici, zdroji autentických signálů.

3.2.3 Zaznamenané incidenty

Obdobně jako jamming (viz kapitola 3.1.2) můžeme rozdělit incidenty spojené s vysíláním podvrženého signálu rozdělit na vojenské a civilní.

Spoofing probíhá jak v rámci cvičení armád, tak v rámci elektronické války v probíhajících konfliktech. Doložené vojenské případy:

- Zajetí bezpilotního dronu využitím spoofingu armády USA iránskou armádou [35].
- GPS spoofing okolí Kremlu, kde podvrhovaná poloha byla mezinárodní letiště Vnukovo [36].
- Masivní GPS spoofing minimálně 20 lodí v Černém moři, kde podvrhovaná poloha byla mezinárodní letiště Gelendzhik [37].

Doložené civilní případy jsou stále z řady průzkumu odolnosti a slabin navigačních signálů. Zatím nebylo zaznamenáno, že by se spoofing použil k překročení zákona. S rostoucí dostupností softwarového a hardwarového vybavení (především softwarově definovaného rádia) se dá předpokládat i rostoucí riziko zneužití spoofingu. Příklady civilního spoofingu:

- Demonstrativní únos luxusní jachty odkloněním autopilota využitím spoofingu týmem profesora Humpreyse [38].
- Ovládnutí bezpilotního dronu pomocí spoofingu týmem z Texaské univerzity [39].
- Demonstrační GPS spoofing v Národní laboratoři Los Almos v roce 2002 [40].
- Demonstrační spoofing na konferenci v Portlandu, provedený pomocí GPS generátoru [41].

4 Rozbor opatření proti podvržení falešných signálů

V poslední době probíhá výzkum různých opatření na detekci a aktivních opatření proti podvržení signálům a tím zvýšení důvěryhodnosti získaných informací z GNSS systémů.

Tato kapitola ve své první části uvádí stručný přehled různých opatření pro odhalení podvržených signálů. Rozebrány jsou metody RAIM, určené k autonomní kontrole integrity systému. Ve své druhé části jsou jednotlivá opatření porovnána podle účinnosti na různé typy útoků, požadavků na zavedení a náročnosti implementace.

4.1 Přehled opatření proti podvržení falešných signálů

4.1.1 Vyhodnocení statistických vlastností signálu

Aleksandr Jovanovic a Cyeil Botteron popisují ve článku [43] tři protiopatření založená na sledování statistických vlastnostech signálu, jako je odstup výkonu nosné vlny od spektrální výkonové hustoty šumu C/N_0, Dopplerův posun a obsah navigační zprávy. Metoda monitoruje výše uvedené statistické vlastnosti a zjišťuje přítomnost signálu, případě jeho nekonzistenci při přítomnosti falešného signálu.

Detektor výkonového prahu PTD (Power Treshold Detector) – Metoda je založena na průběžném sledování a zaznamenání statistik C/N_0 pro jednotlivé navigační signály. Cílem protiopatření je v odhadu klouzavého rozptylu pozorovaného signálu $MV_i(W)$, kde W je velikost klouzavého okna, ve kterém se provádí výpočet rozptylu. Při přítomnosti podvrženého signálu se hodnota zásadně mění. Pokud tato hodnota překročí stanovený práh, dojde k varování. Protiopatření jsou založena na předpokladu, že nesofistikované útoky budou mít tendenci používat GNSS generátory, které poskytují o několik řádů vyšší výkon než jakýkoliv navigační signál na povrchu Země.

Detektor Dopplerova posuvu DOD (Doppler Offset Detector) – Metoda je založena na průběžném sledování, zaznamenání statistik a použití lineárního predikčního modelu Dopplerova posuvu. Stejně jako u PTD se vyhodnocuje klouzavý rozptyl v dané velikosti klouzavého okna a odchylka od lineárního modelu. Při přítomnosti podvrženého signálu se hodnota zásadně mění. Pokud tato hodnota překročí stanovený práh, dojde k varování. Navíc, pokud dojde k varování na možný spoofing útok, na základě lineárního modelu s přibližným Dopplerovo posuvem může GNSS přijímač nadále pokračovat ve sledování správného signálu.

Test konzistence GNSS signálu SCT (GNSS Signal Consistency Tests) – Metoda je založena na konzistenci aktualizace polohy a času, efemerid a změn rychlosti pseudonáhodného kódu. V případě zjištění nekonzistence (například velká změna polohy a času mezi dvěma periodami) dojde k varování uživatele.

Autoři článku zároveň otestovali výše uvedené protiopatření pomocí GNSS generátoru Agilent GSS800 a výsledky testů ukazují, že navrhované metody úspěšně detekují nesofistikovaný a středně obtížný spoofing útok s malou pravděpodobností falešného varování.

4.1.2 Sledování parametrů přijímaného signálu

Celkem sedm metod popsaných v [42] jsou určeny pro systém GPS. Používají sledovaní parametrů přijímaného signálu k vyhodnocení, zda se jedná o podezřelý signál. Vychází se z předpokladu, že výkon falešného signálu bude, minimálně z počátku, vyšší než skutečný signál.

Sledování absolutního výkonu GPS signálu – Porovnává se průměrovaný výkon přijímaného signálu s očekávanou hodnotou -160 dBW. Vychází se z principu, že nesofistikované útoky používají GPS generátory, které mají obvykle o mnohem vyšší výkon signálu, než může mít navigační signál z libovolné družice na povrchu Země.

Sledování relativního výkonu GPS signálu – Hodnota výkonu přijímaného signálu je průměrována a porovnávána s předchozím vzorkem. Extrémní velká změna může znamenat začátek generování podvrženého signálu GPS generátorem.

Sledování výkonu pro každý přijímaný družicový signál – Je kombinací obou předchozích metod, kde se absolutní a relativní výkon porovnává pro každý přijímaný satelitní signál. Vychází se z předpokladu, že signál z GPS simulátoru bude mít pro každý satelit podobný výkon. Skutečný přijímaný GPS signál se nicméně pro každý satelit mění v čase.

Sledování identifikačních kódů družic a počtu družicových signálů – Porovnává se v čase identifikační kód družic, jejich počet a počet navigačních signálů. Vychází z předpokladu, že při útoku pomocí GPS generátoru generátor simuluje větší počet družic, než je počet viditelných družic na obloze.

Sledování časového intervalu – Porovnává se čas příjmu jednotlivých navigačních signálů. Vychází se z předpokladu, že generátor simuluje všechny signály ve stejný okamžik.

Provedení porovnání času – Porovnává se GPS čas určený z příchozích navigačních signálů s nepřetržitým zdrojem přesných hodin v přijímači. Tím lze kontrolovat hodnověrnost příchozích signálů.

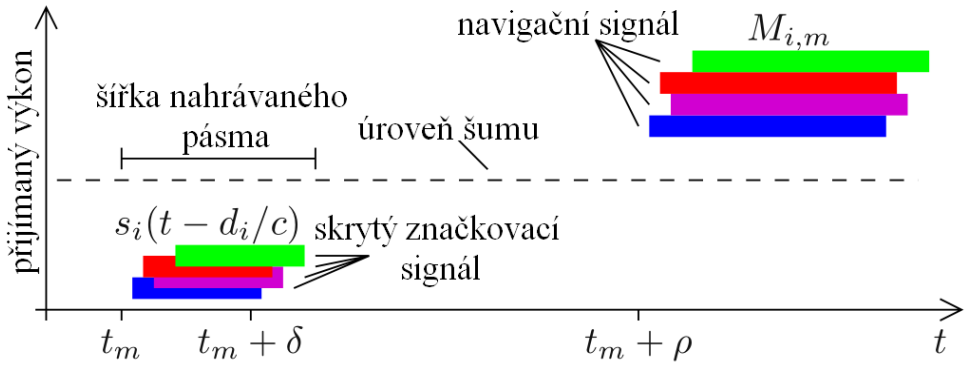
Provedení porovnání údajů s dalším nezávislým snímačem – Porovnání přijímané pozice a pohybu s interním snímačem, jako například kompas nebo akcelerometr.

U všech uvedených metod se uvažuje s nastavením prahu, kdy po jeho překročení dojde k upozornění uživatele. Tyto protiopatření nezabrání spoofing útokům, ale můžou upozornit uživatele GPS přijímače na podezřelou aktivitu a tím snížit pravděpodobnost úspěšného jednoduchého útoku s použitím GPS generátoru, viz kapitola 3.2.1.

4.1.3 Asymetrický bezpečnostní mechanismus

Markus G. Kuhn popisuje v článku [44] odlišný přístup k opatření proti podvrženým signálům. Oproti ostatním diskutovaným opatřením, která se soustřeďují především na vyhodnocení přijímaného signálu, navrhuje změnu struktury navigačního signálu.

Metoda navrhuje, aby každá družice vysílala přídavný signál v podobě obdélníkového pulsu o době trvání δ, rozprostřené ve spektru nezveřejněnou pseudonáhodnou sekvencí. Tento signál je vysílán periodicky s takovou výkonovou úrovní, aby byla nižší aspoň o 20 dB než tepelný šum při přijmutí přijímačem. Přijímače po filtraci ukládají do své paměti šum v daném frekvenčním pásmu. Po odvysílaní skrytého značkovacího signálu je po zpoždění ρ dále vysílán navigační signál, který obsahuje pseudonáhodnou sekvenci předcházejícímu skrytému značkovacímu signálu $M_{i,m}$. Navigační signál je vysílán na normální výkonové úrovni.



Obr. 4.1: Rozložení výkonových úrovní. Převzato a upraveno z [44].

Vzájemnou korelací uloženého šumu a pseudonáhodné sekvence z navigačního signálu se určí zpoždění ρ, které je voleno tak, aby bylo zpoždění větší než nejistota zdroje hodin jednotlivých přijímačů. Protiopatření je založena na předpokladu, že útoky používající generovaný signály nebo dříve nahrané a zpožděné lze provést pouze se zpožděním $\Delta t > \rho$ a tím lze útoky snadno detekovat.

4.1.4 Víceúrovňový bezpečnostní mechanismus

Studie [45] prokázala citlivost fázových měřících jednotek PMU (Phasor Measurement Unit) používaných v inteligentních distribučních sítích na citlivost časové synchronizace na spoofing útoku. Protiopatření popsaná v článku [46] se zabývá aplikací vícevrstvé ochrany PMU.

První vrstva, nazývána fyzická, se skládá ze dvou GPS přijímačů, kde jeden přijímá signál z monopólu a druhý přijímač přijímá signál z flíčkové antény. GPS přijímače jsou blízko sobě. Na základě odlišných směrových charakteristik antén se vypočítá úhel příjmu signálů AOA (Angle of Arrival) všech GPS přijímačů v síti. Úhel příjmu bude stejný pro oba přijímače za předpokladu, že se přijímá signál z družic. Případný rozdíl může detekovat spoofing útok.

Druhá vrstva, nazývána horní vrstva. Pro určení důvěryhodnosti jednotlivých PMU se na základě lineárního modelu přenosové sítě kolem rovnovážného bodu a metody odhadu Kálmánovo filtrem zpracovávají informace z fyzické vrstvy.

Zavedení protiopatření je snadné, je potřeba další GPS přijímač a anténa pro implementaci protiopatření. Při požadavku použití mimo systém chytrá přenosové sítě je nutné přijít s modifikacemi protiopatření. Výsledky z testů ukázaly, že detekce spoofingu je účinná při nesofistikovaném útoku i sofistikovaném útoku.

4.1.5 Zpracování signálu z anténního pole

Autoři J. Magiera a R. Katulski článku [47] předkládají použití prostorového zpracování signálů jako účinný způsob k odhalení podvrženého signálu GPS přijímači. Uvedená metoda slouží nejen k detekci spoofing útoku, ale také snižuje vliv spoofing útoku na GPS přijímač.

Metoda vyžaduje příjem signálu přes anténní pole s takovým počtem dílčích prvků, aby bylo možné vypočítat směr příjmu signálů DOA (Direction of Arrival). DOA určuje azimut a elevaci příchozího signálu. Dále se měří fázové zpoždění (viz 1.3.1). Článek doporučuje použít čtyř prvkové uniformní kruhové pole.

Směr příjmu signálu odpovídá rozdílu fázového zpoždění signálu na výstupu anténního pole. Nejednoznačnost při řešení DOA je velmi závislá na rozložení prvků v poli a jejich vlastnostech. Za předpokladu, že podvržené signály budou vysílány z jednoho zdroje, bude i jejich příjem ze stejného směru, bez ohledu na to, zda jde o přímý nebo odražený signál. Při příjmu navigačních signálů z družic, za předpokladu čistého výhledu na oblohu, bude přijímač přijímat signály z různých směrů v rámci celé polokoule. Na základě tohoto předpokladu je spoofing detekován, když má více přijatých signálů stejné nebo velmi podobné vlastnosti, a takové signály vyloučí z dalšího zpracování.

Přesnost metody byla testována měřením pravděpodobnosti falešného varování a detekci spoofing útoku s různým počtem přijatých signálů (4 až 8). Výsledkem je 99 % šance na detekci spoofingu při C/N_0 alespoň 46 dBHz.

4.1.6 Vzájemná korelace vojenských signálů dvou přijímačů

Metoda uvedená v práci [48] je navržena pro ochranu civilních, veřejných, GNSS signálů a využívá přítomnosti vojenských, zašifrovaných, signálů na stejné frekvenci. Závisí také na znalosti časování a vztahu nosné na fázi neveřejného signálu na civilní.

Civilní signál, například C/A GPS kód ve frekvenčním pásmu L1, je sledován v chráněném referenčním přijímači a druhém ohroženém přijímači, možné oběti útoku. Civilní signál je použit k separaci části přijímaného zašifrovaného signálu. Vzájemná korelace se provádí na částích zašifrovaného signálu z obou přijímačích poté, co jsou přivedeny dohromady skrz komunikační spojení. Použití vzájemné korelace umožňuje použít zašifrovaný signál i bez znalosti příslušné pseudonáhodné posloupnosti.

Vysoká podobnost signálu značí, že nedošlo ke spoofing útoku a šifrovaný signál je přítomen v obou přijímačích. Naopak nízká hodnota podobnosti signálu značí, že šifrovaný signál není přítomen v ohroženém přijímači. To může nastat, pokud přijímaný civilní signál je podvržený. Při nedosažení určitého prahu podobnosti je uživatel varován na možný spoofing útok.

Tato metoda byla autory článku testována nahranými signály a off-line signálovému zpracování. Metoda úspěšně detekovala spoofing útok na C/A GPS signál ve frekvenčním pásmu L1 vzájemnou korelací vojenského P(Y) signálu.

4.1.7 Vyhodnocení kvality signálu

Autoři článku [49] předkládají nový přístup k detekci spoofing útoků, založené na vyhodnocení parametrů signálu. Metoda je založená na měření celkové energie autentického i podvrženého signálu. Na rozdíl od jiných podobných metod popsaných v 4.1.1 a 4.1.2 nepotřebuje měřit další parametry, jako je Dopplerův posuv.

Celkové energie signálů se určí z cyklických charakteristik C/N_0 bez korelace šumových komponent. Interference způsobená podvrženým signálem snižuje odstup signál/šum SNR autentického signálu, mezitímco šumové pozadí přijímače roste společně s výkonem podvrženého signálu. Při překročení stanoveného prahu, dojde k varování uživatele.

Pro stanovení prahu je potřeba znát celkový počet přijímaných navigačních signálů z družic. K tomu je možné použít informaci o počtu dostupných družic z almanachu systému, uloženého v paměti přijímače. Výsledky simulace ukazují, že metoda funguje i když autentický a podvržený signál jsou si výkonově na blízku. Detekce funguje lépe s rostoucí výkonovou úrovní podvrženého signálu.

4.1.8 Metody RAIM

Podvržené signály úspěšně vpravují do výpočtu polohy přijímače falešné pseudovzdálenosti. Určení polohy nemusí být konzistentní, v důsledku toho výpočty polohy nemusí vést k rozumným výsledkům. Velká část GPS přijímačů používá pro kontrolu integrity měření a vyloučení odchylek měření metody pro autonomní monitorování integrity RAIM (Receiver Autonomous Integrity Monitoring). Tato metoda používá redundantní informace k detekci chyby v GNSS systému.

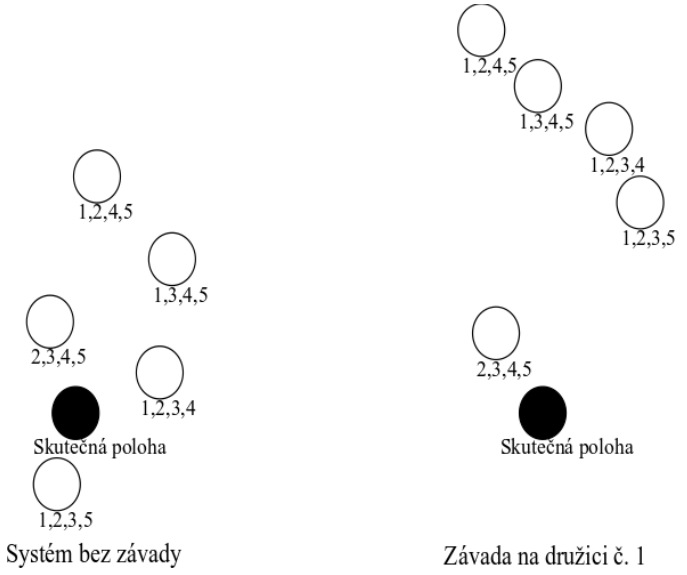
Na úrovni určení polohy můžou být RAIM metody úspěšnou ochranou před spoofingem. Účinnost je zjištěna pouze za předpokladu, že ve výpočtu polohy je pouze jeden nebo dvě podvržené pseudovzdálenosti. V opačném případě, kdy většina pseudovzdálenosti je z podvržených signálů můžou být z výpočtu vyřazené autentické pseudovzdálenosti [50].

Metody RAIM byly zavedeny v požadavku kontroly integrity systému. Dle [51] je integrita měřítkem důvěryhodnosti systému a jeho poskytovanými informacemi. Zahrnuje schopnost systému včas varovat uživatele, že v systému došlo k poruše a nesmí být použit k navigaci.

