ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra elektromagnetického pole

Detektor rušení GNSS

Diplomová práce

Studijní program: Elektronika a komunikace
Studijní obor: Rádiová a optická technika

Vedoucí práce: doc. Dr. Ing. Pavel Kovář

Filip Šturc

Praha 2019

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Šturc** Jméno: **Filip** Osobní číslo: **420361**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra elektromagnetického pole**

Studijní program: **Elektronika a komunikace**

Studijní obor: **Radiová a optická technika**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Detektor rušení GNSS

Název diplomové práce anglicky:

Detector of GNSS Interference

Pokyny pro vypracování:

Seznamte se s problematikou rádiového rušení GNSS. Proveďte rešerši metod vhodných pro odhalování a zaměřování záměrného, nezáměrného a inteligentního rušení. Vybrané metody naprogramujte v Matlabu a ověřte jednak simulací a jednak reálným měřením.

Seznam doporučené literatury:

[1] Petrovski, I, Tsujii, T.: Digital Satellite Navigation and Geophysics: A Practical Guide with GNSS Signal Simulator and Receiver Laboratory. Cambridge University Press, 2012, ISBN-13: 978-0521760546.
[2] Misra, P., Enge, P.: Global Positioning System. Ganga Jamuna Press 2006. ISBN: 0-9709544-7.

Jméno a pracoviště vedoucí(ho) diplomové práce:

doc. Dr. Ing. Pavel Kovář, katedra radioelektroniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **07.02.2018** Termín odevzdání diplomové práce: _____

Platnost zadání diplomové práce: **30.09.2019**

doc. Dr. Ing. Pavel Kovář podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

3. 1. 2019 _____

Datum převzetí zadání Podpis studenta

Prohlášení

„Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.“

V Praze dne:

…….

Podpis

Poděkování

Tímto bych chtěl poděkovat vedoucímu práce doc. Dr. Ing. Pavlu Kovářovi za odborné vedení, cenné rady a za trpělivost

Abstrakt

Tato práce se zabývá detekcí a lokalizací rádiového rušení globálních navigačních systémů. Cílem práce je zpracovat jednotlivé metody pro detekci a lokalizaci záměrného, nezáměrného a inteligentního rušení. Vybrané metody implementovat a provést jejich simulaci a následně je otestovat i reálnými změřenými daty. Pro detekci jsou představeny metody sledování spektrální výkonové hustoty, poměru C/N_0, aplikace statistické analýzy časově frekvenčních charakteristik signálů, sledování výkonu signálu, metrika podílového kritéria a sledování rozdílu pseudovzdáleností. Pro lokalizaci rádiového rušení jsou představeny algoritmy pro odhad úhlu příchodu signálu využívající rozklad do signálových podprostorů, MUSIC a ESPRIT.

Klíčová slova

GNSS, GPS, Galileo, Compass, GLONASS, detekce, lokalizace, MUSIC, ESPRIT, AoA, číslicové zpracování signálu, rádiové rušení, spoofing, jamming, meaconing

Abstract

This thesis deals with detection and localization of radio frequency interference of global navigation systems. Object of this thesis is to elaborate individual methods for detection and localization of intentional, unintentional and intelligent interference. To implement selected methods and perform their simulation and then test them with real measured data. For detection are presented following methods: monitoring of power spectral density, monitoring of C/N_0 ratio, application of the statistical analysis of the time frequency signal characteristics, signal power monitoring, ratio test metric and monitoring of the pseudo-distance difference. To locate radio frequency interference, algorithms for estimating the angle of arrival using decomposition into signal subspaces, MUSIC and ESPRIT, are introduced.

Keywords:

GNSS, GPS, Galileo, Compass, GLONASS, detection, localization, MUSIC, ESPRIT, AoA, DSP, digital signal processing, radio frequency interference, spoofing, jamming, meaconing

Obsah

1. Úvod

Družicové navigační systémy se stávají každodenní součástí našeho života, můžeme je využívat pro volnočasové aktivity, automobilovou navigaci, ale své místo mají i v letectví, ve vojenském sektoru a spoléhají na ně také záchranné složky. S rostoucím využitím však roste i snaha tyto systémy rušit nebo zneužít. Vzhledem k síle navigačních signálu na povrchu Země je velmi snadné a levné systémy družicové navigace zarušit. Rušení dělíme na dvě hlavní skupiny, záměrné a nezáměrné. Záměrné rušení pak ještě můžeme rozlišit na jamming a inteligentní rušení. Jamming spočívá v ovlivnění systému hrubou silou, inteligentní rušení se snaží napodobit autentický navigační signál. Typickým příkladem nezáměrného rušení může být nedostatečné potlačení harmonických vyzařovaných TV, starší elektronické systémy, které vyzařují rušení v důsledku stárnutí součástek nebo špatně navržené systémy.

Rádiové rušení může ovlivnit správnost určení polohy, ale i například času daného systému nebo ho úplně vyřadit z činnosti. To může v některých případech představovat bezpečnostní riziko, a právě proto je této problematice věnována čím dál větší pozornost a množí se navrhované postupy, jak takové rušení detekovat.

V této práci se budeme věnovat detekci jammingu založené na sledování spektrální výkonové hustoty signálu, sledování poměru C/N_0 a statistické analýze časově-frekvenční charakteristiky signálu. Pro detekci inteligentního rušení budou představeny metody založené na monitorování výkonu signálu, metrice podílového kritéria a monitorování rozdílu pseudovzdáleností.

Vzhledem k tomu, že je rušení v pásmu, ve kterém jsou provozovány družicové navigační systémy, ve většině zemí nelegální, má smysl také lokalizovat zdroj rušení. K tomu budou uvedeny algoritmy pro odhad úhlu příchodu signálu MUSIC a ESPRIT.

Cílem této práce je implementovat vybrané metody detekce a lokalizace rušení družicových navigačních systémů. Výstupem práce by měly být okomentované výsledky simulací jednotlivých metod a jejich následné srovnaní.

2. Systémy GNSS

Ve světě je v provozu několik družicových navigačních systémů (zkratka GNSS – Global Navigation Satellite System), mezi ty, které se současně používají nebo budou v brzké době uvedeny do provozu, se řadí především systémy GPS, GLONASS, Galileo a Compass. Signály jednotlivých systémů se liší především nosnými frekvencemi, kódem a modulací signálu. [1]

Systém GLONASS vysílá na dvou kmitočtech L1 a L2, k rozlišení signálu je použito frekvenční dělení FDMA, na rozdíl od systému GPS, kde se používá kódové dělení. Frekvenci nosné vlny lze vyjádřit:

$$f_{k,L1} = 1602 + 0{,}5625\, k \text{ [MHz]} \quad (1)$$

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

kde k = -7,.., +6 je číslo kmitočtu. Pro rozprostření signálu se používá posloupnost maximální délky o délce 511 chipů a rychlosti 511 kchipů/s. [1]

Evropský systém Galileo bude vysílat na třech kmitočtech $f_{E1} =$ 1575,42 MHz, $f_{E5} =$ 1191,795 MHz a $f_{E6} =$ 1275,75 MHz. Používat se budou modulace BPSK (Binary-Phase Shift Keying) a BOC (Binary Offset Carrier Modulation). [1]

Čínský Compass využívá celkem tři kmitočtová pásma 1559,052 – 1591,788 MHz, 1166,22 – 1217,37 MHz a 1250,618 – 1286,423 MHz. [1]

V této práci bude pro simulace algoritmů použit signál GPS L1, který je detailněji popsán v kapitole 2.1.

2.1 GPS

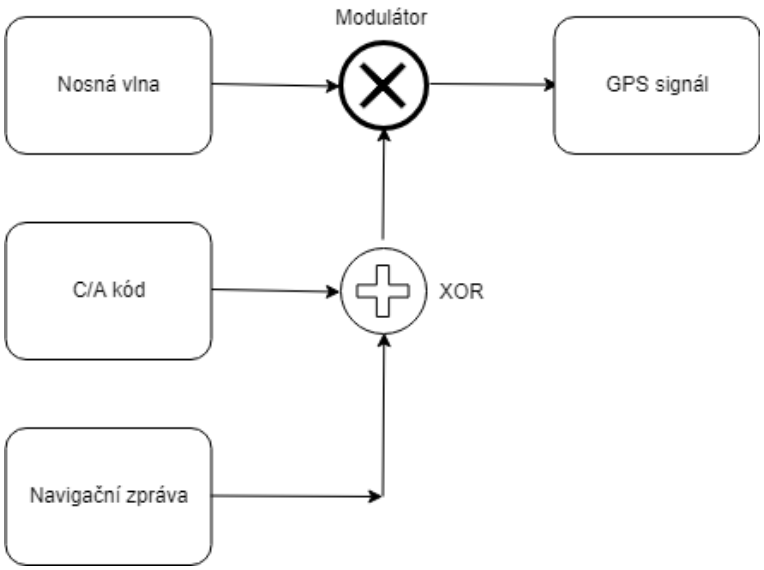
V současnosti vysílá každý satelit nepřetržitě na dvou frekvencích v L-pásmu. A to na frekvencích $f_{L1} = 1575{,}42$ MHz a $f_{L2} = 1227{,}60$ MHz, více než polovina satelitů vysílá i na kmitočtu $f_{L5} = 1176{,}45$ MHz. Tyto signály mají následující strukturu:

- nosná vlna: sinusový, kosinusový signál o frekvenci v závislosti na daném pásmu f_{L1} a f_{L2}.
- dálkoměrný kód: binární kódy, nazývané PRN (Pseudo-Random Noise) kódy, sekvence. PRN kódy pro GPS SPS (Standard Positioning System) se nazývají C/A kódy (coarse/acquisition). Každý satelit vysílá unikátní C/A kód. Jedná se o Goldův kód o délce 1023 bitů, chipů, které se opakují přibližně každou mikrosekundu. Frekvence chipů je 1023 MHz [nebo Mcps/s]
- navigační data: binárně kódovaná GPS data

C/A kód je vynásoben s navigačními daty. Výsledná sekvence bitů je následně modulovaná nosnou vlnou pomocí BPSK modulace. Celý proces je znázorněn na obrázku 2-1 a lze jej vyjádřit vzorcem (2).

$$s_{GPSL1}(t) = 2\sqrt{P}d(t)c(t)\cos(\omega_c t) \tag{2}$$

kde *P* je výkon signálu, *d*(*t*) signál přenášející navigační zprávu, *c*(*t*) C/A kód a ω_c je úhlový kmitočet nosné vlny. [1, 2]



Obrázek 2.1 Struktura signálu GPS

3. Rádiové rušení v GNSS

V této kapitole si definujeme rádiové rušení a představíme si všechny druhy rádiového rušení, v globálních navigačních systémech.

3.1 Rádiové rušení v GNSS

Za rádiové rušení (RFI – Radio Frequency Interference) považujeme jakékoliv signály, zasahující do spektra rušeného systému, kromě navigačních signálů a tepelného šumu. Všechny GNSS systémy jsou náchylné na radiové rušení, protože GNSS signály musí urazit velkou vzdálenost mezi družicí a přijímačem (přibližně 20 000 km) a v důsledku toho jsou přijímané signály extrémně slabé, přibližně 10^{-16} W. Tento výkon je srovnatelný s výkonem přirozeného šumu v pásmu 1 MHz – šířka pásma L1 a L2 u GPS. Pokud se k šumu přidá rušení vytvořené člověkem, ať už záměrně, či nezáměrně, situaci to značně komplikuje. [2]