Jak bylo řečeno, RAIM používá redundantních informací k monitorování integrity. Je potřeba viditelnosti alespoň pěti družic k zjištění závady jedné družice. Existují dvě základní metody pro provedení kontrol konzistence měření polohy.

Solution Separation / Position Comparison RAIM – Princip metody spočívá v tom, že přijímač počítá odhad polohy pro viditelnou konstelaci družic a tento odhad porovnává s dílčími odhady polohy, kdy jedna z družic je vyloučena z výpočtu. Předpokladem je, že nanejvýš jedna družice může poskytovat špatné informace. Pro řešení navigační úlohy je potřeba čtyř družic (viz kapitola 1.4), pro použití RAIM je potřeba minimálně pěti družic. Pokud budou všechny viditelné družice fungovat bezchybně, výsledky porovnání s dílčími řešeními nebudou vykazovat velké odchylky. V případě chyby jedné družice bude porovnání vykazovat velkou odchylku. Výsledky jsou porovnány se statistickým modelem a stanoveny úrovně ochrany.

Obr. 4.2 ilustruje chování Solution Separation metody před poruchou jedné družice a po poruše. V případě správné funkce GNSS systému mají dílčí řešení (kroužky bez výplně) malou odchylku od správného řešení (vyplněný kroužek). Při poruše družice 1 bude odchylka všech dílčích řešení, které zahrnují družici 1 do svého výpočtu, značně větší [52].



Obr. 4.2: Princip Solution Separation RAIM. Převzato a upraveno z [52].

Pseudo-Range residual / Range Comparison RAIM – Rozdíl mezi odhadovanou zdánlivou vzdáleností mezi přijímačem a navigační družicí a vypočtenou zdánlivou vzdáleností – rezidua zdánlivé vzdálenosti se označují pod pojmem „Pseudo-Range residuals“. Tyto rozdíly obsahují dostatečné informace k provedení kontroly integrity přesnosti GPS systému. Algoritmus této RAIM metody provede výpočet určení polohy pro všechny viditelné družice konstelace.

Algoritmus RAIM metody vyhodnocuje průběžně přesnost GPS systému na základě statistické analýzy reziduí zdánlivé vzdáleností. Je známo, že přesné řešení navigační úlohy bude odpovídat malým reziduím zdánlivé vzdáleností, zatímco nepřesné řešení polohy odpovídá velkým reziduím zdánlivé vzdáleností [53].

4.1.9 Inerciální navigace s implementací RAIM

Práce [54] představuje novou metodu přímé detekce spoofing útoku s použitím GPS přijímače a senzorů inerciální navigace fungující na koncepci RAIM. Metoda také poskytuje monitoring integrity systému GPS.

Detektor navržený v této metodě sleduje nesrovnalosti mezi měřením GPS přijímačem a měřením inerciální navigace. Existuje řada možných integračních schémat na spojení GPS navigace a inerciální navigace. Zde se se používá velmi těsná implementace, kdy GPS navigace průběžně kalibruje monitoring chyb inerciální navigace. To zvyšuje citlivost metody na nesrovnalosti v určení polohy způsobené spoofing útokem. RAIM koncepce v této metodě používá redundantní informace ze senzorů inerciální navigace. Pro zvýšení přesnosti se používá historie určených poloh GPS navigací k určení polohového vektoru, stejně jako měření reziduí v dávkovém váženém odhadu nejmenších čtverců.

Metoda byla autory testována a bylo prokázáno, že dokáže detekovat všechny druhy spoofing útoků s jedinou výjimkou. Za předpokladu, že útočník bude znát přesné parametry trajektorie přijímače, dokáže generovat takové podvržené signály, že nebude reagovat varováním.

4.2 Porovnání opatření proti falešným signálům

Kritéria pro porovnání metod, vybraná podle [55], jsou uvedeny v tabulce Tab. 4.1. Cílem je nalézt efektivní protiopatření proti útoku podvrženými signály. Důležitá je nejen detekce jednotlivých druhů spoofing útoků, ale i další parametry. Mezi tyto parametry patří možnost snadné a rychlé implementace, cenová dostupnost nebo možnosti použít opatření na libovolném přijímači s dostatečnou výpočetní kapacitou. Efektivita metody nezávisí pouze na metodě samotné, ale i požadavcích uživatele.

Tab. 4.1: Přehled porovnávaných parametrů. Převzato a upraveno z [55]

Kritérium	Definice	Možnosti
Rychlá implementace	Možnost rychlé implementace metody	Ano/Ne
Efektivní náklady	Cenově dostupné opatření pro zavedení v malých sérií výroby	Ano/Ne
Nesofistikovaný útok	Schopnost detekovat nesofistikovaný útok	Ano/Ne
Středně obtížný útok	Schopnost detekovat středně obtížný útok	Ano/Ne
Sofistikovaný útok	Schopnost detekovat sofistikovaný útok	Ano/Ne
Úprava na straně vysílače	Požadavek na změnu na straně kosmického segmentu pro implementaci opatření	Ano/Ne
Úprava na straně přijímače	Požadavek na změnu na straně uživatelského segmentu pro implementaci opatření	Ano/Ne
Ověření	Opatření bylo otestováno	Ano/Ne
Interoperabilita	Nezávislost na typu přijímače	Ano/Ne
Externí vybavení	Požadavek na externí hardware pro implementaci opatření	Ano/Ne

Z tabulky Tab. 4.2 lze vidět, že všechny opatření mají schopnost detekovat nesofistikovaný útok proti přijímači. Celkem tři metody jsou schopné detekovat i sofistikovaný útok. Konkrétně se jedná o metody:

- Asymetrický bezpečnostní mechanismus
- Vzájemná korelace vojenských signálů dvou přijímačů
- Vyhodnocení kvality signálu

První dvě metody mají nedostatek v náročnosti realizace. První požaduje úpravu vysílání navigačních družic. Tato úprava by byla velmi drahá a časově náročná. Druhá z metod požaduje použití dvou GPS přijímačů vzájemně propojených komunikačním kanálem a dodatečným výpočetním výkonem. Opět se jedná o finančně náročnou metodu. Třetí z metod byla prezentována v roce 2018. Naopak od předchozích opatření požaduje pouze dodatečný výpočetní výkon na straně přijímače pro vyhodnocení kvality signálu. Mezi porovnávanými metodami patří k nejefektivnějším, ale jak bylo uvedeno autory metody, je potřeba další vývoj pro vytvoření spolehlivého detekčního systému proti všem možným scénářům útoků podvrženým signálem.

Tab. 4.2: Analýza parametrů protiopatření

Opatření	Rychlá implementace	Efektivní náklady	Nesofistikovaný útok	Středně obtížný útok	Sofistikovaný útok	Úprava na straně vysílače	Úprava na straně přijímače	Ověření	Interoperabilita	Externí vybavení
Vyhodnocení statistických vlastností signálu	Ano	Ano	Ano	Ne	Ne	Ne	Ano	Ano	Ano	Ne
Sledování parametrů přijímaného signálu	Ano	Ano	Ano	Ne	Ne	Ne	Ano	Ne	Ano	Ne
Asymetrický bezpečnostní mechanismus	Ne	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ne	Ne
Víceúrovňový bezpečnostní mechanismus	Ano	Ano	Ano	Ano	Ne	Ne	Ne	Ano	Ne	Ano
Zpracování signálu z anténního pole	Ne	Ano	Ano	Ano	Ne	Ne	Ne	Ano	Ano	Ano
Vzájemná korelace vojenských signálů dvou přijímačů	Ne	Ne	Ano	Ano	Ano	Ne	Ne	Ano	Ne	Ano
Vyhodnocení kvality signálu	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano	Ano	Ne
Metody RAIM	Ano	Ano	Ano	Ano	Ne	Ne	Ne	Ano	Ano	Ne
Inerciální navigace s implementací RAIM	Ne	Ano	Ano	Ano	Ne	Ne	Ne	Ano	Ne	Ano

5 Generátory GNSS signálů

Tato kapitola se zabývá problematikou GNSS přijímačů. V první části jsou prezentovány komerční GNSS generátory. Ve druhé části jsou představeny volně dostupné projekty pro generování GPS signálu. Volně dostupný projekt GPS-SDR-SIM je následně zprovozněn a otestována jeho funkčnost.

5.1 Komerční

Na trhu je k dostání celá řada generátorů GNSS signálů pro účely testování GNSS přijímačů. Tyto generátory jsou určeny pro testování sériově vyráběných přijímačů nebo k testování specifických scénářů jako je například testování GNSS přijímačů pro nadzvukové letouny. Vysoké pořizovací náklady na tyto generátory představují překážku pro jejich pořízení pro menší společnosti nebo výzkumné týmy. Jako alternativa drahým hardwarovým řešení je softwarové řešení, kdy generování signálu probíhá v PC a s použitím softwarově definovaného rádia je signál vysílán.

5.1.1 Hardwarové simulátory

Do této skupiny se řadí jednoúčelové přístroje používané pro simulaci GNSS signálů a přídavné moduly pro RF signálové generátory. V tabulce Tab. 5.1 je přehled některých aktuálně nabízených simulátorů, včetně základních charakteristik [56, 57]. Hardwarově jsou tyto simulátory často založeny na softwarovém rádiu, z důvodu malých výrobních sérií.

Tab. 5.1: Komerční hardwarové simulátory GNSS

Výrobce	Označení	Podporované systémy	Frekvenční pásma	Počet kanálů
CAST Navigation	Cast-4000	GPS	L1, L2, L5	16
	Cast-5000	GPS	L1, L2	84
iFEN	NCS Titan Simulator	GPS, GLONASS, BeiDou, Galileo, QZSS	L1, L2C, L5, G1, G2, G3, B1, B2, B3, E1, E5ab, E6	256
Jackson Labs	CLAW	GPS	L1	18
L3M Technologies	GPSG-1000	GPS, Galileo	L1, L1C, L2C, E1, E5, E5ab	12
Rohde & Schwarz	SMBV100A	GPS, GLONASS, BeiDou, Galileo, QZSS	L1, L2, G1, G2, B1, B2, E1	24
Spectracom	GSG-6	GPS, GLONASS, BeiDou, Galileo, QZSS	L1, L2C, L5, B2, E5	32
Spirent	GSS9000	GPS, GLONASS, Beidou, QZSS	L1, L2, L5, E1, E6, E5ab, B1, B2	160

5.1.2 Softwarové simulátory

Do této kategorie jsou zařazeny takové softwarové simulátory, které nejsou svázány se specifickým hardwarem jako periférií. V tabulce Tab. 5.2 je uveden výběr těchto softwarových generátorů [58, 59]. Zastoupeny jsou placená rozšíření pro vývojové prostředí MATLAB [60] a LabVIEW [61].

Tab. 5.2: Komerční softwarové GNSS simulátory

Výrobce	Označení	Podporované systémy	Frekvenční pásma
NavSat	LabSat 3	GPS, GLONASS, BeiDou, Galileo, QZSS, SBAS	L1, G1, B1, E1
Sydel	SDX	GPS, GLONASS, BeiDou, Galileo	L1, L2C, L5, G1, G2, B1, B2, E1, E5ab
Navsys	GNSS Signal Architect	GPS, GLONASS	L1, L2
	GNSS Signal Architect toolkit	GPS, GLONASS	L1, L2
National Instruments	GNSS Simulation Toolkit	GPS, GLONASS	L1

5.2 Nekomerční

Pod licencí MIT je na serveru GitHub volně dostupný projekt GPS-SDR-SIM [62], jehož autorem je Takuji Ebinuma z Tokijské univerzity. GPS-SDR-SIM generuje podle zadaných údajů GPS signál v základním pásmu v podobě souboru s I/Q vzorky L1 C/A signálu. Tento soubor může být vysílán pomocí softwarově definovaného rádia jako např. USRP, BladeRF nebo HackRF. Program umožňuje generovat statický scénář pro jednu polohu a dynamický scénář, kdy se generovaná poloha mění dle předem dané trasy. Maximální délka pro statický scénář je 24 hodin, pro dynamický scénář 5 minut.

Na serveru GitHub je volně ke stažení projekt na generování gps signálu s názvem GPS-SIM [63]. Projekt je napsaný v programovacím prostředí MATLAB, avšak nejsou zveřejněny klíčové skripty k jeho funkčnosti. Funkčnost projektu však byla autory prezentována na konferenci DEF CON [64].

5.3 Zprovoznění GPS-SDR-SIM

5.3.1 Stažení a kompilace

Stažení a kompilace projektu pro použití v operačním systému Linux se realizuje následujícími příkazy:

```
$ git clone - https://github.com/osqzss/gps-sdr-sim
$ cd gps-sdr-sim
$ gcc gpssim.c -lm -O3 -o gps-sdr-sim
```

Pro generování GPS signálu je potřeba BRDC soubor s GPS efemeridy v RINEX formátu pro znalost platné konstelace navigačních družic.

5.3.2 BRDC soubor

BRDC (Broadcast Ephemeris Data) soubor obsahuje data v podobě vysílaných efemerid pro každou navigační družici. Soubor obsahuje informace o přesné poloze pro každou družici s 24 hodinovým zpožděním. Tyto údaje se používají pro generování simulovaných zdánlivých vzdáleností a Dopplerova posuvu pro navigační družice ve výhledu. Takto simulovaná data jsou následně použita ke generování digitálních I/Q vzorků GPS signálu.

BRDC soubory ve formě RINEX (Receiver Independent Exchange Format) se denně aktualizují a jsou k dispozici v archivu NASA [65]. Soubory v archivu jsou pojmenovány podle následujícího klíče:

- YYYY/DDD/YYn/brdcDDD0.YYn.Z

Tab. 5.3: Značení BRDC souborů

Kód	Význam
YYYY	Rok (2018)
YY	Rok (18)
n	GNSS (n = GPS)
DDD	Pořadové číslo dne v roce
.Z	Komprimovaný unixový soubor

Například soubor brdc1240.18n.Z je soubor efemerid pro GPS navigační družice z 4. května roku 2018.

Soubory je možné stáhnout přímo z konzole použitím FTP protokolu:

```
$ ftp -p cddis.gsfc.nasa.gov
$ 'brdc' + <3 digit day of year> + '0.' +  <2 digit year> + 'n.Z'
```

```
$ date +%j
$ uncompress brdc1240.18n.Z
```

5.3.3 Nastavení generování signálu

Uživatelské možnosti, které jsou k dispozici při generování pomocí GPS-SDR-SIM jsou uvedeny v tabulce Tab. 5.4.

Použití:

```
$ gps-sdr-sim [příkaz]
```

Tab. 5.4: Příkazy GPS-SDR-SIM

Příkaz	Popis	Příklad
-e	odkazuje na BRDC soubor	brdc1240.18n
-u	odkazuje na soubor s pohybem uživatele (dynamický scénář)	Motion.csv
-g	odkazuje na NMEA GGA stream (dynamický scénář)	
-c	odkazuje na ECEF souřadnice v metrech (statický scénář) [X, Y, Z]	4019.618,954.586,4842.933
-l	odkazuje na LLA souřadnice (statický scénář) [šířka, délka, nadmořská výška]	49.723135,13.359265, 390
-t	Začátek simulovaného scénáře [YYYY/MM/DD,hh:mm:ss]	2018/05/01,04:42:42
-T	Přepíše TOC a TEC v navigační zprávě na čas začátku simulovaného scénáře [YYYY/MM/DD,hh:mm:ss]	2018/05/01,04:42:42
-d	délka simulovaného scénáře [s]	statický scénář maximálně 86400 sekund, dynamický scénář maximálně 300 sekund
-o	název výstupního generovaného souboru	defaultně: gpssim.bin
-s	vzorkovací frekvence [Hz]	defaultně: 2600000
-b	formát I/Q dat [1/8/16]	defaultně: 16
-i	vypne ionosférické zpoždění	
-v	zobrazí detaily o simulovaných kanálech	

Příklad příkazu pro generování statického scénáře:

```
$ ./gps-sdr-sim -v -e brdc1240.18n -b 16 -s 2500000 -l
49.723135,13.359265,390
```

Kde:

`-v` zobrazení informací během simulace,
`-e` uvádí se před BRDC souborem,
`-b` 16 bitové I/Q vzorkování z důvodů použití USRP,
`-s` vzorkovací frekvence generovaného souboru,
`-l` generované souřadnice.

5.3.4 Ověření funkčnosti

Generátor byl úspěšně ověřen pro statický a dynamický scénář na následující konfiguraci:

- Softwarově definované rádio – USRP NI 2920
- GPS přijímač – μ-blox EVK-5H se softwarem u-center

Pro generování souboru s digitalizovanými I/Q vzorky GPS signálu byl použit pro statický scénář následující příkaz:

```
$ ./gps-sdr-sim -v -e brdc0043.18n -b 16 -s 2500000 -l
39.043612,125.768733 ,120 -d 1200
```

```
ras@ek709p08-kae:~/Diplomova_prace_Flachs/gps-sdr-sim$ ./gps-sdr-sim -v -e brdc0430.18n -b 16 -s 2500000 -l 39.043612,125.76
8733,120 -d 1200
Using static location mode.
     8.382e-09   -7.451e-09   -5.960e-08    5.960e-08
     8.806e+04   -1.638e+04   -1.966e+05    6.554e+04
    -4.656612873308e-09  -1.33226762955e-14     319488      1988
    18
Start time = 2018/02/12,00:00:00 (1988:86400)
Duration = 1200.0 [sec]
02  156.5   0.2  25325005.5   6.9
05  101.4  33.9  22541224.4   2.8
13   40.9  57.5  20874328.1   1.8
15  312.5  76.0  20093035.8   1.5
20  351.2  76.6  20209198.6   1.5
21  298.2  44.0  22322778.9   2.1
24  184.8  33.1  22375583.3   2.6
28   63.6   4.2  25646968.7   6.0
29  226.4   9.2  24786709.7   4.1
30   35.6   4.5  25290118.5   5.2
Time into run = 30.0
05  101.6  33.8  22555056.0   2.8
13   41.0  57.3  20884811.3   1.8
15  313.5  76.0  20092723.4   1.5
20  352.0  76.8  20205971.2   1.5
21  298.0  44.1  22313157.0   2.1
24  184.8  33.4  22356033.8   2.6
28   63.4   4.2  25641504.5   6.0
29  226.2   9.0  24803639.5   4.1
30   35.5   4.4  25308197.6   5.2
Time into run = 60.0
```

Obr. 5.1: Průběh generování signálu v GPS-SDR-SIM.

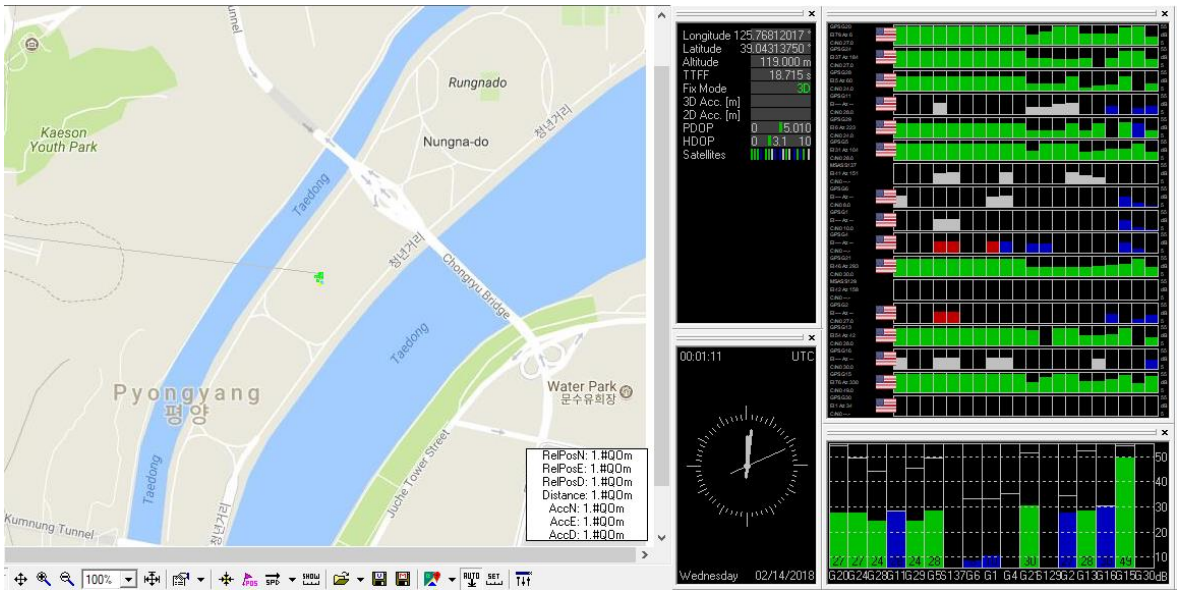
Vygenerovaný soubor gpssim.bin byl následně vysílán pomocí USRP jednotky dalším příkazem:

```
$ python gps-sdr-sim-uhd.py -t gpssim.bin -s 2500000 -f 157542000 -x 0 -c
external
```

Kde možnosti nastavení jsou:

`-t` název souboru k vysílání,
`-s` vzorkovací frekvence USRP jednotky,
`-f` vysílaná frekvence,
`-x` zesílení výstupu USRP,
`-c` zdroj hodinového signálu.

Takto simulovaný a generovaný signál byl vysílán do GPS přijímače od švýcarské společnosti μ-blox EKV-5H s hodnotícím softwarem u-center. Na Obr. 5.2 je vidět, že simulovaný signál byl úspěšně přijat a zpracován přijímačem, kdy čas k prvnímu určení pozice TTFF (Time To First Fix) byl za 18,715 vteřin.



Obr. 5.2: Statický scénář prezentovaný na dni otevřených dveří FEL ZČU.

Pro generování souboru s digitalizovanými I/Q vzorky GPS signálu byl použit pro dynamický scénář následující příkaz:

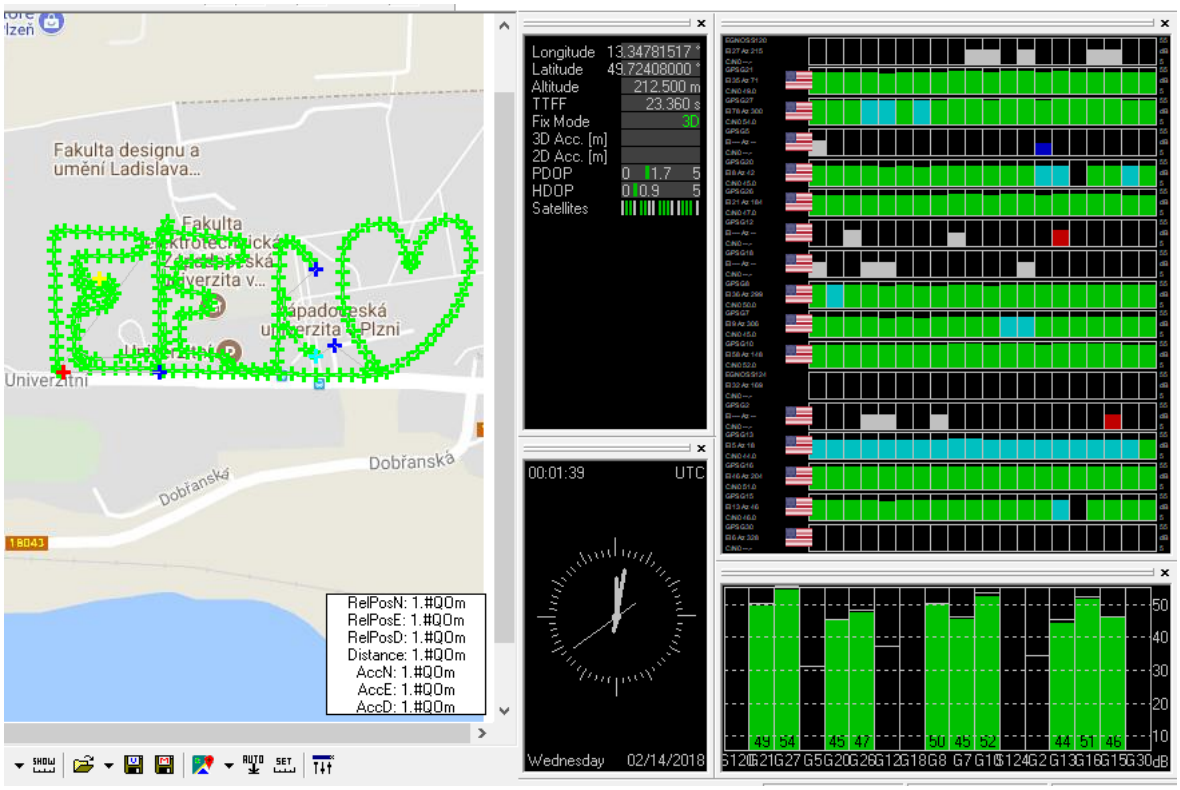
```
$ ./gps-sdr-sim -v -e brdc0043.18n -b 16 -s 2500000 -u FEL.csv -d
```

Kde:

`-u` název souboru trajektorií pohybu.

Soubor s trajektorií pohybu používá k popisu pohybu ECEF souřadnicový systém. Ty je možné získat konverzí NMEA GGA dat ze simulátoru od společnosti LabSat [66].

Takto simulovaný a generovaný signál byl vysílán opět do GPS přijímače μ-blox EKV-5H s hodnotícím softwarem u-center. Na Obr. 5.3 je vidět, že simulovaný signál byl úspěšně přijat a zpracován přijímačem, kdy čas k prvnímu určení pozice TTFF byl za 23,360 vteřin.



Obr. 5.3: Dynamický scénář prezentovaný na dni otevřených dveří FEL ZČU.

Simulátor GPS signálu GPS-SDR-SIM se osvědčil pro oba typy scénáře. Proto bude použit ke generování podvržených signálů ke zjištění chování GPS přijímačů pod spoofing útokem a otestování schopnosti detekovat tyto podvržené signály.

6 Návrh metodiky testování GPS přijímačů na schopnost odhalit podvržené signály

Pro otestování schopnosti GPS přijímačů odhalit podvržený signál jsou navrženy dva scénáře simulující středně obtížný útok, definovaný v kapitole 3.2. V této kapitole je shrnuta jejich realizace, popsáno zapojení pro jednotlivé scénáře a nutné vybavení. V závěru kapitoly jsou představeny testované přijímače.

6.1 Postup testování

Pro účely testování byly vybrány dvě pozice zobrazené na Obr. 6.1 vzdálené od sebe 172 metrů vzdušnou čarou:

- autentická pozice, přijímaná střešní anténou na budově FEL,

Tab. 6.1: Souřadnice skutečné polohy

D° M' S"	49°43'25.617"N	13°20'58.218"E
D° M.mmm'	49°43.431'N	13°20.973'E
D.ddddd°	49.723852°N	13.349543°E

- podvržená pozice, získána z generátoru GPS signálů.

Tab. 6.2: Souřadnice podvržené polohy

D° M' S"	49°43'27.268"N	13°21'6.665"E
D° M.mmm'	49°43.454'N	13°21.111'E
D.ddddd°	49.7242411°N	13.3518514°E

Obr. 6.1: Autentická a podvržená pozice na mapě.

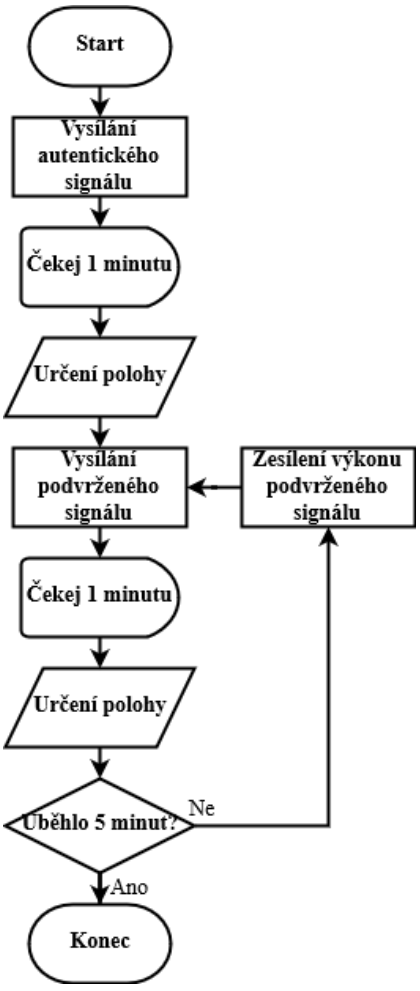
6.1.1 Scénář testování středně obtížného útoku

K testování byly navrženy dva různé scénáře středně obtížného útoku:

- generování podvržených signálů s platnými efemeridy,
- generování podvržených signálů se starými efemeridy.

Princip testování spočívá ve vysílání autentického signálu do prostoru s testovaným GPS přijímačem. Po první minutě se společně s autentickým GPS signálem vysílá generovaný podvržený GPS signál, kterému je každou minutu zvyšován vysílací výkon. Údaje o poloze se z přijímačů vyčte každou minutu. Délka testování je nastavena na pět minut a je celkem třikrát zopakován pro každý přijímač. Vývojový diagram testování scénáře středně obtížného útoku je na Obr. 6.2.

Cílem tohoto testu je testovat schopnost přijímačů odhalit podvržené signály a porovnat chování přijímačů při příjmu podvržených signálů s autentickými efemeridy a podvržených signálů se zastaralými efemeridy.



Obr. 6.2: Vývojový diagram testování.

6.2 Vybavení

6.2.1 USRP N210 a NI USRP 2920

Jednotka softwarově definovaného rádia USRP N210 od společnosti Ettus Research disponuje velkou šířkou pásma a velkým dynamickým rozsahem pro náročné komunikační aplikace. SDR je postaveno na Xilinx Spartan 3A-DSP 3400 FPGA čipu, 100 MS/s A/D převodníku, 400 MS/s D/A převodníku a gigabitovým ethernetem ke spojení s hostitelským počítačem. Jednotka je vybavena WBX kartou, s jedním kanálem pro vysílání signálu a dvěma kanály pro příjem signálu. Parametry WBX karty jsou uvedené v tabulce Tab. 6.3 níže.

Tab. 6.3: Parametry WBX karty

Parametr	Hodnota
Frekvenční rozsah	50 MHz – 2,2 GHz
Zesílení TX/RX	0-25 dB / 0-31,5 dB
Šířka pásma	40 MHz
Rozlišení A/D převodníku	14 bitů
Rozlišení D/A převodníku	16 bitů
Přesnost TCXO	2,5 ppm

Obr. 6.3: USRP N210.

6.2.2 NI USRP-2920

NI USRP-2920 je totožné softwarově definované rádio jako výše popsaná jednotka USRP N210, pouze prodávána pod značkou National Intruments. Jednotka má totožné parametry a disponuje stejnou kartou WBX s parametry uvedené v tabulce Tab. 6.3 výše.

Obr. 6.4: NI USRP-2920.

6.2.3 PicoSync - II

Zdroj přesných synchronizačních signálů. Disponuje interním oscilátorem OCXO a GPS přijímačem. PicoSync - II generuje synchronizační signály 10 MHz a 2,048 MHz. Generované signály mají po 48 hodinovém příjmu GPS signálu přesnost [67]:

- frekvenční přesnost: $1 \cdot 10^{-12}$,
- časová přesnost: <50 ns.

Obr. 6.5: PicoSync – II.

6.2.4 Rozvod GPS signálu

V budově Fakulty elektrotechnické je realizován rozvod GPS signálu určený pro synchronizaci měřících laboratorních přístrojů. GPS signál je přijímán střešní anténou (Obr. 6.6) s vestavěným LNA zesilovačem a typickým ziskem 38 dB. Signál zesílen v selektivním zesilovačem a rozveden do pracovišť.

Obr. 6.6: Střešní GPS anténa.

6.3 Realizace středně obtížného útoku

Pro realizaci tohoto útoku byly použity dvě jednotky softwarově definovaného rádia, zdroj referenčního signálu, střešní GPS anténa jako zdroj autentického signálu a switch na propojení USRP jednotek s PC. Zapojení je uvedené na Obr. 6.7.

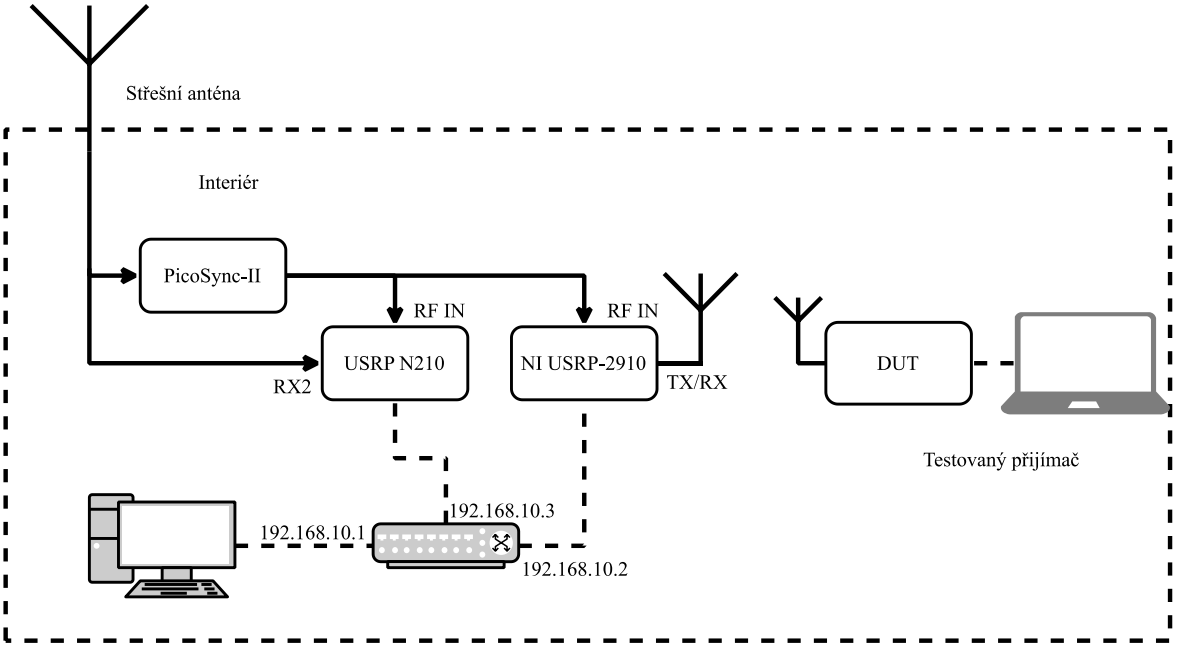
Autentický signál ze střešní antény je pomocí anténního rozvodu přijímán USRP N210 jednotku.

Zároveň je spuštěn softwarově definovaný GNSS přijímač, který jako svoji periférii používá tuto jednotku. Účelem je získání souboru v RINEX formátu s platnými efemeridy, který je nutný k vygenerování souboru s I/Q digitalizovanými vzorky podvrženého GPS signálu.

Ke generování souboru s podvrženým signálem je použit GPS-SDR-SIM generátor. Podvržené souřadnice jsou uvedené v Tab. 6.2.

Přijímaný autentický signál a vygenerovaný signál jsou dále signálově zpracovány v řetězci realizovaném v prostředí GNU Radio Companion a vysílány testovanému zařízení.

6.3.1 Schéma zapojení



Obr. 6.7: Zapojení pro simulaci středně obtížného útoku.

Obr. 6.8: Realizované zapojení.

6.3.2 Získání platných efemerid dat s použitím GNSS-SDR

GNSS-SDR je open-source projekt [68] softwarově definovaného GNSS přijímače implementovaný v jazyce C++. Je realizován v podobě signálových bloků, které uživatel definuje v konfiguračním souboru a implementuje celý řetězec zpracování, od přijímače k řešení navigační úlohy. Umožňuje příjem a zpracování všech globálních navigačních družicových systémů nezávisle na RF front-endu.