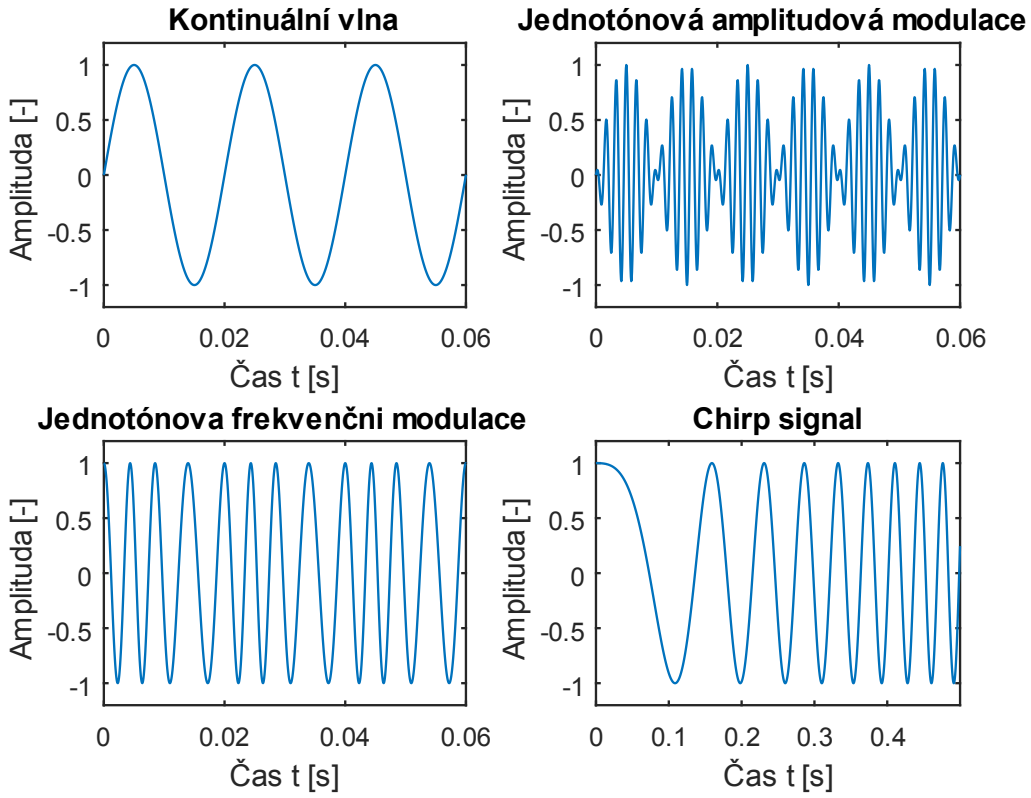
Nezáměrné rušení způsobují systémy, které vyzařují signál v GNSS pásmu v důsledku stárnutí součástek nebo špatného návrhu. Rušit mohou, ale i dobře navržené systémy, které jsou blízko k přijímači. Například TV signály, jejichž harmonické mohou zasahovat do GNSS spektra. [2]

Mezi záměrné rušení patří Jamming, ten pracuje na principu přesycení navigačního signálu silným rušivým signálem. Jamming může být pulzní nebo kontinuální. Pulzní rušení je někdy velmi dobře tolerováno, pokud je přijímač dobře navržený. U pulzního rušení lze sledovat dobu trvání jednoho pulzu, střídu pulzu a takzvaný duty cycle, doba trvání rušení, vůči době trvání navigačního signálu v procentech. Pokud je duty cycle menší než 10 %, nebývá toto rušení problematické i pokud jsou pulzy silné. Kontinuální rušení se dělí na úzkopásmové a širokopásmové. Signály s šířkou pásma větší, než přibližně 20 MHz (v závislosti na šířce pásma přijímače), jsou považovány za širokopásmové. Rušení s menší šířkou pásma jsou považována za úzkopásmové, může se jednat i o jediný tón. [2]

Dalším typem záměrného rušení je inteligentní rušení, to můžeme dále rozlišit na spoofing a meaconing. Spoofing spočívá v generování a vysílání signálu, který se přijímači jeví jako autentický GNSS signál, pokud přijímač takový signál přijímá, způsobí to značnou chybu v určování polohy. Je zřejmé, že je značně komplikovanější rušit pomocí spoofingu než pomocí jammingu, ale lze pomocí něho rušit na velké vzdálenosti a je podstatně složitější jej odhalit. Rušení pomocí meaconingu je podstatně snazší, jelikož spočívá pouze v přijímání, zpoždění a vysílání reálného GNSS signálu. [3]

3.2 Jamming

Jamming může být v podstatě jakýkoliv signál, zasahující do některého z kmitočtových pásem GNSS. Mezi nejčastěji používané signály patří kontinuální sinusová vlna, amplitudově modulovaný sinusový signál, frekvenčně modulovaný sinusový signál a takzvaný chirp, což je signál, u kterého dochází ke zvyšování nebo snižování frekvence v čase. Tato změna může být lineární nebo například logaritmická. Na obrázku 3-1 jsou vykresleny časové průběhy jednotlivých signálů [4]:



Obrázek 3.1 Časové průběhy rušivých signálů (jamming)

3.3 Inteligentní rušení

U spoofingu lze rozlišovat tři základní typy. Ty se liší podle toho, jak je spoofing generován:

- Asynchronní spoofing: jedná se o nejjednodušší typ spoofingu, který pracuje na principu napodobování autentického GPS signálu.

- Spoofing synchronizovaný na čas a polohu GPS: pokročilejší způsob spoofingu, který se skládá z GPS přijímače a radiového vysílače. Systém se nejdříve synchronizuje se současným GPS signálem a získá tak informace o pozici, času a celé navigační zprávě satelitu a za pomoci znalosti těchto údajů následně generuje rušivý signál.

- Spoofing respektující pohyb uživatele: nejkomplexnější a nejefektivnější technika spoofingu založená na znalosti pozice přijímače s přesností na centimetry. Díky tomu je takový Spoofer schopný perfektně synchronizovat kód a fázi nosné vlny s autentickým signálem.

Meaconing byl již definován jako příjem, zpoždění a opakované vysílání autentického GPS signálu. [5]

4. Metody pro detekci rušení

Tato kapitola pojednává o metodách detekce nezáměrného, záměrného a inteligentního rušení. Metody používají různý přístup v různých fázích zpracování navigačních signálů, pre-korelační i post-korelační. Pro detekci lze využít Spektrální výkonovou hustotu přijatého signálu, dále poměr C/N_0, statistickou analýzu časově-frekvenčních charakteristik signálu, sledování výkonu signálu nebo rozdílu pseudovzdáleností.