V distribucích operačního systému Linux založené na Debianu je možné nainstalovat GNSS-SDR s použitím balíčkovacího systému:

```
$ sudo apt-get install gnss-sdr
```

Nevýhodou tohoto řešení je, že při aktualizaci programu trvá dlouhou dobu, než je nová verze distribuována i do balíčkovacího systému. V případě instalace vždy aktuální verze nebo instalace na jiný typ distribuce je potřeba nejprve nainstalovat všechny závislosti pomocí balíčků:

```
$ sudo apt-get install build-essential cmake git libboost-dev \
   libboost-date-time-dev libboost-system-dev libboost-filesystem-dev \
   libboost-thread-dev libboost-chrono-dev libboost-serialization-dev \
   libboost-program-options-dev libboost-test-dev liblog4cpp5-dev \
   libuhd-dev gnuradio-dev gr-osmosdr libblas-dev liblapack-dev \
   libarmadillo-dev libgflags-dev libgoogle-glog-dev libhdf5-dev \
   libgnutls-openssl-dev libmatio-dev python-mako python-six \
```

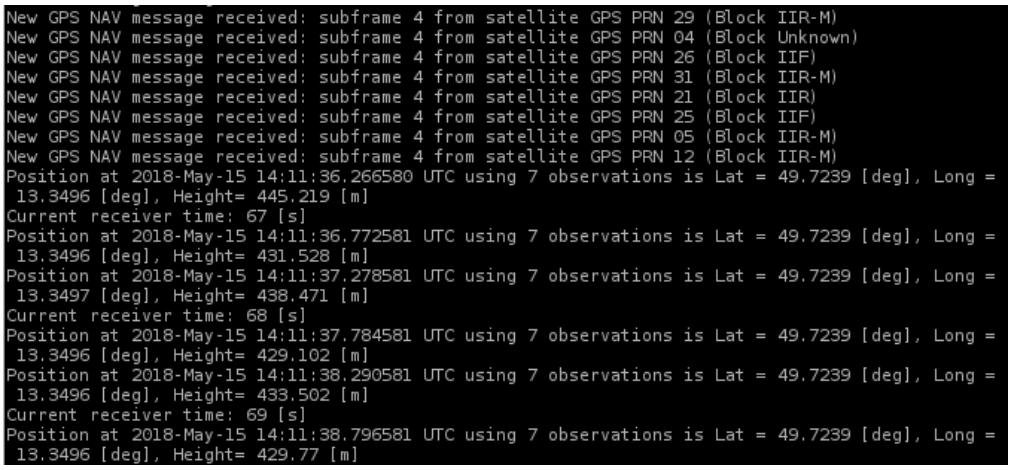
Po nainstalování všech závislostí se může přistoupit k naklonování projektu z depozitáře, kompilaci a instalaci:

```
$ git clone https://github.com/gnss-sdr/gnss-sdr
$ cd gnss-sdr/build
$ git checkout next
$ cmake ..
$ make
$ sudo make install
```

Po úpravě konfiguračního souboru, který je přiložen v příloze B, je možné spustit GNSS-SDR následujícím příkazem:

```
~/Diplomova_prace_Flachs/gps-sdr-sim$ gnss-sdr --config_file=./GNSS-SDR-
realtime.conf
```

Po určení pozice, jak je zachyceno na obrázku Obr. 6.9 je do složky s konfiguračním souborem uložen i soubor ve formátu RINEX s aktuálními efemeridy navigačních družic, jejichž signály byly zpracovány GNSS-SDR.



Obr. 6.9: Výpis programu GNSS-SDR při určení polohy.

6.3.3 Generování simulovaného signálu s použitím GPS-SDR-SIM

Soubor s aktuálními efemeridy získány pomocí GNSS-SDR je použit k vygenerování podvrženého GPS signálu s těmito parametry:

- souřadnice: 49.7242411N, 13.3518514E,
- vzorkovací frekvence: 2,5 MHz,
- 16 bitový formát I/Q dat,
- začátek generovaného scénáře na počátek testování,
- Délka generovaného scénáře 20 minut.

Pro generování je použit následující příkaz, zahrnující výše uvedené parametry:

```
./gps-sdr-sim -v -e GSDR120q6.18N -b 16 -s 2500000 -l 49.723852,
13.359265,390 -d 1200
```

```
Kde:
```

```
GSDR120q6.18N  je výstupní soubor GNSS-SDR.
```

S výsledným souborem, pojmenovaný gpssim.bin o velikosti 12 GB se nadále pracuje v prostředí GNU Radio Companion.

Pro druhou verzi testování s podvrženým signálem s starými efemeridy byl vygenerován soubor se stejnými parametry, pouze s BRDC souborem ze dne 30.1.2018:

```
$ ./gps-sdr-sim -v -e brdc1240.18n -b 16 -s 2500000 -l 49.723852,
13.359265,390 -d 1200
```

6.3.4 Implementace signálového zpracování v GNU Radio

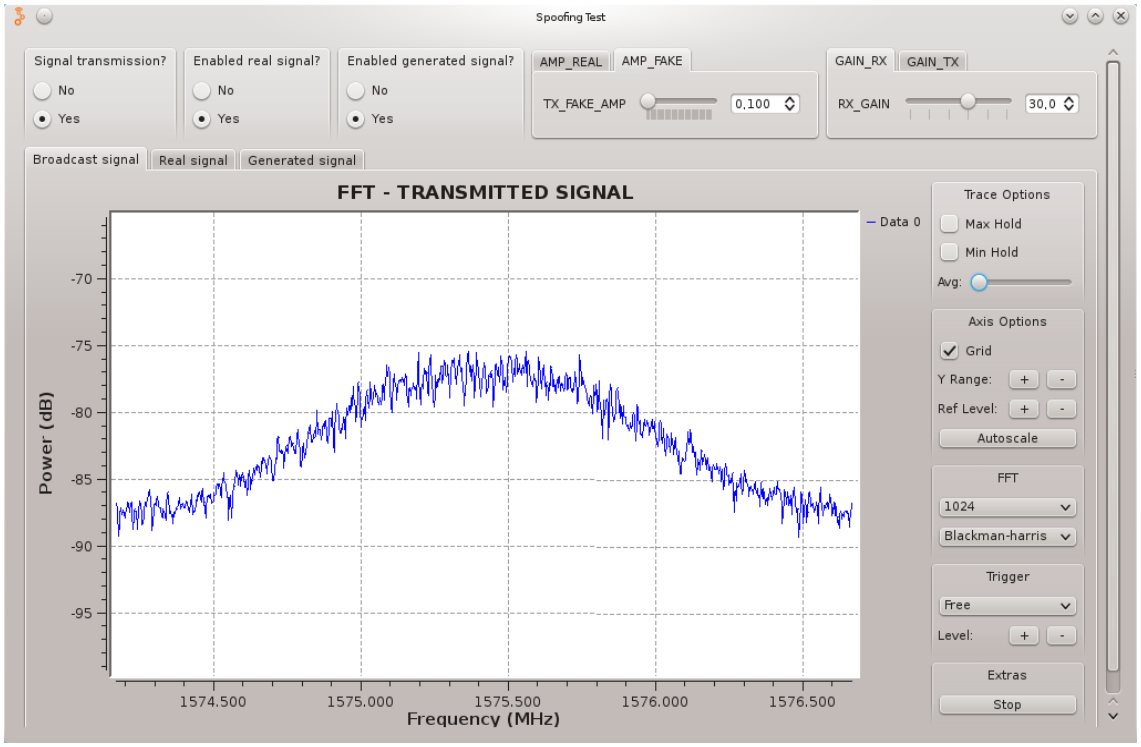
GNU Radio je open-source toolkit [69], který nabízí všechny typické bloky signálového zpracování pro vývoj a implementaci softwarově definovaného rádia. Je možné ho používat v kombinaci s reálným hardwarem nebo jako simulační nástroj.

GNU Radio Companion (GRC) je grafické rozhraní pro tvorbu aplikací v GNU Radio. Je založeno na propojení jednotlivých bloků signálového zpracování, mezi kterými je možné přenášet data. Blokový diagram nazývaný „flowgraph“ je při kompilaci převeden do kódu v pythonu. Ten vytváří požadované GUI prvky a propojení mezi bloky signálového zpracování v blokovém diagramu.

Pro účely testování bylo v GRC realizováno interaktivní ovládání:

- úrovní autentického a podvrženého signálu,
- řízení datového toku signálů,
- nastavení zisku USRP jednotek,
- zobrazení frekvenčního spektra signálů, včetně součtového signálu.

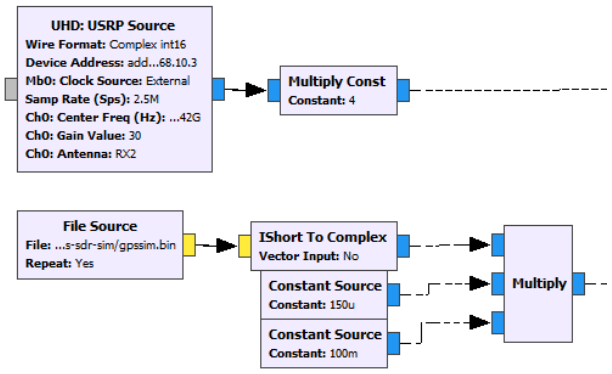
Ve vygenerovaném grafickém prostředí (viz Obr. 6.10) má uživatel možnost zapínat dílčí signály, řídit jejich výkonovou úroveň a zobrazit jejich frekvenční spektrum. Celý blokový diagram je přiložen v příloze C. Dále jsou popsány dílčí části digramu.



Obr. 6.10: Navržené grafické prostředí v GNU Radio.

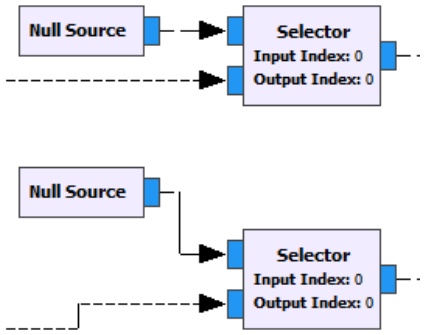
Obr. 6.10 znázorňuje použité zdroje signálu. USRP N210 je nakonfigurován v bloku „UHD: USRP Source“. Výstupním datovým tokem je digitalizovaný autentický signál. Výstupním datovým tokem v případě bloku „File Source“ je generovaný signál. Datové toky signálů jsou pomocí bloku „Multiply“ upraveny vynásobením konstantou z důvodu odlišných

amplitud signálů. V případě autentického signálu je potřeba signál dostatečně zesílit a v případě vygenerovaného signálu naopak je potřeba amplitudu snížit. V případě podvrženého signálu je potřeba provést konverzi datovaného typu dat vygenerovaných GPS-SDR-SIM na typ používaný v rámci signálového zpracování v GNU Radio.



Obr. 6.11: Zdroje signálů a úprava amplitudy.

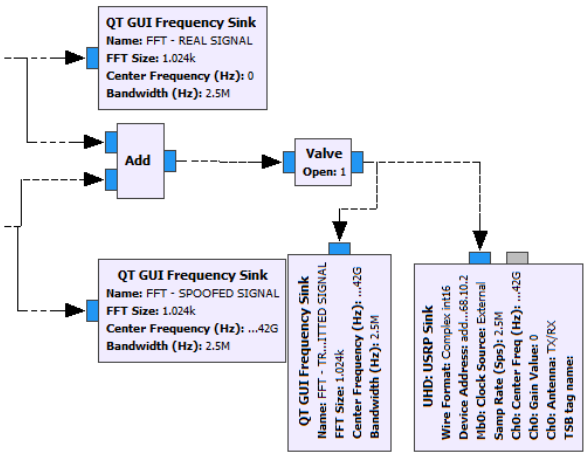
Obr. 6.12 zobrazuje možnost ovládání datového toku ze signálových zdrojů pomocí bloku „Selector“. Ten podle nastavené hodnoty v grafickém prostředí propojí datový tok z požadovaného vstupu na výstup a ostatní porty zůstávají nezapojené. V defaultním stavu je na výstupu datový tok nulových vzorků.



Obr. 6.12: Přepínání zdrojů signálů.

Obr. 6.13 znázorňuje realizaci součtového signálu z autentického a podvrženého signálu v bloku „Add“. Ten sčítá vzorky na všech vstupních datových tocích vzorek po vzorku. Blok „Valve“ funguje na stejném principu jako „Selector“, ale má pouze po jednom vstupním a výstupním portu. Grafický výstup v podobě výkonového spektra je realizován bloky „QT GUI Frequency Sink“. Grafický výstup je pro všechny tři typy signálů. Posledním blokem

v této části je „UHD USRP Sink“. Ten nastavuje parametry NI USRP-2920 jednotky a vstupní datový tok je zařízením odvysílán.



Obr. 6.13: Realizace souštového signálu, vizualizace frekvenčních spekter a vysílání.

6.3.5 Nastavení výkonových úrovní signálů

Hodnoty v dB výkonového spektra realizovaného blokem QT GUI Frequency Sink nejsou vzhledem k podstatě číslicového zpracování signálů založeny na fyzických veličinách. USRP jednotky navíc nemají lineární závislost mezi parametrem zesílení Gain [dB] a výstupním výkonem. Dílčí výkonové úrovně signálů použité při testování byly změřeny na výstupu USRP jednotky spektrálním analyzátorem. Výsledky jsou uvedeny v tabulce Tab. 6.4.

Tab. 6.4: Naměřené výkonové úrovně, středně obtížný útok

Výkonová spektrální hustota [dB]		Naměřená výkonová hustota[dBm]	
P_{au}	P_{gen}	P_{au}	P_{gen}
-75	-	-57,04	-
-75	-80	-57,04	-58,28
-75	-75	-57,04	-57,47
-75	-70	-57,04	-55,32
-75	-65	-57,04	-52,75
-75	-60	-57,04	-46,62
-75	-30	-57,04	-38,13

6.4 Testované přijímače

Pro otestování byla vybrána množina osmi GPS přijímačů, které zastupují tři různé kategorie GPS přijímačů. Evalution kity určené pro výzkum a vývoj. GPS navigace do automobilu a ruční, turistické GPS navigace. Níže jsou uvedeny testované GPS přijímače a v případě dostupnosti podrobnějších informací jsou uvedeny i jejich parametry.

Obr. 6.14: µ-blox AEK-4H.

µ-blox AEK-4H:

- GPS L1 C/A
- 16 kanálů
- Rok výroby: 2006 [70]

Obr. 6.15: µ-blox EVK-5H.

µ-blox EVK-4H:

- GPS L1 C/A
- Galileo L1 OS
- 50 kanálů
  Rok výroby: 2008 [71]

Obr. 6.16: µ-blox EVK-M8N.

µ-blox EVK-M8N:

- GPS L1 C/A
- GLONNAS L1
- Beidou B1
- Galileo E1
- SBAS L1
- QZSS L1
- 72 kanálů
- Rok výroby: 2013 [72]

Obr. 6.17: Kouwell KW-9882.

Kouwell KW-9882:

- GPS L1 C/A
- 12 kanálů
- Rozhraní: COM port
- Rok výroby: 2006

Garmin nüvi 350:

- GPS L1 C/A
- 20 kanálů
- SiRFstarIII
- Rok výroby: 2007 [73]

Obr. 6.18: Garmin nüvi 350.

Garmin nüvi 775t:

- GPS L1 C/A
- 32 kanálů
- MTK v1 3318
- Rok výroby: 2012 [74]

Obr. 6.19: Garmin nüvi 750.

TomTom Start 25:

- GPS L1 C/A
- 24 kanálů
- Broadcom GoGPS Barracuda
- Rok výroby: 2016 [75]

Obr. 6.20: TomTom Start 25.

Mini GPS:

- GPS L1 C/A
- 14 kanálů
- Rok výroby: 2015 [76]

Obr. 6.21: Mini GPS.

Obr. 6.22: Garmin Dakota 20.

Garmin Dakota 20:

- GPS L1 C/A
-
- Rok výroby: 2010 [78]

7 Vyhodnocení testování

7.1 Metodika vyhodnocení

Pro účely vyhodnocení byly určeny tři kategorie přijímačů podle schopnosti odhalit podvržený signál.

- **První kategorie** – přijímač je schopný varovat uživatele při určení podezřelé polohy způsobené příjmem podvržených signálů.
- **Druhá kategorie** – přijímač při příjmu podvržených signálů přestane určovat polohu.
- **Třetí kategorie** – přijímač určí chybně svoji polohu na základě přijímaných podvržených signálů. Za chybnou polohu je považována taková poloha přijímače, která se liší od referenční polohy přijímače o odchylku větší, než je stanovená mez. Ta je nastavena na hodnotu 10 metrů.

Rozdělení přijímačů do těchto kategorií závisí na vyhodnocení výsledků scénáře středně obtížného útoku, popsaného v předchozí kapitole.

Jako referenční poloha k určení odchylek je určena poloha střešní GPS antény, která má jasný výhled na obzor bez jakýchkoliv překážek. Proto je možné předpokládat příjem signálů ze všech viditelných navigačních družic a malou chybu určení polohy.

Pro analýzu výsledků se počítá odchylka poloh v metrech mezi referenční polohou a polohou určenou při příjmu podvržených signálů. Metoda výpočtu vzdálenosti mezi dvěma souřadnicovými body je uvedena v kapitole 7.1.2.

Pro každý přijímač jsou výsledky uvedeny ve dvou tabulkách. První tabulka shrnuje odchylky polohy při příjmu podvržených signálů vygenerovaných z aktuálních efemerid. Druhá tabulka shrnuje odchylky při příjmu podvržených signálů vygenerovaných z neplatných efemerid. Tučně vyznačená odchylka polohy znamená, že odchylka přesáhla stanovený práh a je brána jako důsledek působení podvrženého signálu na přijímač. Pomlčka naznačuje, že poloha přijímače nebyla určena.

Vyhodnocení probíhá na základě sestavení souhrnné tabulky pro všechny přijímače. V tabulce je uveden celkový počet dílčích případů určené polohy. Tedy zda došlo k varování uživatele, určená pozice má odchylku menší nebo větší než 10 metrů anebo zda poloha nebyla určena. Přijímač je zařazen do příslušné kategorie podle toho, jaký případ je převládající.

7.1.1 Přepočet formátu souřadnic

Testované přijímače používají různé formáty zeměpisných souřadnic. Pro účely vzájemného porovnání a výpočtu vzdáleností byly souřadnice převedeny na Stupně° DD.ddddd formát.