4.1 Nezáměrné rušení a jamming

4.1.1 Metoda využívající sledování spektrální výkonové hustoty

Frekvenční pásma využívaná GNSS jsou striktně regulována, proto může být spektrální výkonová hustota (PSD) efektivní nástroj pro detekci záměrného i nezáměrného rádiového rušení. PSD přijatého signálu lze spočítat pomocí Wiener-Khinchinova teorému:

$$S_{xx}(\omega) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \Gamma_{xx}(t)e^{-j\omega t}dt \tag{3}$$

kde ω je úhlová frekvence a $\Gamma_{xx}(t)$ je autokorelační funkce signálu *x(t)*. Autokorelační funkci lze vypočítat jako:

$$\Gamma_{xx}(\tau) = \int_{-\infty}^{\infty} x(t+\tau)\, x^*(t)dt \tag{4}$$

kde $x^*(t)$ značí komplexní sdružení signálu *x(t)*. [4]

PSD lze určit také Welchovou metodou, která spočívá v rozdělení signálu do bloků, výpočtu periodogramů jednotlivých bloků a jejich následného průměrování. [6]

Spektrální výkonovou hustotu lze použít pro detekci jak úzkopásmového, tak širokopásmového rušení, porovnáním vypočítaného PSD z přijatého signálu a masky prahové úrovně rušení. Úroveň tolerovaného rušení lze určit z doporučení ICAO [7], viz tabulka 4.1. Vliv konkrétního rušení na GNSS signál záleží na spektru obou signálů a může být odhadnut pomocí koeficientu spektrální separace (SSC). SSC κ_k představuje úroveň vzájemného ovlivňování se obou signálů a je formulován následovně:

$$\kappa_k = \int_{-B/2}^{B/2} S_{kk}(f) S_{xx}(f)\, df \tag{5}$$

$S_{kk}(f)$ a $S_{xx}(f)$ jsou PSD dvou signálů $k(t)$ a $x(t)$. [4]

f_i [MHz]	P [dBW]
< 1315	-4,5
1315 - 1525	Lineárně klesající z -4,5 na -42
1525 - 1565,42	Lineárně klesající z -42 na -150,5
1565,42 - 1585,42	-150,5
1585,42 - 1610	Lineárně rostoucí z -150,5 na -60
1610 - 1618	Lineárně rostoucí z -60 na -42
1618 - 2000	Lineárně rostoucí z -42 na -8,5
> 2000	-8,5

Tabulka 4.1 Spektrální maska pro rádiové rušení v pásmu GPS L1 podle [7]

4.1.2 Metoda využívající sledování poměru C/N_0

Poměr C/N_0 je silně ovlivněn rušivými signály a může tedy být indikátorem pro detekci rušení. Existuje mnoho algoritmů pro výpočet odhadu poměru C/N_0. V této práci bude použit algoritmus Narrowband Wideband Power Ratio (NWPR), který je založený na porovnávání šumu na výstupu korelátoru ve velké a malé šířce pásma.. Algoritmus zpracovává vzorky výstupního signálu korelátoru $r_C[n]$:

$$r_C[n] = \sqrt{P_d} D[n] + \sqrt{P_n} \eta[n] \tag{6}$$

kde $D[n]$ je navigační zpráva a $\eta[n]$ je šum. P_D je výkon užitečného signálu po odstranění rozprostření dálkoměrným kódem a P_η je výkon šumu. Celkový výkon výstupu korelátoru je porovnáván přes dvě různá pásma, široké a úzké. Odhad výkonu WBP_k v širokém pásmu je založen na šířce pásma šumu $1/T_{int}$:

$$WBP_k = \sum_{m=1}^{M} |r_C[kM + m]|^2, \qquad k = 0,1, \ldots, (\frac{N}{M} - 1) \tag{7}$$

kde T_{int} je doba koherentní integrace, M počet koherentních integrací v době trvání jednoho navigačního bitu a N je počet koherentních integrací použitých pro jeden odhad C/N_0. Odhad výkonu v úzkém pásmu (šířka pásma $1/MT_{int}$) NBP_k lze vyjádřit:

$$NBP_k = \left(\sum_{m=1}^{M} \mathcal{R}\{r_C[kM+m]\}\right)^2 + \left(\sum_{m=1}^{M} \Im\{r_C[kM+m]\}\right)^2 \quad (8)$$

($\mathcal{R}$) *a* ($\Im$) značí reálnou a imaginární složku výstupu korelátoru. Odhadovaná střední hodnota $\hat{\mu}_{NP}$ výkonu šumu $NP_k = NBP_k/WBP_k$, lze určit jako:

$$\hat{\mu}_{NP} = \frac{M}{N}\sum_{k=0}^{\frac{N}{M}-1} NP_k \quad (9)$$

Ta je použita pro finální odhad poměru C/N_0:

$$\frac{C}{N_0} = \frac{1}{T_{int}}\frac{\hat{\mu}_{NP}-1}{M-\hat{\mu}_{NP}} \quad (10)$$

C/N_0 je ovlivněno řadou faktorů, patří mezi ně elevace satelitů, útlum v atmosféře, způsobený například srážkami, útlum v troposféře, vyzařovací charakteristika družice a přijímače, mnohocestné šíření, výkon vysílače konkrétní družice, a tak dále. Poměr C/N_0 tedy nemůže být považován za konstantní. Pro efektivní detekci pomocí C/N_0 je nutné určit efektivní poměr C/N_0:

$$\left(\frac{C}{N_0}\right)_{eff} = \frac{CL_s}{N_0L_n + I_{total}} \quad (11)$$

kde C je výkon nosné vlny, N_0 je spektrální výkonová hustota šumu, L_s a L_n jsou ztráty při zpracování. Kromě ztrát při zpracování signálu v přijímači a vyzařovací charakteristice antény, existuje další významný příspěvek, který ovlivňuje efektivní poměr C/N_0, způsobený rušením. I_{total} vyjadřuje celkovou úroveň rušení. Podíl na rušení, pro každý signál, lze určit jako SSC κ_k, z rovnice (5), výkonů jednotlivých nosných C_k a ztrát při zpracování L_k. Jako příklad lze uvést intra-systémové rušení způsobené M satelity stejného GNSS:

$$I_{intra} = \sum_{k=1}^{M} C_k L_k \kappa_k \quad (12)$$

Jakýkoliv znatelný rozdíl mezi změřeným C/N_0 a efektivním C/N_0 poukazuje na přítomnost záměrného nebo nezáměrného rušení v monitorovaném GNSS pásmu. [4]