Převod formátu Stupně° Minuty' Vteřiny" (D° M' S") na formát Stupně° (D.ddddd°) formát:

$$D.ddddd = D + \left(\frac{M}{60}\right) + \left(\frac{S}{3600}\right). \tag{7.1}$$

Převod formátu Stupně° Minuty' (D° M.mmm') na formát Stupně° (D.ddddd°) formát:

$$D.ddddd = D + \left(\frac{M.mmm}{60}\right). \tag{7.2}$$

7.1.2 Přepočet souřadnic na vzdálenost

Pro určení vzdálenosti mezi dvěma body v prostoru dané souřadnicemi je použit algoritmus „Great Circle“, který využívá většina GPS přijímačů. Algoritmus počítá nejkratší spojnici dvou bodů na kulové ploše s poloměrem Země.

$$d = arcos(\sin(\varphi_1)\sin(\varphi_2) + \cos(\varphi_1)\cos(\varphi_2)\cos(\Delta\lambda))R \tag{7.3}$$

Kde:

φ_1, φ_2 zeměpisná šířka poloh,

$\Delta\lambda$ rozdíl mezi zeměpisnými délkami poloh $\Delta\lambda = \lambda_2 - \lambda_1$,

R poloměr Země na rovníku.

7.2 Výsledky testování scénáře středně obtížného útoku

7.2.1 AEK-4H

Tab. 7.1: AEK-4H, podvržený signál s aktuálnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	-	-	-
-75	-75	180	-	-	-
-75	-70	240	-	-	-
-75	-65	300	-	-	-
-75	-60	360	-	-	**35,7**
-75	-30	420	-	-	**38,0**

Z tabulky Tab. 7.1 je patrné, že přijímač AEK-4H je velmi citlivý na podvržený signál. Od okamžiku, kdy začne přijímat podvržený signál, není schopen určit svoji polohu. Ve dvou ze tří měření přijímač neurčí svoji pozici od okamžiku vysílání podvrženého signálu po konce měření. Ve třetím případě dochází k zajímavému momentu, kdy přijímač určí autentickou polohu i v případě, že generovaný signál má znatelně vyšší výkonovou úroveň než autentický signál.

Tab. 7.2: AEK-4H, podvržený signál se neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	-	-	-
-75	-75	180	-	-	-
-75	-70	240	-	-	-
-75	-65	300	-	-	-
-75	-60	360	-	-	-
-75	-30	420	-	-	-

Z tabulky Tab. 7.2 je patrné, že podvržený signál vygenerovaný s použitím neaktuálních efemerid funguje jako účinný jammer. Přijímač AEK-4H není schopen určit svoji polohu od okamžiku, kdy přijímá takto podvržený signál.

7.2.2 EVK-5H

Tab. 7.3: EVK-5H, podvržený signál s aktuálnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	4,8	7,0	3,8
-75	-75	180	**173,1**	**11,6**	**50,4**
-75	-70	240	**173,4**	-	**67,6**
-75	-65	300	**173,8**	-	**89,6**
-75	-60	360	**173,9**	-	**28,3**
-75	-30	420	**185,4**	-	**156,6**

U přijímače EVK-5H dochází s rostoucí výkonovou úrovní podvrženého signálu k nárůstu interferencí s autentickým signálem a tím i odchylky polohy od referenční. Ve dvou ze tří měření dochází k určení podvržené polohy. Ve třetím případě přijímač není schopen určit svoji polohu od okamžiku, kdy generovaný signál má vyšší výkonovou úroveň než autentický.

Tab. 7.4: EVK-5H, podvržený signál s neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	5,1	7,0	2,1
-75	-75	180	**45,1**	**11,6**	**131,0**
-75	-70	240	**45,1**	-	**62,0**
-75	-65	300	**45,6**	-	**28,8**
-75	-60	360	**45,8**	-	**20,8**
-75	-30	420	**185,4**	-	-

Podvržený signál vygenerovaný s použitím neaktuálních efemerid má vliv na zvětšující se odchylku určení polohy přijímače. V prvním případě dochází při znatelně vyšším výkonové úrovni podvrženého signálu oproti autentickému signálu ke skokové změně určené pozice. Ve druhém případě přijímač přestává určovat svoji polohu. Ve třetím případě dochází ke skokovému určení nesprávné pozice, a i přes zesilující výkonovou úroveň k postupnému zmenšování odchylky a přibližování určené pozice k autentické pozici.

7.2.3 EVK-M8N

Tab. 7.5: EVK-M8N, podvržený signál s aktuálnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	2,6	3,5	6,2
-75	-75	180	**201,1**	1,0	2,2
-75	-70	240	**200,8**	0,7	-
-75	-65	300	**197,1**	1,6	-
-75	-60	360	**194,1**	1,6	**322,5**
-75	-30	420	**191,7**	1,0	**322,4**

Z tabulky Tab. 7.5 je patrné, že s rostoucí výkonovou úrovní podvrženého signálu rostou i interference s autentickým signálem a tím odchylky polohy od referenční. Ve dvou ze tří měření dochází k určení nesprávné polohy. Ve třetím případě přijímač i přes rostoucí výkonovou úroveň podvrženého signálu stále určuje autentickou polohu s odchylkou nepřekračující stanovené meze.

Tab. 7.6: EVK-M8N, podvržený signál s neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	1,8	1,9	1,8
-75	-75	180	1,6	**11,8**	-
-75	-70	240	0,6	3,7	1,3
-75	-65	300	1,1	4,7	2,2
-75	-60	360	0,5	2,8	1,1
-75	-30	420	-	-	-

Vliv podvrženého signálu vygenerovaného s použitím neaktuálních efemerid nemá na přijímač EVK-M8N vliv a odchylka poloh nepřekračuje stanovené meze. Pouze v případě, kdy podvržený signál má znatelně vyšší výkonovou úroveň než autentický signál, dojde k zarušení autentického signálu a přijímač není schopen určit svoji polohu.

7.2.4 Kouwell KW-9882

Tab. 7.7: Kouwell KW-9882, podvržený signál s aktuálnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	-	-	-
-75	-75	180	-	-	-
-75	-70	240	-	**43275,0**	-
-75	-65	300	-	-	-
-75	-60	360	-	-	-
-75	-30	420	**170,2**	-	**388,6**

Přijímač Kouwell KW-9882 v případě příjmu podvrženého signálu s aktuálními efemeridy nedokáže určit autentickou polohu. Ve všech třech měření došlo k určení nesprávné polohy vlivem nekonzistence mezi autentickým signálem a podvrženým signálem.

Tab. 7.8: Kouwell KW-9882, podvržený signál s neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	-	7,5	**36,7**
-75	-75	180	-	1,6	**36,7**
-75	-70	240	-	1,6	**36,7**
-75	-65	300	**202,3**	1,6	**36,7**
-75	-60	360	-	-	**30,9**
-75	-30	420	-	**192,0**	**30,9**

Při příjmu podvrženého signálu se zastaralými efemeridy dojde ve dvou ze tří případů k určení nesprávné polohy. Ve třetím případě GPS přijímač určuje po celou dobu příjmu podvrženého signálu stejnou polohu, vlivem interferencí ale s odchylkou 30 metrů od skutečné polohy.

7.2.5 Garmin nüvi 350

Tab. 7.9: Garmin nüvi 350, podvržený signál s aktuálnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,00	0,00	0,00
-75	-80	120	**66,63**	9,84	**175,03**
-75	-75	180	1,24	**121,08**	1,35
-75	-70	240	4,18	-	**61,82**
-75	-65	300	7,17	-	-
-75	-60	360	3,22	-	-
-75	-30	420	-	**171,03**	-

První testovaná automobilová navigace Garmin nüvi 350 je náchylná na příjem podvrženého signálu. Z tabulky je patrné, že určí nesprávnou pozici ve dvou ze tří měření. Ve třetím měření dochází vlivem nekonzistence mezi podvrženým signálem a autentickým signálem k odchylce od autentické polohy, která překračuje stanovené meze.

Tab. 7.10: Garmin nüvi 350, podvržený signál s neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	8,0	9,2	3,9
-75	-75	180	3,9	**52,1**	2,5
-75	-70	240	3,1	**61,9**	6,4
-75	-65	300	**28,1**	**55,3**	3,4
-75	-60	360	**25,2**	-	3,1
-75	-30	420	-	-	-

Zvyšující se výkonová úroveň podvrženého signálu se zastaralými efemeridy způsobuje u GPS navigace zvětšující se odchylku určení polohy. V případě, kdy podvržený signál má znatelně vyšší výkonovou úroveň než autentický signál, dojde k zarušení autentického signálu a přijímač není schopen určit svoji polohu.

7.2.6 Garmin nüvi 775t

Tab. 7.11: Garmin nüvi 775t, podvržený signál s aktuálními efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,00	0,00	0,00
-75	-80	120	-	0,96	2,20
-75	-75	180	-	3,35	8,70
-75	-70	240	-	3,35	**13,02**
-75	-65	300	-	3,35	**11,51**
-75	-60	360	-	3,35	**29,64**
-75	-30	420	**168,18**	-	-

V tabulce Tab. 7.11 jsou zobrazeny odchylky polohy GPS navigace Garmin nüvi 775t způsobené podvrženým signálem s aktuálními efemeridy. V prvním případě dojde k určení nesprávné polohy při znatelně vyšší výkonové úrovni podvrženého signálu, než má autentický signál. Ve druhém případě V vlivem působení podvrženého signálu přijímač udržuje stále stejnou určenou polohu v době, kdy podvržený signál má znatelně vyšší výkonovou úroveň než autentický signál, dojde k zarušení autentického signálu a přijímač není schopen určit svoji polohu V posledním případě dochází ke zvětšování odchylky vlivem podvrženého signálu do doby, kdy podvržený signál má znatelně vyšší výkonovou úroveň než autentický signál. Dochází k zarušení autentického signálu a přijímač není schopen určit svoji polohu.

Tab. 7.12: Garmin nüvi 775t, podvržený signál s neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	-	2,1	**42,9**
-75	-75	180	9,2	-	**34,7**
-75	-70	240	9,2	-	-
-75	-65	300	8,1	-	-
-75	-60	360	**13,2**	-	**171,2**
-75	-30	420	-	-	-

S rostoucí výkonovou úrovní podvrženého signálu se zvětšuje i odchylka určené pozice. V jednom ze tří měření dojde k určení nesprávné pozice. U ostatních dvou dochází ke zvětšující se odchylce určené polohy a ke ztrátě určené pozice.

7.2.7 TomTom Start 25

Tab. 7.13: TomTom Start 25, podvržený signál s aktuálnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,00	0,00	0,00
-75	-80	120	6,74	-	**54,16**
-75	-75	180	-	-	**52,16**
-75	-70	240	-	-	**52,16**
-75	-65	300	-	-	-
-75	-60	360	-	-	-
-75	-30	420	-	-	-

GPS navigace TomTom start 25 ve dvou případech příjmu podvrženého signálu s aktuálními almanachy ztrácí informace o své poloze po celou dobu trvání testování. Ve třetím případě dojde při příjmu podvrženého signálu k určení polohy s odchylkou 50 metrů. Po zesílení podvrženého signálu přijímač přestává určovat polohu.

Tab. 7.14: TomTom Start 25, podvržený signál s neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	-	**27,8**	**198,2**
-75	-75	180	-	**16,7**	-
-75	-70	240	-	**16,7**	**82,1**
-75	-65	300	-	9,2	**82,1**
-75	-60	360	-	4,1	-
-75	-30	420	-	-	-

Při příjmu podvrženého signálu s neplatnými efemeridy dochází ke zvětšujícím se odchylkám od skutečné polohy. Při znatelně vyšší výkonové úrovni podvrženého signálu GPS přijímač přestává určovat svoji polohu.

7.2.8 Mini GPS

Tab. 7.15: Mini GPS, podvržený signál s aktuálnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,00	0,00	0,00
-75	-80	120	**282,44**	-	6,48
-75	-75	180	**199,63**	-	-
-75	-70	240	-	-	**12,28**
-75	-65	300	-	8,16	3,65
-75	-60	360	-	-	-
-75	-30	420	-	-	-

Jednoduchá turistická GPS navigace v podobě klíčenky při příjmu podvrženého signálu v první případě reaguje skokovým určením nesprávné polohy a při vyšší výkonové úrovni podvrženého signálu dochází ke ztrátě přijímané pozice. V dalších dvou případech dochází ke zvětšující se odchylce určené polohy a při vyšších výkonových úrovní podvrženého signálu zároveň ke ztrátě příjmu signálu.

Tab. 7.16: Mini GPS, podvržený signál s neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	4,8	5,5	0,1
-75	-75	180	7,5	2,1	2,2
-75	-70	240	**63,2**	4,9	2,6
-75	-65	300	-	4,9	0,6
-75	-60	360	-	-	1,8
-75	-30	420	-	-	2,2

Podvržený signál způsobuje rostoucí odchylku od skutečné polohy. Ve dvou ze tří měření přestává GPS přijímač u vyšších výkonových úrovní podvrženého signálu určovat svoji polohu.

7.2.9 Garmin Dakota 20

Tab. 7.17: Garmin Dakota 20, podvržený signál s aktuálnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,00	0,00	0,00
-75	-80	120	-	-	-
-75	-75	180	-	-	-
-75	-70	240	-	-	-
-75	-65	300	-	-	-
-75	-60	360	-	-	-
-75	-30	420	-	-	-

Turistická GPS navigace Garmin Dakota 20 reaguje na podvržený signál tím, že okamžitě přestane určovat svoji polohu. Podvržený signál zde funguje jako kvalitní jammer, který zabraňuje přijímači určit polohu. To platí pro všechny výkonové poměry mezi autentickým a podvrženým signálem a časem měření.

Tab. 7.18: Garmin Dakota 20, podvržený signál s neplatnými efemeridy

Výkon [dB]		Čas [s]	1. měření	2. měření	3. měření
P_{au}	P_{sp}		Odchylka [m]	Odchylka [m]	Odchylka [m]
-75	-	60	0,0	0,0	0,0
-75	-80	120	-	-	-
-75	-75	180	-	-	-
-75	-70	240	-	-	-
-75	-65	300	-	-	-
-75	-60	360	-	-	-
-75	-30	420	-	-	-

Situace se opakuje i při scénář s použitím vygenerovaného signálu se zastaralými efemeridy. Opět zde podvržený signál jako účinný jamming signál a zabraňuje přijímači určit svoji polohu.

7.3 Vyhodnocení testování

Bylo otestováno osm přijímačů, které byly vystaveny útoku vysílání podvrženého signálu. V prvním případě byl k útoku použit podvržený signál vygenerovaný pomocí aktuálních efemerid. Ve druhém případě byl použit signál vygenerovaný pomocí neplatných efemerid. Měření bylo provedeno na šesti různých výkonových poměrech mezi autentickým signálem a podvrženým signálem a bylo celkem třikrát zopakováno.

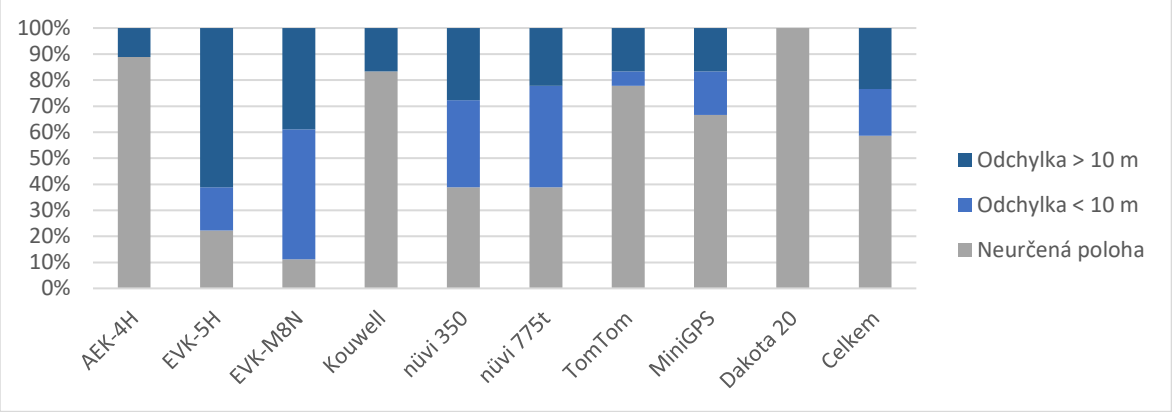
7.3.1 Analýza zdrojů chyb

Na základě analýzy protokolu NMEA a UBX v rámci vyhodnovacího softwaru U-Center použitého pro GPS navigace řady μ-blox lze říci, že:

- Odchylky v řádech metrů – Přijímaný podvržený signál je přijímačem detekován, protože má nereálnou hodnotu pseudovzdálenosti a působí jako zdroj šumu.
- Odchylky v řádech desítkách metrů – Přijímaný podvržený signál ovlivňuje určenou pseudovzdálenost autentických navigačních signálů.
- Odchylky v rozmezí 150–200 metrů – Přijímaný podvržený signál je použit k určení pozice a GPS přijímač začne sledovat i podvržený časový údaj. V tomto případě reálný signál zde působí jako zdroj šumu.
- Odchylky větší než 200 metrů – K výpočtu jsou určeny informace z autentických i podvrženého signálu, což vede k určení chybné a nesmyslné polohy. To se například u GPS přijímače Kouwell KW-9982 při příjmu podvrženého signálu s aktuálními efemeridy.

7.3.2 Vyhodnocení testování podvrženým signálem s aktuálními efemeridy

Shrnutí výsledku testování schopnosti přijímače odhalit podvržený signál v případě použití podvrženého signálu s aktuálními efemeridy je uveden v Tab. 7.19 a na grafu v Obr. 7.1



Obr. 7.1: Souhrn testování podvrženým signálem s aktuálními efemeridy.

Tab. 7.19: Souhrn testování podvrženým signálem s aktuálními efemeridy

Typ přijímače	Celkový počet				
	Varování	Neurčená poloha	Odchylka <10 m	Odchylka> 10 m	Podvržená poloha
AEK-4H	0	16	0	2	0
EVK-5H	0	4	3	11	4
EVK-M8N	0	2	9	7	0
Kouwell	0	15	0	3	1
nüvi 350	0	7	6	5	2
nüvi 775t	0	7	7	4	1
TomTom	0	14	1	3	0
Mini GPS	0	12	3	3	0
Dakota 20	0	18	0	0	0
Celkem	0	95	29	38	8

Při aplikaci rozdělení přijímačů do tří kategorií, definovaných na začátku této kapitoly, lze na základě výsledku testování říct:

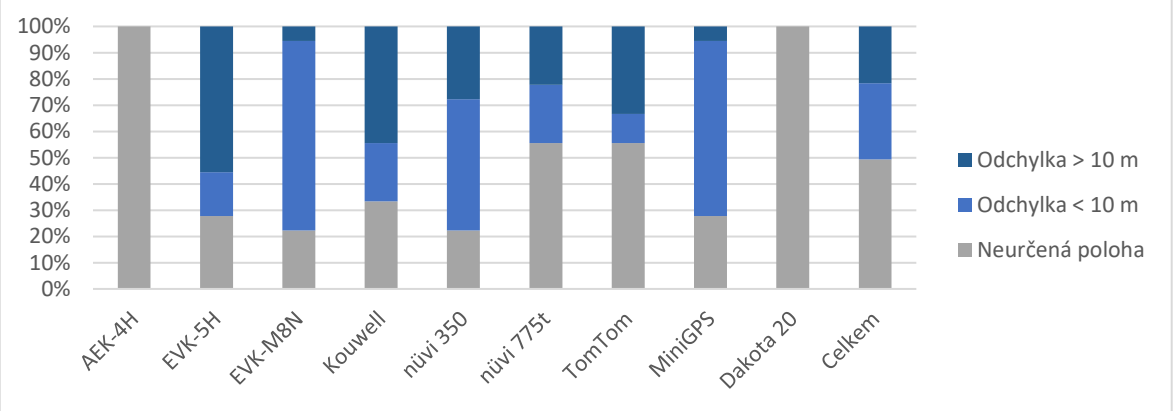
- Žádný z testovaných přijímačů neumožňuje varovat uživatele při určení podezřelé polohy.
- Přijímače μ-blox AEK-4H a Garmin Dakota 20 přestanou určovat polohu při příjmu podvrženého signálu.
- Přijímače Kouwell KW-9882, TomTom Start 25 a Mini GPS přestanou ve většině případů určovat svoji polohu při příjmu podvrženého signálu.
- Přijímače Garmin nüvi 350 a Garmin nüvi 775t jsou při příjmu podvrženého signálu ve většině případů schopny stále určit polohu. Přičemž u určených poloh převládají polohy s odchylkou menší než 10 metrů.
- Přijímač μ-blox EVK-M8N v nadpolovičním případě určil svoji polohu s odchylkou menší než 10 metrů při příjmu podvrženého signálu. Avšak taktéž určil druhý nejvyšší počet poloh s odchylkou větší než 10 metrů.
- Přijímač μ-blox EVK-5H ze všech testovaných přijímačů určil nevyšší počet nesprávných pozic s odchylkou větší než 10 metrů. Zároveň z určených pozic jich nejvíce (4) byla podvrhovaná poloha.

7.3.3 Vyhodnocení testování podvrženým signálem s neplatnými efemeridy

Shrnutí výsledku testování schopnosti přijímače odhalit podvržený signál v případě použití podvrženého signálu s aktuálními efemeridy je uvedeno v tabulce Tab. 2.1 a v grafu Obr. 7.2.

Tab. 7.20: Souhrn testování podvrženým signálem s neplatnými efemeridy

Typ Přijímače	Celkový počet				
	Varování	Neurčená poloha	Odchylka < 10 m	Odchylka > 10 m	Podvržená poloha
AEK-4H	0	18	0	0	0
EVK-5H	0	5	3	10	0
EVK-M8N	0	4	13	1	0
Kouwell	0	6	4	8	0
nüvi 350	0	4	9	5	0
nüvi 775t	0	10	4	4	1
TomTom	0	10	2	6	0
Mini GPS	0	5	12	1	0
Dakota 20	0	18	0	0	0
Celkem	0	80	47	35	1



Obr. 7.2: Souhrn testování podvrženým signálem s neplatnými efemeridy.

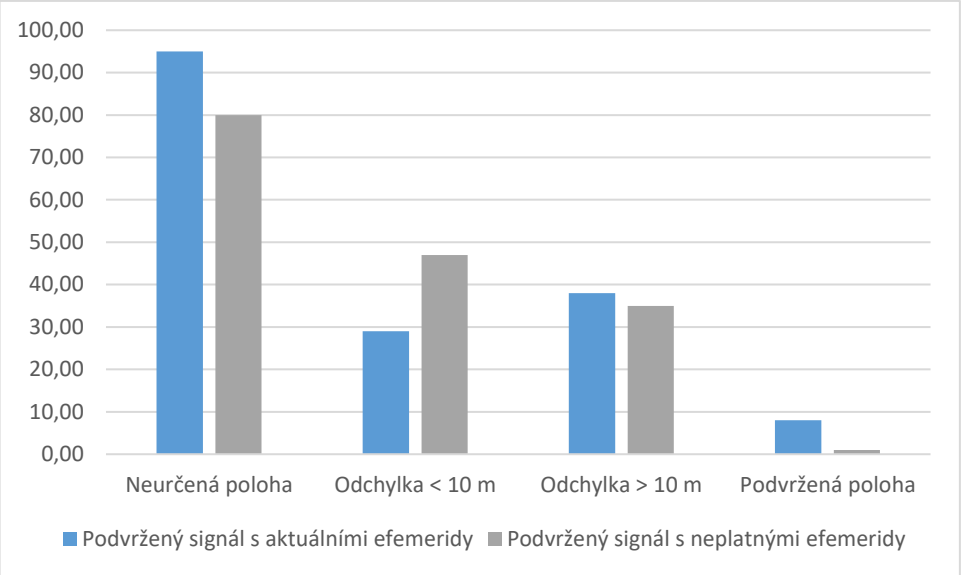
Obdobně jako u vyhodnocení testování podvrženým signálem s neplatnými efemeridy lze na základě výsledku testování říct:

- Žádný z testovaných přijímačů neumožňuje varovat uživatele při určení podezřelé polohy.
- Přijímače µ-blox AEK-4H a Garmin Dakota 20 přestávají při příjmu podvrženého signálu určovat polohu.
- Garmin nüvi 775t a TomTom Start 25 v nadpolovičním případě přestávají při příjmu podvrženého signálu určovat svoji polohu. Přičemž přijímač nüvi 775t je jediný, který určil podvrženou polohu při příjmu signálu s neplatnými efemeridy.
- Přijímače µ-blox EVK-M8N, Garmin nüvi 350, Mini GPS jsou ve většině případů schopny určit svoji polohu.Přičemž u určených poloh převládají polohy s odchylkou menší než 10 metrů.
- Přijímače µ-blox EVK-5H a Kouwell KW-9882 určily polohu v nadpolovičním případě s odchylkou větší než 10 metrů.

7.3.4 Celkové shrnutí výsledků

Graf zobrazený na Obr. 7.3 porovnává testování podvrženým signálem s aktuálními efemeridy a testování podvrženým signálem s neplatnými efemeridy.

Z grafu je patrné, že GPS přijímače jsou méně náchylné na útok podvrženým signálem s neplatnými efemeridy. Přijímače jsou oproti útoku podvrženým signálem s platnými efemeridy schopny častěji určit polohu s odchylkou od referenční polohy menší, než je 10 metrů.



Obr. 7.3: Porovnání dílčích testování.

Příkladem mohou být GPS přijímače Mini GPS a Kouwell KW-9982. Ty při útoku podvrženým signálem s aktuálními efemeridy nebyly schopny určit svoji polohu ve většině případů. Při použití signálu s neplatnými efemeridy dokáže přijímač Mini GPS ve většině případů určit svoji polohu s odchylkou menší než 10 metrů. Naopak přijímač Kouwell KW-9982 je citlivý na rozdílné informace obou signálů a jeho určená pozice má ve většině případů odchylku větší než 10 metrů.

Obecně lze u přijímačů z řady μ-blox říci, že dokáží detekovat podvržený signál a vyřadit ho z výpočtu určení pozice v případě, že určená pseudovzdálenost je nesmyslná.

Zařazení přijímačů na základě jejich chování při spoofing útoku podvrženým signálem s aktuálními efemeridy je uvedeno v tabulce Tab. 7.21. Zařazení přijímačů na základě jejich chování při spoofing úroku podvrženým signálem s neplatnými efemeridy je uvedeno v tabulce Tab. 7.22.

Tab. 7.21: Zařazení GPS přijímačů podle výsledku testování podvrženým signálem s aktuálními efemeridy

První kategorie		-
Druhá kategorie		µ-blox AEK-4H, Kouwell KW-9882, TomTom Start 25, Mini GPS, Garmin Dakota 20
Třetí kategorie	odchylka < 10 m	µ-blox EVK-M8N, Garmin nüvi 350, Garmin nüvi 775t
	odchylka > 10 m	µ-blox EVK-5H

Tab. 7.22: Zařazení GPS přijímačů podle výsledku testování podvrženým signálem s neplatnými efemeridy

První kategorie		-
Druhá kategorie		µ-blox AEK-4H, TomTom Start 25, Garmin Dakota 20, Garmin nüvi 775t
Třetí kategorie	odchylka < 10 m	µ-blox EVK-M8N, Garmin nüvi 350, Mini GPS
	odchylka > 10 m	µ-blox EVK-5H, Kouwell KW-9882

Závěr

Cílem této práce bylo seznámit se s problematikou zranitelnosti GNSS systémů a provést rozbor opatření proti útoku na přijímače GNS signálů. Vybrané možnosti útoků realizovat a porovnat rozdílné přijímače s ohledem na jejich odolnost a schopnost rozpoznat tyto útoky. Pro tyto účely prostudovat existující projekty na generování GNSS signálu a realizovat generátor vybraného systému pomocí softwarově definovaného rádia.

V rámci práce byl proveden rozbor devíti možných opatření proti útoku podvrženým signálem. U všech metod byl rozebrán jejich princip, technické požadavky a očekávaná přesnost. V závěru kapitoly byly metody porovnány dle zadaných kritérií. Bylo zjištěno, že všechny popsané metody jsou schopny odhalit nesofistikovaný útok proti přijímači. Celkem tři metody jsou schopny odhalit i sofistikovaný útok proti přijímači. Vyhodnocení kvality signálu vyžaduje pouze dostatečný výpočetní výkon na straně přijímače, nikoliv nutné zásahy do infrastruktury GPS systému nebo použití rozšiřujícího hardwaru.

Na základě studia zranitelnosti GNSS systémů na podvržený signál byly navrženy dva testovací postupy simulující středně obtížný útok. U prvního testovacího postupu byly s využitím softwarově definovaného GNSS přijímače GNSS-SDR získány aktuální efemeridy. Tyto efemeridy byly následně použity ke generování podvrženého signálu. U druhého postupu byly ke generování použity neplatné efemeridy. Podvržený signál byl vysílán společně s autentickým signálem v různých výkonových poměrech testovanému přijímači.

Podle výsledku testování celkem devíti přijímačů lze konstatovat, že žádný z testovaných přijímačů neumožňuje varovat uživatele v případě určení podezřelé polohy. Při příjmu podvrženého signálu s aktuálními efemeridy bylo na testovaném vzorku GPS přijímačů pozorováno častější určení nesprávné polohy s odchylkou větší než deset metrů a určení podvržené polohy. Také vlivem nekonzistence mezi autentickým signálem a podvrženým signálem došlo častěji k neurčení polohy. Naopak u podvrženého signálu s neplatnými efemeridy je pozorováno častější určení polohy s odchylkou menší než deset metrů.

Problematika zranitelnosti GNSS systémů je velmi aktuální. Proto by bylo přínosné, realizovat simulaci útoku pomocí více zdrojů podvržených signálů a otestovat odolnost a schopnost odhalit podvržené signály i přijímače určené k synchronizaci kritické infrastruktury v podobě telekomunikačních či energetických sítí, protože byla dokázána možnost podvrhnout přijímači i přijímaný časový údaj za zfalšovaný.

Seznam obrázků

Obr. 1.1: Doppletova metoda. Převzato z [1]. 3
Obr. 1.2: Dálkoměrná metoda. Převzato z [3]. 5
Obr. 2.1: Frekvenční spektrum GPS signálů. Převzato ä upraveno z [9]. 12
Obr. 2.2: Blokové schéma generování signálu v pásmech L1 a L2. Převzato z [1]. 13
Obr. 2.3: Generování C/A kódu pro GPS družice. Převzato a upraveno z [5]. 14
Obr. 2.4: Struktura navigační zprávy. Převzato z [5]. 15
Obr. 2.5: Obecný popis navigační zprávy GPS. Převzato z [1]. 16
Obr. 2.6: Eliptická dráha družice. Převzato z [3]. 19
Obr. 3.1: Příklady možných GPS jammerů. Převzato z [25]. 25
Obr. 3.2: Signál jammerů z první skupiny. Převzato a upraveno z [25]. 26
Obr. 3.3: Reklama na osobní rušičku rušící i GPS systém 26
Obr. 3.4: Princip nesofistikovaného útoku. 28
Obr. 3.5: Princip středně obtížného útoku. 28
Obr. 4.1: Rozložení výkonových úrovní. Převzato a upraveno z [44]. 34
Obr. 4.2: Princip Solution Separation RAIM. Převzato a upraveno z [52]. 38
Obr. 5.1: Průběh generování signálu v GPS-SDR-SIM. 46
Obr. 5.2: Statický scénář prezentovaný na dni otevřených dveří FEL ZČU. 47
Obr. 5.3: Dynamický scénář prezentovaný na dni otevřených dveří FEL ZČU. 48
Obr. 6.1: Autentická a podvržená pozice na mapě. 49
Obr. 6.2: Vývojový diagram testování. 50
Obr. 6.3: USRP N210. 51
Obr. 6.4: NI USRP-2920. 52
Obr. 6.5: PicoSync – II. 52
Obr. 6.6: Střešní GPS anténa. 53
Obr. 6.7: Zapojení pro simulaci středně obtížného útoku. 54
Obr. 6.8: Realizované zapojení. 54
Obr. 6.9: Výpis programu GNSS-SDR při určení polohy. 56
Obr. 6.10: Navržené grafické prostředí v GNU Radio. 57
Obr. 6.11: Zdroje signálů a úprava amplitudy. 58
Obr. 6.12: Přepínání zdrojů signálů. 58
Obr. 6.13: Realizace souštového signálu, vizualizace frekvenčních spekter a vysílání. 59
Obr. 6.14: µ-blox AEK-4H. 60
Obr. 6.15: µ-blox EVK-5H. 60

Obr. 6.16: µ-blox EVK-M8N.....60
Obr. 6.17: Kouwell KW-9882. 60
Obr. 6.18: Garmin nüvi 350.....61
Obr. 6.19: Garmin nüvi 750.....61
Obr. 6.20: TomTom Start 25. 61
Obr. 6.21: Mini GPS.....61
Obr. 6.22: Garmin Dakota 20. 62
Obr. 7.1: Souhrn testování podvrženým signálem s aktuálními efemeridy.....74
Obr. 7.2: Souhrn testování podvrženým signálem s neplatnými efemeridy.....76
Obr. 7.3: Porovnání dílčích testování. 77

Seznam tabulek

Tab. 2.1: Přehled navigačních družic. Převzato a upraveno z [8] 10
Tab. 2.2: Přehled frekvencí signálů GPS 11
Tab. 2.3: Generování Goldovy posloupnosti. Převzato z [5] 14
Tab. 2.4: Parametry WGS-84 souřadnicového systému. Převzato a upraveno z [3] 18
Tab. 2.5: Přehled používaných kmitočtů systému Galileo 22
Tab. 2.6: Přehled používaných kmitočtů systému BeiDou - 2 23
Tab. 4.1: Přehled porovnávaných parametrů. Převzato a upraveno z [55] 40
Tab. 4.2: Analýza parametrů protiopatření 41
Tab. 5.1: Komerční hardwarové simulátory GNSS 42
Tab. 5.2: Komerční softwarové GNSS simulátory 43
Tab. 5.3: Značení BRDC souborů 44
Tab. 5.4: Příkazy GPS-SDR-SIM 45
Tab. 6.1: Souřadnice skutečné polohy 49
Tab. 6.2: Souřadnice podvržené polohy 49
Tab. 6.3: Parametry WBX karty 51
Tab. 6.4: Naměřené výkonové úrovně, středně obtížný útok 59
Tab. 7.1: AEK-4H, podvržený signál s aktuálnými efemeridy 65
Tab. 7.2: AEK-4H, podvržený signál se neplatnými efemeridy 65
Tab. 7.3: EVK-5H, podvržený signál s aktuálnými efemeridy 66
Tab. 7.4: EVK-5H, podvržený signál s neplatnými efemeridy 66
Tab. 7.5: EVK-M8N, podvržený signál s aktuálnými efemeridy 67
Tab. 7.6: EVK-M8N, podvržený signál s neplatnými efemeridy 67
Tab. 7.7: Kouwell KW-9882, podvržený signál s aktuálnými efemeridy 68
Tab. 7.8: Kouwell KW-9882, podvržený signál s neplatnými efemeridy 68
Tab. 7.9: Garmin nüvi 350, podvržený signál s aktuálnými efemeridy 69
Tab. 7.10: Garmin nüvi 350, podvržený signál s neplatnými efemeridy 69
Tab. 7.11: Garmin nüvi 775t, podvržený signál s aktuálnými efemeridy 70
Tab. 7.12: Garmin nüvi 775t, podvržený signál s neplatnými efemeridy 70
Tab. 7.13: TomTom Start 25, podvržený signál s aktuálnými efemeridy 71
Tab. 7.14: TomTom Start 25, podvržený signál s neplatnými efemeridy 71
Tab. 7.15: Mini GPS, podvržený signál s aktuálnými efemeridy 72
Tab. 7.16: Mini GPS, podvržený signál s neplatnými efemeridy 72
Tab. 7.17: Garmin Dakota 20, podvržený signál s aktuálnými efemeridy 73

Tab. 7.18: Garmin Dakota 20, podvržený signál s neplatnými efemeridy 73
Tab. 7.19: Souhrn testování podvrženým signálem s aktuálními efemeridy 75
Tab. 7.20: Souhrn testování podvrženým signálem s neplatnými efemeridy 76
Tab. 7.21: Zařazení GPS přijímačů podle výsledku testování podvrženým signálem s aktuálními efemeridy 78
Tab. 7.22: Zařazení GPS přijímačů podle výsledku testování podvrženým signálem s neplatnými efemeridy 78

Seznam literatury a informačních zdrojů

[1] ŠEBESTA, Jiří. *Globální navigační systémy* [online]. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2012 [cit. 2018-03-12]. ISBN 978-80-214-4500-0.