4.1.3 Detekce rušení v časově-frekvenční a statistické doméně

Metoda detekce rušení v časově-frekvenční a statistické doméně používá kombinaci časově–frekvenční (TF – time-frequency) a statistické analýzy, k detekci různých typů rádiového rušení (RFI) při nízkých poměrech JNR (jammer to noise ratio).
Jako nástroj pro analýzu v TF doméně je zvolena pseudo Wigner–Ville distribuce (PWVD), pro odhad okamžité frekvence signálu (IF). Pomocí detekce hran v TF doméně jsou získány dvě sekvence IF odhadů, jedna pro signál bez rušení – posuzovací okno a druhá pro signál s rušením - vyhodnocovací okno. Z obou sekvencí se spočítá rozptyl a podrobí se statistickému F-testu, testu shodnosti rozptylů. F-test je citlivý na odchylku pravděpodobnostního rozdělení od normálního rozdělení dvou sekvencí vzorků. Odhady IF jsou přibližně uniformě rozloženy, je tedy nutné odvodit parametry v F rozdělení, korekcí koeficientů použitých ve statistickém testu a použití aproximace mezi normálním a chi-square rozdělením. Tato modifikace je použita pro určení kritické oblasti (KO). [8]

a) Definice úlohy a testování hypotéz

Přijatý signál včetně šumu a rušení lze popsat jako:

$$y(t) = s(t) + w(t) + u(t) \tag{13}$$

kde $s(t)$ je GNSS signál, $w(t)$ bílý Gaussovský šum a $u(t)$ je RFI. RFI, širokopásmové i úzkopásmové lze modelovat jako:

$$u(t) = A_u(t)\exp(j\varphi(t)) \tag{14}$$

kde $A_u(t)$ je okamžitá amplituda a $\varphi(t)$ je okamžitá fáze. Okamžitá amplituda je obvykle velmi pomalu se měnící funkce, takže ji zjednodušeně považujeme za konstantní.
Okamžitou frekvenci IF můžeme získat pomocí první derivace okamžité fáze podle času:

$$IF = \frac{1}{2\pi}\frac{d\varphi(t)}{dt} \tag{15}$$

Cílem je najít metodu, která může být použita k určení, zda je přítomno rušení $u(t)$ nebo nikoliv, za použití testu hypotéz. Nulová hypotéza (H_0) a k ní alternativní hypotéza (H_a) jsou formulovány následovně:

$$H_0 : y(t) = w(t) \tag{16}$$

$$H_a : y(t) = w(t) + u(t)$$

Přijímaný GNSS signál je přibližně o 20 dB slabší než termální šum v pásmu 2 MHz, proto má nulová hypotéza daný tvar (16). [8]

Testování hypotéz uvažující rozptyl ze dvou výběrů

Předmětem je testování hypotézy v závislosti na hodnotách jednoho nebo více parametrů daného výběru (rozptyl, střední hodnota, …). Obecně bývají formulovány dvě vzájemně jednoznačné hypotézy. Kritická oblast specifikuje hodnoty, pro které je vyvrácena nulová hypotéza ve prospěch hypotézy alternativní. Pro každou fixní kritickou oblast mohou nastat dva druhy chyb, chyba prvního druhu, kdy je rozhodnuto ve prospěch H_a, když je H_0 pravda a chyba druhého druhu, kdy je rozhodnuto ve prospěch H_0, když je pravda H_a. Pravděpodobnost chyby prvního druhu je stanovena hladinou významnosti testu α. [8]

Statistické rozhodnutí v závislosti na střední hodnotě je často používáno kvůli její robustnosti díky předpokladu normality plynoucí z centrální limitní věty. Rozptyl je další důležitý parametr, který může být použit pro statistické rozhodování. Pro toto rozhodnutí můžeme použít jednostranný F-test, který porovnává rozptyly ze dvou normálních výběrů pomocí statistického testu poměru rozptylů těchto výběrů. Předpokládejme, že $Y_{11}, Y_{12}, \ldots, Y_{1N1}$ a $Y_{21}, Y_{22}, \ldots, Y_{2N2}$ jsou nezávislé náhodné vzorky ze dvou normálních rozdělení, s neznámou střední hodnotou, s rozptyly σ_1^2 a σ_2^2. N_1 a N_2 jsou délky jednotlivých sekvencí. Chceme testovat nulovou hypotézu H_0: $\sigma_1^2 = \sigma_2^2$ proti alternativní hypotéze H_a: $\sigma_1^2 < \sigma_2^2$. Hodnoty rozptylů nebývají v reálných aplikacích k dispozici, proto musíme použít odhady rozptylů s_1^2 a s_2^2. Pak můžeme test formulovat jako:

$$F = \frac{s_1^2}{s_2^2} \tag{17}$$

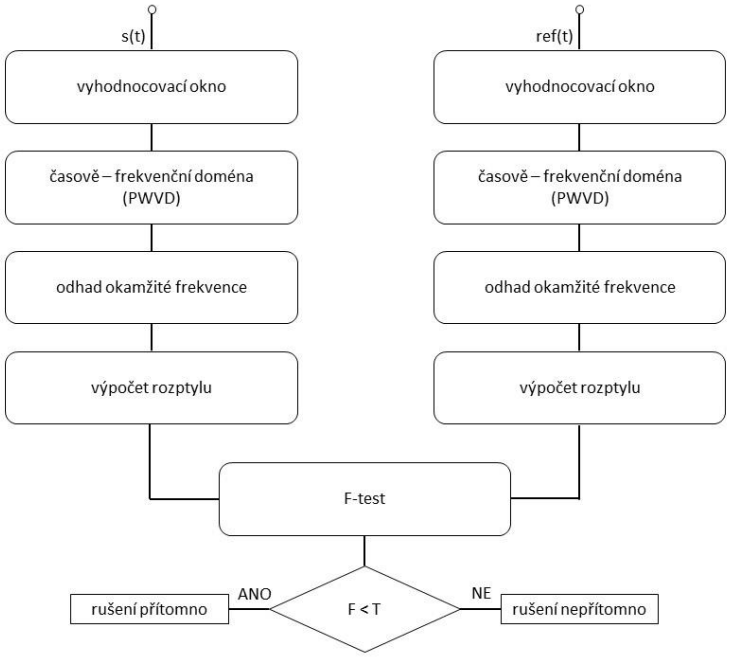
který má F rozdělení se stupni volnosti $N_1 - 1$, pro čitatel a $N_2 - 1$, pro jmenovatel. Pokud je α fixní můžeme pak vyjádřit kritickou oblast jako:

$$KO = \left\{ \frac{s_1^2}{s_2^2} < T \right\} \tag{18}$$

kde T je rozhodovací úroveň stanovená úrovní signifikance α. [8]

b) Metoda detekce

Algoritmus pro detekci rušení je znázorněn v diagramu na obrázku 4-1. Pro realizaci tohoto algoritmu, je kromě analyzovaného přijatého signálu potřeba také signál, o kterém víme, že neobsahuje žádné rušení. Pro detekci se vždy vybere jedna část signálu, okno. A to okno vyhodnocovací pro zkoumaný signál a posuzovací pro signál bez rušení. Obě okna jsou následovně převedena z časové oblasti do oblasti časově – frekvenční, TFR. Z TFR se vypočítají odhady okamžité frekvence, z tohoto odhadu spočítáme rozptyly a ty podrobíme dvou-výběrovému F-testu. Pokud je hodnota získaná pomocí F-testu menší než rozhodovací úroveň T, vyhodnotí se zkoumaná část signálu jako signál s přítomným rušením. [8]



Obrázek 4.2 Algoritmus pro detekci

Pro časový okamžik t v jednotlivých oknech je $f(t)$ pozice maxima TFR. Odhad okamžité frekvence poté můžeme získat jako:

$$IF = arg\left[max_f TFR(t, f)\right] \tag{19}$$

Náhodný šum je rozložený přes všechny frekvence v TF doméně. V důsledku toho se *IF* odhady v posuzovacím okně IF_{pos} náhodně mění. Ve vyhodnocovacím okně IF_{vyh} tomu tak není, jelikož funkce *IF* reálného rušení mívá nějaký geometrický tvar. Díky tomu můžeme pomocí náhodnosti těchto dvou sekvencí určit, zda je rušení přítomno, či nikoliv.
Kvůli hraničnímu efektu (boundary effect) v TF doméně je odhad *IF* signálu v blízkosti hranic špatný. Proto použijeme střední část odhadů zahozením *2L - 1* vzorků:

$$IF_{vyh}[n] = \hat{f}_1[n], n = L, \ldots, N_1 - L \qquad (20)$$
$$IF_{pos}[n] = \hat{f}_2[n], n = L, \ldots, N_2 - L$$

kde N_1 a N_2 jsou délky jednotlivých oken. Následovně můžeme spočítat rozptyl obou sekvencí:

$$\sigma_{roz}^2 = \frac{1}{\widetilde{N_1} - 1} \sum_{n=L}^{N_1 - L} (IF_{roz}[n] - m_{roz})^2 \qquad (21)$$
$$\sigma_{pos}^2 = \frac{1}{\widetilde{N_2} - 1} \sum_{n=L}^{N_1 - L} (IF_{pos}[n] - m_{pos})^2$$

kde $\widetilde{N_1} = N_1 - 2L + 1$ a $\widetilde{N_2} = N_2 - 2L + 1$ jsou efektivní délky jednotlivých oken, m_{roz} a m_{pos} jsou střední hodnoty jednotlivých *IF* odhadů. Vztah pro výpočet F hodnot je uveden výše (17). [8]

c) Analýza signálu v TF doméně

Jako nástroj pro analýzu v TF doméně je zde použita pseudo Wigner-Villeho transformace, modifikace Wigner-Villeho distribuce. Jedná se o nelineární metodu časově frekvenční analýzy, která je definována:

$$PWVD_y(t, f) = \int_{-\infty}^{+\infty} h(\tau) y(t + \frac{\tau}{2}) y^*(t - \frac{\tau}{2}) e^{-j2\pi f \tau} d\tau \qquad (22)$$

kde ´*´ je komplexní sdružení, *t* je čas, τ je posunutí podél časové osy, *h* je váhovací okno a *y* je časová reprezentace signálu. [8]

d) Určení rozhodovací úrovně

Jak již bylo řečeno, pro signál bez rušení jsou odhady *IF* přibližně rovnoměrně rozloženy přes frekvenční pásmo. F-test je velmi citlivý na odchylky od normality. Pokud je rozdělení symetrické

s kratšími okraji než normální rozdělení, jako třeba rovnoměrné rozdělení, skutečná úroveň signifikance je pak menší než α. Proto musíme zvážit lepší stanovení kritické oblasti pro testování hypotéz. [8]