[2] Tsikada. *Encyclopedia Astronautica* [online]. [cit. 2018-03-12]. Dostupné z: http://www.astronautix.com/t/tsikada.html

[3] KOVÁŘ, Pavel. *Družicová navigace: od teorie k aplikací v softwarovém přijímači*. Praha: České vysoké učení technické v Praze, Česká technika – nakladatelství ČVUT, 2016. ISBN 978-80-01-05989-0.

[4] GNSS – Global Navigation Satellite System. *Český kosmický portál* [online]. [cit. 2018-03-12]. Dostupné z: http://www.czechspaceportal.cz/3-sekce/gnss-systemy/gnss-mimo-evropu/americky-navstar-gps/

[5] HRDINA, Zdeněk, Petr PÁNEK a František VEJRAŽKA. *Rádiové určování polohy (Družicový systém GPS)*. Praha: České vysoké učení technické, 1995. ISBN 80-010-1386-3.

[6] GPS Begins. *Time and Navigation* [online]. [cit. 2018-03-31]. Dostupné z: https://timeandnavigation.si.edu/satellite-navigation/gps/gps-begins

[7] Americký družicový navigační systém NAVSTAR GPS. *Český kosmický portál* [online]. [cit. 2018-03-31]. Dostupné z: http://www.czechspaceportal.cz/3-sekce/gnss-systemy/gnss-mimo-evropu/americky-navstar-gps/

[8] *GPS: The Global Positioning System: Official U.S. government information about the Global Positioning System (GPS) and related topics* [online]. [cit. 2018-04-01]. Dostupné z: https://www.gps.gov/systems/gps/

[9] GPS Signal Plan. *ESA navipedia* [online]. [cit. 2018-04-02]. Dostupné z: http://www.navipedia.net/index.php/GPS_Signal_Plan

[10] Navstar GPS Space Segment / Navigation User Interfaces IS_GPS_200G. In: *GPS: The Global Positioning System* [online]. [cit. 2018-04-08]. Dostupné z: https://www.gps.gov/technical/icwg/IS-GPS-200G.pdf

[11] KAPLAN, Elliott; HEGARTY, Christopher. *Understanding GPS: principles and applications*. Artech house, 2005.

[12] GLOBAL POSITIONING SYSTEM / STANDARD POSITIONING SERVICE / SIGNAL SPECIFICATION. In: *GPS: The Global Positioning System* [online]. [cit. 2018-04-09]. Dostupné z: https://www.gps.gov/technical/ps/1995-SPS-signal-specification.pdf

[13] Relation Between GNSS system times and UTC [online]. [cit. 2018-04-09]. Dostupné z: https://www.itu.int/ITUD/tech/events/2012/ResultsWRC12_CIS_StPetersburg_June12/Presentations/Session6/S6_3_b_E.pdf

[14] GPS Modernization. In: *GPS: The Global Positioning System* [online]. [cit. 2018-04-21]. Dostupné z: https://www.gps.gov/systems/gps/modernization/

[15] Constellation status. In: *Information analytical centre of GLONASS and GPS controlling* [online]. [cit. 2018-04-21]. Dostupné z: https://www.glonass-iac.ru/en/GLONASS/index.php

[16] Constellation Information. In: *European GNSS Service Centre* [online]. [cit. 2018-04-21]. Dostupné z: https://www.gsc-europa.eu/system-status/Constellation-Information

[17] GLOBAL NAVIGATION SATTELITE SYSTEM GLONASS INTERFACE CONTROL DOCUMENT: Navigational radiosignal In bands L1, L2 (Edition 5.1). In: *University of New Brunswick | UNB* [online]. [cit. 2018-04-22]. Dostupné z: http://gauss.gge.unb.ca/GLONASS.ICD.pdf

[18] European GNSS (Galileo) Open Service, Signal In Space Interface Control Document. In: *European GNSS Service Centre* [online]. [cit. 2018-04-22]. Dostupné z: https://www.gsc-europa.eu/system/files/galileo_documents/Galileo-OS-SIS-ICD.pdf

[19] BEIDOU constellation status. In: Information analytical centre of GLONASS and GPS controlling [online]. [cit. 2018-04-22]. Dostupné z: https://www.glonass-iac.ru/en/BEIDOU/

[20] BEIDOU GLOBAL NAVIGATION SATELLITE SYSTEM. In: *Information analytical centre of GLONASS and GPS controlling* [online]. [cit. 2018-04-22]. Dostupné z: https://www.glonass-iac.ru/en/guide/beidou.php

[21] BeiDou Navigation Satellite System Signal In Space Interface Control Document: Open Service Signal (Version 2 .0). In: *University of New Brunswick | UNB* [online]. [cit. 2018-04-22]. Dostupné z: http://www2.unb.ca/gge/Resources/beidou_icd_english_ver2.0.pdf

[22] The entire global financial system depends on GPS, and it's shockingly vulnerable to attack. In: *QUARTZ* [online]. [cit. 2018-04-27]. Dostupné z: https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/

[23] PRIORITIZING DANGERS TO THE UNITED STATES FROM THREATS TO GPS: Ranking Risks and Proposed Mitigations. In: *The Resilient Navigation and Timing Foundation* [online]. 2016 [cit. 2018-04-27]. Dostupné z: https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf

[24] INFRASTRUCTURE, Transportation. *Vulnerability assessment of the transportation infrastructure relying on the global positioning system*. Technical Report, Center, John A. Volpe National Transportation Systems, 2001.

[25] MITCH, Ryan H., et al. Signal characteristics of civil GPS jammers. In: Proceedings of ION GNSS. 2011. p. 20-23.

[26] SEO, Jiwon; KIM, Mincheol. eLoran in Korea—Current status and future plans. In: *European Navigation Conference, ENC*. 2013. p. 23-25.

[27] Russian Exercise Jams Aircraft GPS in North Norway for a Week – NRK. In: *Resilient Navigation and Timing Foundation* [online]. 2017 [cit. 2018-04-29]. Dostupné z: https://rntfnd.org/2017/10/05/russian-exercise-jams-aircraft-gps-in-north-norway-for-a-week-nrk/

[28] Russian Electronic Warfare in Ukraine: Between Real and Imaginable. In: *The Jamestown Foundation* [online]. 2017 [cit. 2018-04-29]. Dostupné z: https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/

[29] *Russia Jamming GPS in Syria to Counter US Drones – NBC News* [online]. In: . 2018 [cit. 2018-04-29]. Dostupné z: https://rntfnd.org/2018/04/11/russia-jamming-gps-in-syria-to-counter-us-drones-nbc-news/

[30] USAF Is Jamming GPS In The Western U.S. For Largest Ever Red Flag Air War Exercise. In: *The Drive - Automotive News, Car Reviews and Car Tech* [online]. 2018 [cit. 2018-04-29]. Dostupné z: http://www.thedrive.com/the-war-zone/17987/usaf-is-jamming-gps-in-the-western-u-s-for-largest-ever-red-flag-air-war-exercise

[31] FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS: Jamming events continue — an average of five per day at EWR. In: *Inside GNSS | Engineering Solutions from the Global Navigation Satellite System Community* [online]. [cit. 2018-04-29]. Dostupné z: http://www.insidegnss.com/node/3676

[32] Jamming GPS Signals Is Illegal, Dangerous, Cheap, and Easy. In: *Gizmodo - We come from the future* [online]. [cit. 2018-04-29]. Dostupné z: https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955

[33] Thousands using GPS jammers on UK roads pose risks, say experts. In: *The Guardian* [online]. 2013 [cit. 2018-04-29]. Dostupné z: https://www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks

[34] HUMPHREYS, Todd E., et al. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In: *Proceedings of the ION GNSS international technical meeting of the satellite division*. 2008. p. 56.

[35] Reports Say U.S. Drone was Hijacked by Iran Through GPS Spoofing. In: *Information Security News, IT Security News and Cybersecurity Insights: SecurityWeek* [online]. 2011 [cit. 2018-05-01]. Dostupné z: https://www.securityweek.com/reports-say-us-drone-was-hijacked-iran-through-gps-spoofing

[36] Getting lost near the Kremlin? Russia could be 'GPS spoofing'. In: *Tech News - CNN Tech* [online]. 2016 [cit. 2018-04-30]. Dostupné z: http://money.cnn.com/2016/12/02/technology/kremlin-gps-signals/index.html

[37] Mass GPS Spoofing Attack in Black Sea?. In: *The Maritime Executive: Maritime News | Marine News* [online]. 2017 [cit. 2018-04-30]. Dostupné z: https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#gs.QAoFdzo

[38] GPS Spoofing Experiment Knocks Ship off Course. In: Inside GNSS: Engineering Solutions from the Global Navigation Satellite System Community [online]. 2013 [cit. 2018-04-30]. Dostupné z: http://www.insidegnss.com/node/3659

[39] KERNS, Andrew J., Daniel P. SHEPARD, Jahshan A. BHATTI a Todd E. HUMPHREYS. Unmanned Aircraft Capture and Control Via GPS Spoofing. *Journal of Field Robotics* [online]. 2014, **31**(4), 617-636. DOI: 10.1002/rob.21513. ISSN 15564959. Dostupné také z: http://doi.wiley.com/10.1002/rob.21513

[40] WARNER, Jon S.; JOHNSTON, Roger G. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *Journal of Security Administration*, 2002, 25.2: 19-27.

[41] Spoofing Incident Report: An Illustration of Cascading Security Failure. In: *Inside GNSS: Engineering Solutions from the Global Navigation Satellite System Community* [online]. 2017 [cit. 2018-04-30]. Dostupné z: http://insidegnss.com/node/5661

[42] WARNER, Jon S.; JOHNSTON, Roger G. GPS spoofing countermeasures. Homeland Security Journal, 2003, 25.2: 19-27.

[43] JOVANOVIC, Aleksandar, Cyril BOTTERON a Pierre-Andre FARINE. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers. In: *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014* [online]. IEEE, 2014, 2014, s. 1258-1271 [cit. 2018-05-04]. DOI: 10.1109/PLANS.2014.6851501. ISBN 978-1-4799-3320-4. ISSN 2153-3598. Dostupné z: http://ieeexplore.ieee.org/document/6851501/

[44] KUHN, Markus G. An Asymmetric Security Mechanism for Navigation Signals. *Information Hiding: 6th International Workshop on Information Hiding* [online]. Toronto, Canada: Springer, 2004, 2004, , 239-252 [cit. 2018-05-03]. Lecture Notes in Computer Science. DOI: 10.1007/978-3-540-30114-1_17. ISBN 978-3-540-24207-9. Dostupné z: http://link.springer.com/10.1007/978-3-540-30114-1_17

[45] SHEPARD, Daniel P., Todd E. HUMPHREYS a Aaron A. FANSLER. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*. 2012, **5**(3-4), 146-153. DOI: 10.1016/j.ijcip.2012.09.003. ISSN 18745482. Dostupné také z: http://linkinghub.elsevier.com/retrieve/pii/S1874548212000480

[46] FAN, Yawen, Zhenghao ZHANG, Matthew TRINKLE, Aleksandar D. DIMITROVSKI, Ju Bin SONG a Husheng LI. A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids. *IEEE Transactions on Smart Grid*. 2015, **6**(6), 2659-2668. DOI: 10.1109/TSG.2014.2346088. ISSN 1949-3053. Dostupné také z: http://ieeexplore.ieee.org/document/6887343/

[47] MAGIERA, J. a R. KATULSKI. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *Journal of Applied Research and Technology*. 2015, **13**(1), 45-57. DOI: 10.1016/S1665-6423(15)30004-3. ISSN 16656423. Dostupné také z: http://linkinghub.elsevier.com/retrieve/pii/S1665642315300043

[48] PSIAKI, Mark L., Brady W. O'HANLON, Jahshan A. BHATTI, Daniel P. SHEPARD a Todd E. HUMPHREYS. GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals. In: *IEEE Transactions on Aerospace and Electronic Systems*. 2013, **49**(4), s. 2250-2267. DOI: 10.1109/TAES.2013.6621814. ISSN 0018-9251. Dostupné také z: http://ieeexplore.ieee.org/document/6621814/

[49] HU, Yanfeng, Shaofeng BIAN, Kejin CAO a Bing JI. GNSS spoofing detection based on new signal quality assessment model. *GPS Solutions*. 2018, **22**(1), -. DOI: 10.1007/s10291-017-0693-7. ISSN 1080-5370. Dostupné také z: http://link.springer.com/10.1007/s10291-017-0693-7

[50] JAFARNIA-JAHROMI, Ali, Ali BROUMANDAN, John NIELSEN a Gérard LACHAPELLE. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation*. 2012, **2012**, 1-16. DOI: 10.1155/2012/127072. ISSN 1687-5990. Dostupné také z: https://www.hindawi.com/archive/2012/127072/

[51] 2008 Federal Radionavigation Plan. In: *U.S. Coast Guard Navigation Center* [online]. Department of Defense, Department of Homeland Security, and Department of Transportation, 2008 [cit. 2018-05-07]. Dostupné z: https://www.navcen.uscg.gov/pdf/2008_Federal_Radionavigation_Plan.pdf

[52] GROVES, Paul D. *Principles of GNSS, inertial, and multisensor integrated navigation systems*. Boston: Artech House, 2008. ISBN 978-1-58053-255-6.

[53] WANG, Ershen, Ming CAI a Tao PANG. A Simple and Effective GPS Receiver Autonomous Integrity Monitoring and Fault Isolation Approach. In: *2012 International Conference on Control Engineering and Communication Technology*. IEEE, 2012, 2012, s. 657-660. DOI: 10.1109/ICCECT.2012.145. ISBN 978-1-4673-4499-9. Dostupné také z: http://ieeexplore.ieee.org/document/6414449/

[54] KHANAFSEH, Samer, Naeem ROSHAN, Steven LANGEL, Fang-Cheng CHAN, Mathieu JOERGER a Boris PERVAN. GPS spoofing detection using RAIM with INS coupling. *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*. IEEE, 2014, 2014, , 1232-1239. DOI: 10.1109/PLANS.2014.6851498. ISBN 978-1-4799-3320-4. Dostupné také z: http://ieeexplore.ieee.org/document/6851498/

[55] HAIDER, Zeeshan a Shehzad KHALID. Survey on effective GPS spoofing countermeasures. In: *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*. IEEE, 2016, 2016, s. 573-577. DOI: 10.1109/INTECH.2016.7845038. ISBN 978-1-5090-2000-3. Dostupné také z: http://ieeexplore.ieee.org/document/7845038/

[56] 2018 Simulator Buyers Guide. In: *GPS World* [online]. [cit. 2018-05-12]. Dostupné z: http://gpsworld.com/2018-simulator-buyers-guide/

[57] GNSS Simulator for the R&S®SMBV100A Vector Signal Generator. In: *Rohde & Schwarz* [online]. [cit. 2018-05-12]. Dostupné z: https://www.rohde-schwarz.com/us/product/gnss-powerslave_63491-11461.html?rusprivacypolicy=0

[58] SDX GPS/GNSS Simulator Specifications - Skydel. In: *Software-defined GNSS simulator (GPS - Galileo - GLONASS - BeiDou) - Home - Skydel* [online]. [cit. 2018-05-12]. Dostupné z: https://www.skydelsolutions.com/en/products/sdx/specifications/

[59] LabSat 3 GNSS Simulator User Manual. In: *Commercial GPS | Military GPS | GPS Networking | NavtechGPS* [online]. [cit. 2018-05-12]. Dostupné z: https://www.navtechgps.com/assets/1/7/Labsat_3_Manual.pdf

[60] NAVSYS | GNSS Signal Architect Toolbox. In: *NAVSYS Corporation - GNSS and Inertial Systems, Receivers and Signal Processing* [online]. [cit. 2018-05-12]. Dostupné z: http://www.navsys.com/products/signal_architect_toolbox.htm

[61] GNSS Simulation Toolkit 3.0. In: *National Instruments: Testovací, měřicí a integrované systémy - National Instruments* [online]. [cit. 2018-05-12]. Dostupné z: http://www.ni.com/download/gnss-simulation-toolkit-3.0/3717/en/

[62] Software-Defined GPS Signal Simulator. *The world's leading software development platform · GitHub* [online]. [cit. 2018-05-12]. Dostupné z: https://github.com/osqzss/gps-sdr-sim

[63] A GPS simulator. *The world's leading software development platform · GitHub* [online]. [cit. 2018-05-12]. Dostupné z: https://github.com/sywcxx/gps-sim

[64] HUANG, Lin a Qing YANG. GPS SPOOFING. In: *DEF CON® Hacking Conference* [online]. 2015 [cit. 2018-05-12]. Dostupné z: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf

[65] *CDDIS | | Data and Derived Products | GNSS | broadcast ephemeris data* [online]. [cit. 2018-05-12]. Dostupné z: https://cddis.nasa.gov/Data_and_Derived_Products/GNSS/broadcast_ephemeris_data.html

[66] Free GPS NMEA Simulator software. *LabSat GPS/GNSS Simulator - Home* [online]. [cit. 2018-05-12]. Dostupné z: https://www.labsat.co.uk/index.php/en/free-gps-nmea-simulator-software

[67] PICOSYNC-II GPS ENGINE. In: *Network Synchronization Experts | Gillam-Fei* [online]. [cit. 2018-05-12]. Dostupné z: http://www.gillam.be/files/uploads/2013/08/Leaflet-PICOSYNC-II-GPS-ENGINE.pdf

[68] Quick-Start Guide - GNSS-SDR. *GNSS-SDR* [online]. [cit. 2018-05-12]. Dostupné z: https://gnss-sdr.org/quick-start-guide/

[69] About GNU Radio. *GNU Radio* [online]. [cit. 2018-05-12]. Dostupné z: https://gnuradio.org/about/

[70] LEA-4 ANTARIS ® 4 GPS Modules Data Sheet. In: *Universidad Tecnológica Nacional* [online]. [cit. 2018-05-13]. Dostupné z: http://www.investigacion.frc.utn.edu.ar/sensores/Equipamiento/gps/LEA-4x_Data_Sheet(GPS.G4-MS4-06143).pdf

[71] LEA - 5 u - blox 5 GPS Modules Data Sheet. In: *AmoBBS* [online]. [cit. 2018-05-13]. Dostupné z: http://d1.amobbs.com/bbs_upload782111/files_33/ourdev_581165TSVA0S.pdf

[72] NEO - M8 u - blox M8 concurrent GNSS modules Data Sheet. In: *M-blox* [online]. [cit. 2018-05-13]. Dostupné z: https://www.µ-blox.com/sites/default/files/NEO-M8_DataSheet_(UBX-13003366).pdf

[73] SiRFstarIII GSC3e/LP & GSC3f/LP. In: *SymmetryElectronics.com* [online]. [cit. 2018-05-13]. Dostupné z: http://www.semiconductorstore.com/pdf/newsite/sirf/gsc3lpx_pb.pdf

[74] Garmin nuvi 775T. *Špičkové navigace amerického výrobce Garmin - Garmin Česká republika* [online]. [cit. 2018-05-13]. Dostupné z: https://www.garmin.cz/garmin-nuvi-775t/5298

[75] BCM4750 Product Brief. In: *MILEDROPEDIA* [online]. [cit. 2018-05-13]. Dostupné z: http://www.droid-developers.org/images/e/e5/BCM4750.pdf

[76] Mini GPS lokátor PG03 - na klíče. In: *H A D E X , spol. s r.o.* [online]. [cit. 2018-05-13]. Dostupné z: http://www.hadex.cz/navody/v187.pdf

[77] Garmin Dakota 20. *Špičkové navigace amerického výrobce Garmin - Garmin Česká republika* [online]. [cit. 2018-05-13]. Dostupné z: https://www.garmin.cz/garmin-dakota-20/9322

Seznam zkratek

AOA	Angle of Arrival
A-S	Anti-Spoofing
C/A	Coarse/Acquisition
CDMA	Code Division Multiple Access
CS	Commercial Service
DOA	Direction of Arrival
DOD	Doppler Offset Detector
ECEF	Earth centered, Earth fixed
ECI	Earth-centered inertial
ESA	Evropská kosmická agentura
FDMA	Frequency Division Multiple Access
FOC	Final Operation Capability
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPS	Global Position System
GPST	Global Position System Time
GRC	GNU Radio Companion
GTRF	Galileo Terrestrial Reference Frame
HP	High Positioning
IOC	Initial Operational Capability
OCX	Next Generation Operational Control System
OS	Open Service

PMU	Phasor Measurement Unit
PPS	Precision Position Service
PRN	Pseudo Random Noise
PRS	Public Regulated Service
PTD	Power Treshold Detector
PVT	Position, Velocity, Time
RAIM	Receiver Autonomous Integrity Monitoring
RINEX	Receiver Independent Exchange Format
S/A	Selective Availability
SAR	Search and Rescue service
SCT	GNSS Signal Consistency Tests
SDR	Software Defined Radio
SoL	Safety of Life Service
SP	Standard Positioning
SPS	Standard Position Service
SVN	Space vehicle Number
TTFF	Time To First Fix
WGS-84	World Geodetic System
XYZ	Kartézská souřadnicová soustava

Seznam symbolů

$\boldsymbol{a}_m$, $\boldsymbol{b}$	řídící vektory
$a_{x,k}$, $a_{y,k}$, $a_{z,k}$	směrové kosiny jednotkového vektoru
C(t)	civilní C/A kód
c	rychlost šíření signálu
$\widehat{\boldsymbol{d}}_m^{au}$	směrový jednotkový vektor z počátku ke k m-té navigační družici, zdroji autentických signálů
$\widehat{\boldsymbol{d}}^{sp}$	směrový jednotkový vektor z počátku ke zdroji podvržených signálů
N_{au}	počet autentických pseudonáhodných signálů
N_{sp}	počet podvržených pseudonáhodných signálů
T_s	vzorkovací perioda
$c(nT_s)$	pseudonáhodná sekvence v okamžiku T_s
$c(nT_s)$	pseudonáhodná sekvence v okamžiku T_s
D(t)	navigační zpráva družice
d_i	vzdálenost časové značky
$t_{r,k}$	čas odvysílání časové značky k-tou družicí
$t_{t,k}$	doba příjmu časové značky k-té družice
$\boldsymbol{d}_{i1}^{ant}$	směrový vektor z počátku (fázový centrum referenční antény) k fázovému středu i-té antény
f	dopplerova frekvence nosné vlny
f_0	kmitočet místního oscilátoru
f_p	kmitočet nosné vlny v době příjmu
f_v	kmitočet nosné vlny v době vysílání

$h(nT_s)$	vysílaná data navigační zprávy v okamžiku T_s
H	matice směrových kosinů
n	komplexní přídavný bílý Gaussovský šum s odchylkou σ^2
N_i	počet period
p	přijímaný výkon
P(t)	autorizovaný P(Y) kód
r_k	vzdálenost mezi i-tou družicí a přijímačem
T	doba, perioda
t_i	časový okamžik
W	diagonální matice
x_i, y_i, z_i	poloha i-té družice v kartézském souřadném systému
x_u, y_u, z_u	poloha uživatele v kartézském souřadném systému
ρ_k	změřená pseudovzdálenost k navigačním družici
τ_{di}	doba šíření signálu na trase d_i
ΔΦ	fázový rozdíl
ϑ_i	elevační úhel
λ	vlnová délka
Δx	vektor neznámých
Δρ	vektor odchylek pseudovzdáleností
τ	časový posun kódu přijímaného signálu
ϕ	fáze nosné vlny
$\boldsymbol{\eta}$	Nx1 komplexní přídavný bílý Gaussovský šum

Přílohy

Příloha A: Obsah navigační zprávy

Tab. A.1: Popis parametrů v prvním podrámci. Převzato a upraveno z [12]

Parametr	Počet bitů	Rozsah	Jednotka
n_W	10	0-1023	týden
Kód na L_2	2	-	-
Přesnost	4	0-15	-
Stav	6	-	-
IODC	10	0-1023	-
L_2	1	-	-
T_{GD}	8	$\pm 6 \cdot 10^{-8}$	s
t_{OC}	16	0-604784	s
α_{f2}	8	$\pm 3{,}6 \cdot 10^{-15}$	s^{-1}
α_{f1}	16	$\pm 3{,}7 \cdot 10^{-9}$	-
α_{f0}	22	$\pm 9{,}8 \cdot 10^{-4}$	s

Kde význam jednotlivých parametrů prvního podrámce jsou následující:

- n_W udává pořadí GPS týdne od půlnoci ze soboty na neděli 5. ledna 1980.
- Kód na L_2 udává jaký kód je vysílán na pásmu L2.
- Přesnost charakterizuje přesnost určení mezi družicí a uživatelem v důsledku chyby družice.
- Stav neboli zdraví vyjadřuje kvalitu nosných frekvencí a modulace daty.
- IODC (Issue of Data, Clock) určuje počet provedených změn v obsahu prvního podrámce.
- L_2 v případě nenulové hodnoty indikuje, že P kód v pásmu L2 neobsahuje žádné informace.
- T_{GD} obsahuje korekce skupinového zpoždění signálu v pásmu L1, který lze použít pro korekci ionosférického zpoždění v případě příjmu jen v jednom pásmu.
- t_{OC} je vztažný čas koeficientů časové základny družice.
- α_{f2}, α_{f1}, α_{f0} jsou koeficienty časové základny družice.

Tab. A.2: Popis parametrů druhého a třetího podrámce. Převzato a upraveno z [12]

Parametr	Počet bitů	Rozsah	Jednotka
IODE	8	-	-
C_{rs}	16	±1024	m
Δn	16	$\pm 3{,}7 \cdot 10^{-9}$	$sc \cdot s^{-1}$
M_0	32	±1	sc
C_{uc}	16	$\pm 6{,}1 \cdot 10^{-5}$	rad
e	32	0-0,5	-
C_{us}	16	$\pm 6{,}1 \cdot 10^{-5}$	rad
$\sqrt{A}$	32	0-8192	$m^{1/2}$
t_{oe}	16	0-604784	s
Interval	1	-	-
C_{ic}	16	$\pm 6{,}1 \cdot 10^{-5}$	rad
Ω_o	32	±1	sc
C_{is}	16	$\pm 6{,}1 \cdot 10^{-5}$	rad
i_0	32	±1	sc
C_{rc}	16	±1024	m
ω	32	±1	sc
$\dot{\Omega}$	24	$\pm 9{,}5 \cdot 10^{-7}$	$sc \cdot s^{-1}$
IODE	8	-	-
i_{dot}	14	$\pm 9{,}3 \cdot 10^{-10}$	$sc \cdot s^{-1}$

Kde význam jednotlivých parametrů druhého a třetího podrámce jsou následující:

- IODE (Issue of Data, Ephemeris) je počet provedených změn dat v daném podrámci.
- C_{rs} je amplituda sinusové složky harmonické korekce poloměru orbity.
- Δn je korekce středního pohybu družice.
- M_0 určuje střední anomálii ve vztažném čase t_{oe}.
- C_{uc} je amplituda kosinové složky harmonické korekce poloměru orbity.
- e představuje excentricitu dráhy družice.
- C_{us} je amplituda sinusové složky harmonické korekce argumentu šířky.
- $\sqrt{A}$ je odmocnina z délky hlavní poloosy dráhy.
- t_{oe} definuje vztažný bod efemerid.
- Interval aktualizace efemerid řídícím segmentem.
- C_{ic} je amplituda kosinové složky harmonické korekce inklinace.
- Ω_o je vzestupný uzel ve vztažném čase t_{oe}.
- C_{is} je amplituda harmonické sinusové složky harmonické korekce inklinace.

- i_0 je inklinace ve vztažném čase t_{oe}.
- C_{rc} je amplituda kosinové složky harmonické korekce inklinace.
- ω reprezentuje argument perigea.
- $\dot{\Omega}$ je rychlost změny vzestupného uzlu;
- i_{dot} je rychlost změny inklinace.

Tab. A.3: Popis parametrů almanachu. Převzato a upraveno z [12]

Parametr	Počet bitů	Rozsah	Jednotka
e	16	2^{-5}	-
t_{oa}	8	602112	s
δ_i	16	±0,0625	sc
$\dot{\Omega}$	16	$\pm 1{,}2 \cdot 10^{-7}$	$sc \cdot s^{-1}$
Stav	8	-	-
$\sqrt{A}$	24	8192	$m^{1/2}$
Ω_o	24	±1	sc
ω	24	±1	sc
M_0	24	±1	sc
α_{f0}	11	$\pm 9{,}8 \cdot 10^{-4}$	s
α_{f1}	11	$\pm 3{,}7 \cdot 10^{-9}$	-

Kde význam jednotlivých parametrů almanachu jsou následující:

- e je excentricita dráhy družice.
- t_{oa} je vztažný čas efemerid v almanachu, řídící segment aktualizuje almanach minimálně jednou za šest dní.
- δ_i je rovno odchylce inklinace ve vztažném čase t_{oa} od hodnoty 0,3 sc = 54°.
- $\dot{\Omega}$ je rychlost změny vzestupného uzlu.
- Stav neboli zdraví vyjadřuje kvalitu dat vysílaných družicí.
- $\sqrt{A}$ je odmocnina z délky hlavní poloosy dráhy.
- Ω_o je vzestupný uzel ve vztažném čase t_{oa}.
- ω reprezentuje argument perigea.
- M_0 určuje střední anomálii ve vztažném čase t_{oa}.

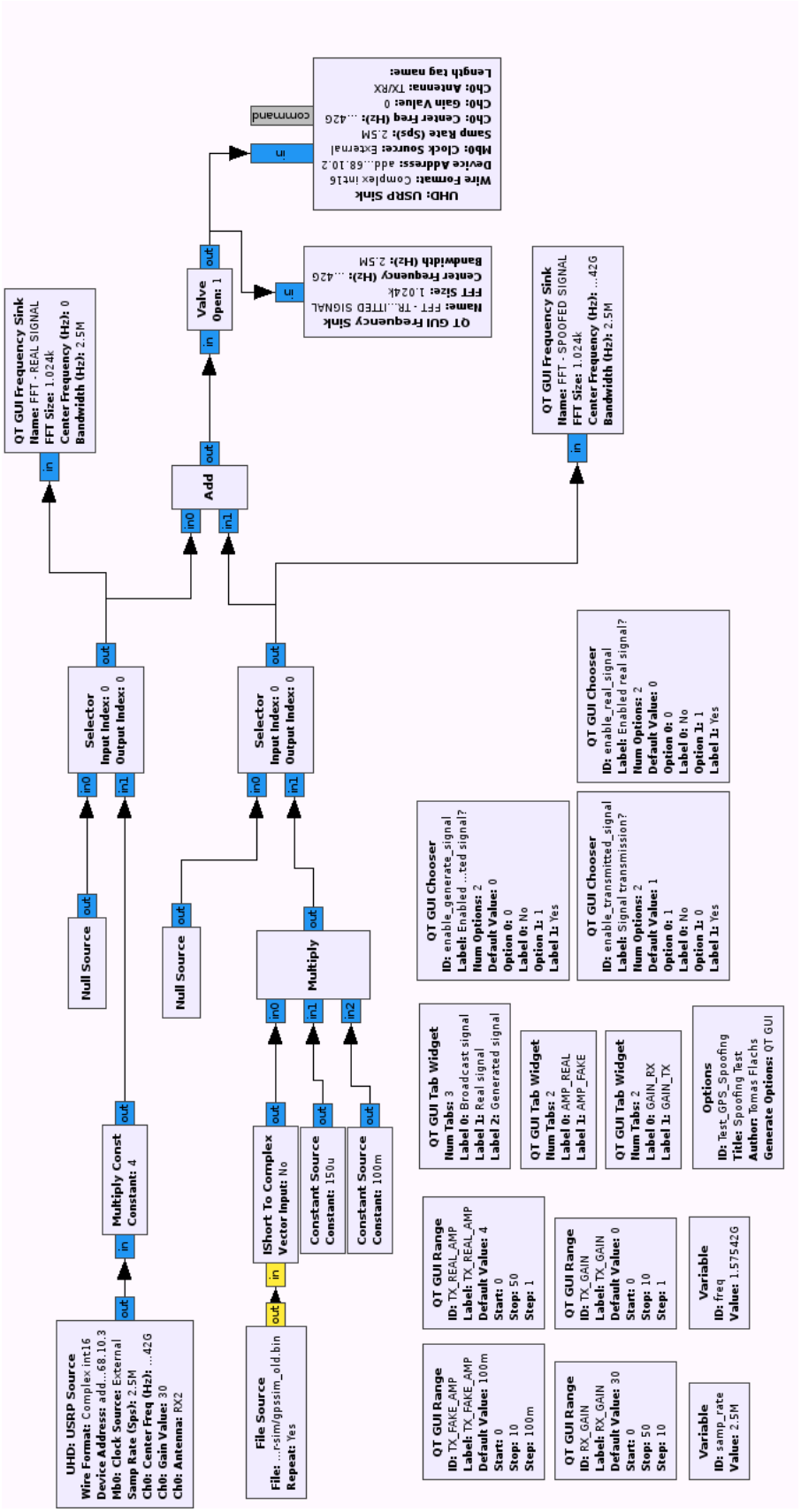
α_{f1}, α_{f0} jsou koeficienty časové základny družice.

Příloha B: Konfigurační soubor GNSS-SDR

```
[GNSS-SDR]

;######### GLOBAL OPTIONS ##################
GNSS-SDR.internal_fs_hz=2000000

;######### SIGNAL_SOURCE CONFIG ############
SignalSource.implementation=UHD_Signal_Source
SignalSource.device_address=192.168.10.3
SignalSource.item_type=gr_complex
SignalSource.sampling_frequency=2500000
SignalSource.freq=1575420000
SignalSource.gain=40
SignalSource.subdevice=A:0
SignalSource.samples=0

;######### SIGNAL_CONDITIONER CONFIG ############
SignalConditioner.implementation=Signal_Conditioner
DataTypeAdapter.implementation=Pass_Through
InputFilter.implementation=Pass_Through
InputFilter.item_type=gr_complex
Resampler.implementation=Direct_Resampler
Resampler.sample_freq_in=2500000
Resampler.sample_freq_out=2000000
Resampler.item_type=gr_complex

;######### CHANNELS GLOBAL CONFIG ############
Channels_1C.count=8
Channels.in_acquisition=1
Channel.signal=1C

;######### ACQUISITION GLOBAL CONFIG ############
Acquisition_1C.implementation=GPS_L1_CA_PCPS_Acquisition
Acquisition_1C.item_type=gr_complex
Acquisition_1C.threshold=0.008
Acquisition_1C.doppler_max=10000
Acquisition_1C.doppler_step=250

;######### TRACKING GLOBAL CONFIG ############
Tracking_1C.implementation=GPS_L1_CA_DLL_PLL_Tracking
Tracking_1C.item_type=gr_complex
Tracking_1C.pll_bw_hz=40.0;
Tracking_1C.dll_bw_hz=4.0;

;######### TELEMETRY DECODER GPS CONFIG ############
TelemetryDecoder_1C.implementation=GPS_L1_CA_Telemetry_Decoder
TelemetryDecoder_1C.dump=true

;######### OBSERVABLES CONFIG ############
Observables.implementation=Hybrid_Observables

;######### PVT CONFIG ############
PVT.implementation=RTKLIB_PVT
PVT.averaging_depth=100
PVT.flag_averaging=true
PVT.output_rate_ms=10
```

```
PVT.display_rate_ms=500
PVT.rinex_version=2
```

Příloha C: Blokový diagram v GNU Radio



Obsah přiloženého CD

1. Diplomová práce
2. Složka s výsledky měření
3. Spoofing_testing.grc
4. Spoofing_testing.py