Rozptyl vzorků s^2 z X, který je použit pro F-test, je náhodná proměnná. Asymptotické rozdělení rozptylu s^2 může být považováno za normální, pokud je splněna podmínka dostatečného počtu vzorků. Tato podmínka je, v případě GNSS, snadno splněna díky dlouhé periodě kódu. Střední hodnota rozptylu $E(s^2) = \mu_2$, kde μ_2 je rozptyl populace. V případě nenormální populace X může být rozptyl vypočten jako:

$$Var(s^2) = \frac{1}{N}(\mu_4 - \mu_2^2 \frac{N-3}{N-1}) \tag{23}$$

kde $\mu_k = E[(X - E[X])^k]$ je centrální moment k-tého řádu z X a $E[X]$ je střední hodnota X. N je počet vzorků. V našem případě je N počet *IF* odhadů, ze kterých se počítá rozptyl s^2. Jak již bylo řečeno odhady *IF* získané pomocí PWVD mají přibližně rovnoměrné rozdělení. Pokud tedy předpokládáme, že X je rovnoměrně rozloženo na intervalu [a, b], pak může být vypočten jeho druhý a čtvrtý centrální moment pomocí vztahu:

$$\mu_2 = (b-a)^2/12 \tag{24}$$
$$\mu_4 = (b-a)^4/80$$

a dosazením můžeme získat vztah pro výpočet rozptylu rovnoměrného rozdělení:

$$Var(s^2) = \frac{2N+3}{N(N-1)} \frac{(b-a)^4}{360} \tag{25}$$

Jelikož má F-test, při testování nulové hypotézy F rozdělení s chi-square rozdělením čitatele a jmenovatele, potřebujeme definovat dvě proměnné, které budou mít přibližně chi-square rozdělení. Pokud mají chi-square rozdělení dostatečný počet stupňů volnosti, můžeme použít následující aproximaci:

$$\chi_k^2 \xrightarrow{d} N(k, 2k) \tag{26}$$

Poté, pokud použijeme zpětně tuto aproximaci, můžeme definovat novou proměnnou, která je lineární k normálně rozloženému rozptylu s^2 jako $Z = vs^2/\mu_2^2$. Pak je Z náhodná proměnná z normálního rozdělení se střední hodnotou a rozptylem:

$$E[Z] = \nu \tag{27}$$
$$Var[Z] = \nu^2 Var(s^2)/\mu_2^2$$

Z použité aproximace plyne, že rozptyl musí být dvojnásobek střední hodnoty. Při předpokladu, že Var[*Z*] = *2*E[*Z*], získáme koeficient *ν* jako:

$$\nu = \frac{2\mu_2^2}{Var(s^2)} = \frac{5N(N-1)}{2N+3} \tag{28}$$

Za předpokladu velikosti vzorku, $N \to \infty$, získáme přibližný vztah $\nu \approx 2{,}5(N-1)$. Nově definovaná proměnná *Z* má přibližně chi-square rozdělení s *ν* stupni volnosti.

Nyní můžeme formulovat F-test pro dvě náhodné proměnné Z_1 a Z_2:

$$F = \frac{Z_1/\nu_1}{Z_2/\nu_2} = \frac{s_1^2\mu_{2,2}}{s_2^2\mu_{2,1}} \tag{29}$$

kde $Z_1 = \nu_1 s_1^2/\mu_{2,1}$ a $Z_2 = \nu_2 s_2^2/\mu_{2,2}$ jsou náhodné proměnné s přibližně chi-square rozdělením a s ν_1 a ν_2 stupni volnosti. Při platnosti nulové hypotézy platí $\mu_{2,1} = \mu_{2,2}$. V našem případě je velikost vzorku v jednotlivých oknech $\widetilde{N_1}$ a $\widetilde{N_2}$. Naše F rozdělení pak tedy bude mít počet stupňů volnosti roven $\nu_1 = 2{,}5(\widetilde{N_1} - 1)$ pro čitatel a $\nu_2 = 2{,}5(\widetilde{N_2} - 1)$ pro jmenovatel.
V závislosti na těchto odvození je teoretická rozhodovací úroveň, při fixní úrovni signifikance, předdefinován jako:

$$T = F_{\nu_1,\nu_2,\alpha} \tag{30}$$

při $P(F < T) = \alpha$. [8]

4.2 Inteligentní rušení

V této kapitole si představíme několik metod pro detekci inteligentního rušení. Tyto metody využívají monitorování výkonu signálu, analýzu vzorků korelátoru pomocí podílového kritéria nebo monitorování rozdílu pseudovzdáleností.

4.2.1 Metody pro detekci spoofingu založené na monitorování výkonu signálu

Model přijatého signálu

Přijímač s jednou anténou

Uvažujeme-li GPS L1 C/A kód, přijatý signál s přítomností spoofingu lze modelovat následovně:

$$r(nT_s) = \sum_{m=1}^{N_{Aut}} \sqrt{p_m^a} F_m^a(nT_s) + \sum_{q=1}^{N_{Spof}} \sqrt{p_q^s} F_q^s(nT_s) + w(nT_s) \tag{31}$$

kde:

$$F_m^a(nT_s) = h_m^a(nT_s - \tau_m^a) c_m^a(nT_s - \tau_m^a) e^{j\phi_m^a + j2\pi f_m^a nT_s} \tag{32}$$

$$F_q^s(nT_s) = h_q^s(nT_s - \tau_q^s) c_q^s(nT_s - \tau_q^s) e^{j\phi_q^s + j2\pi f_q^s nT_s}$$

N_{Aut} a N_{Spoof} je počet autentických a rušivých signálů. Indexy *s* a *a* odkazují na autentické a rušivé signály, T_s je vzorkovací interval a ϕ, *f*, *p* a τ jsou fáze nosné vlny, Dopplerův posuv, výkon signálu a kódové zpoždění přijatého signálu. $h(nT_s)$ jsou vysílaná navigační data a $c(nT_s)$ je PRN sekvence v časovém okamžiku nT_s. Indexy *m* a *q* korespondují s *m*-tým autentickým signálem a *q*-tým rušivým signálem. *w* je komplexní aditivní bílý Gaussovský šum s rozptylem σ^2 a *j* je komplexní jednotka. [5]

Přijímač s více anténami

Uvažujme *N*-prvkovou anténní řadu. V této konfiguraci je jedna anténa zvolena za referenční. Předpokládejme, že referenční souřadnicový systém je umístěn v referenční anténě (r_1), viz obrázek 4-1. Dále předpokládejme, že spoofer je vysílač s jednou anténou, který vysílá několik PRN signálů ze

stejného směru. Komplexní pásmová reprezentace N přijatých prostorových vzorků autentických a rušivých signálů dopadajících na anténní řadu před de-spreadingem, může být zapsáno jako:

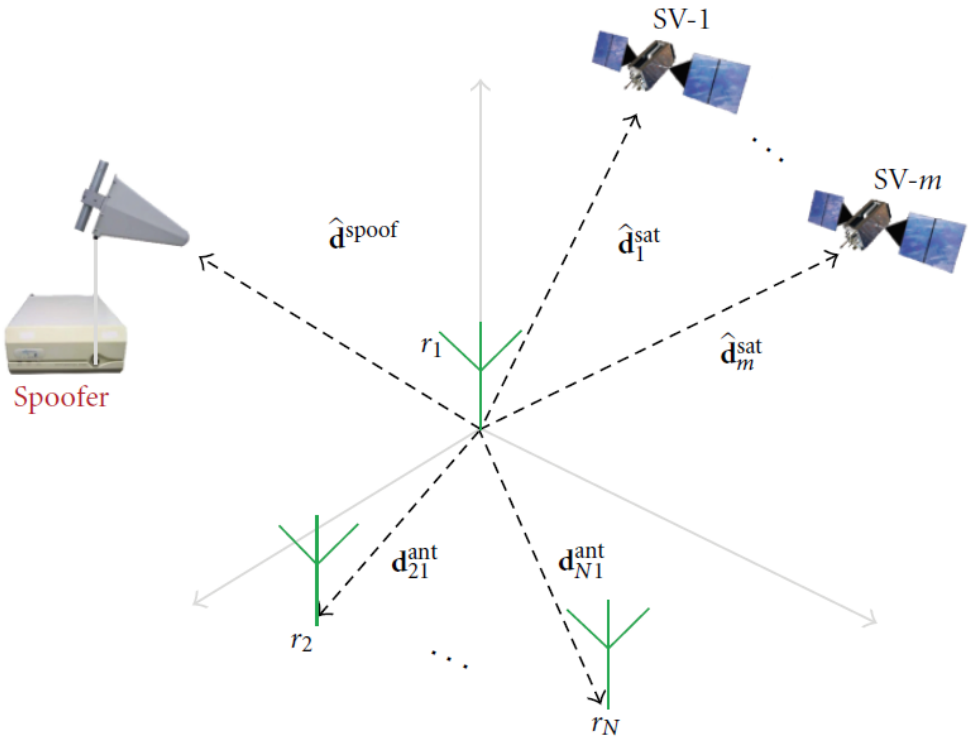
$$\mathbf{r}(nT_s) = \begin{bmatrix} r_1(nT_s) \\ \vdots \\ r_N(nT_s) \end{bmatrix} = \sum_{m=1}^{N_{Aut}} \mathbf{a}_m \sqrt{p_m^a} F_m^a(nT_s) + \mathbf{b} \sum_{q=1}^{N_{Spoof}} \sqrt{p_q^s} F_q^s(nT_s) + \boldsymbol{w}(nT_s) \tag{33}$$

kde $\boldsymbol{w}$ je vektor N x 1 komplexního aditivního bílého Gaussovského šumu s kovarianční maticí $\sigma^2\mathbf{I}$, $\mathbf{I}$ reprezentuje N x N matici identity. $\boldsymbol{a}_m$ a $\boldsymbol{b}$ jsou vektory zahrnující všechny prostorové charakteristiky anténní řady pro autentický a rušivý signál:

$$\mathbf{b} = \begin{bmatrix} 1 \\ b_2 \\ \vdots \\ b_N \end{bmatrix} = \begin{bmatrix} e^{-j(\frac{2\pi \mathbf{d}_{11}^{ant} . \hat{\mathbf{d}}^{spoof}}{\lambda})} \\ e^{-j(\frac{2\pi \mathbf{d}_{21}^{ant} . \hat{\mathbf{d}}^{spoof}}{\lambda})} \\ \vdots \\ e^{-j(\frac{2\pi \mathbf{d}_{N1}^{ant} . \hat{\mathbf{d}}^{spoof}}{\lambda})} \end{bmatrix}$$

$$\mathbf{a}_m = \begin{bmatrix} 1 \\ (a_m)_2 \\ \vdots \\ (a_m)_N \end{bmatrix} = \begin{bmatrix} e^{-j(\frac{2\pi \mathbf{d}_{11}^{ant} . \hat{\boldsymbol{d}}_m^{sat}}{\lambda})} \\ e^{-j(\frac{2\pi \mathbf{d}_{21}^{ant} . \hat{\boldsymbol{d}}_m^{sat}}{\lambda})} \\ \vdots \\ e^{-j(\frac{2\pi \mathbf{d}_{N1}^{ant} . \hat{\boldsymbol{d}}_m^{sat}}{\lambda})} \end{bmatrix} \tag{34}$$

kde $\mathbf{d}_{i1}^{ant}$ reprezentuje vektor směřující z počátku (střed fáze referenční antény) do středu fáze i-té antény. $\hat{\mathbf{d}}_m^{sat}$ a $\hat{\mathbf{d}}^{spoof}$ jsou vektory směřující z počátku do m-tého autentického satelitu a do zdroje rušení. λ je vlnová délka nosné vlny v pásmu GPS L1. [5]



Obrázek 4-1 Konfigurace přijímače s více anténami [5]

a) Sledování poměru C/N_0

Většina GPS přijímačů používá parametr C/N_0 k určení kvality přijímaného signálu. Při dobré viditelnosti tento parametr ovlivňuje jenom pohyb satelitů a změny v ionosféře, jedná se pouze o postupné hladké změny, nikoliv skokové. Když, naproti tomu, spoofer s vyšším výkonem začne ovlivňovat GPS přijímač, lze v signálu sledovat skokovou změnu C/N_0, která může posloužit jako indikátor přítomnosti spoofingu. Přijímač může průběžně sledovat jakékoliv nezvyklé změny C/N_0, jež mohou být znakem spoofingu. Pro GPS přijímač není problém ukládat přijatý signál z jednotlivých satelitů. [5]

Uvažujme výstup korelátoru pro l-tý autentický signál daný následující rovnicí:

$$y_l^a(kNT_s) = \underbrace{\sqrt{p_l^a}e^{j\varphi_l^a}}_{S:\text{požadovaný signál}} + \underbrace{\sum_{m=1,m\neq l}^{N_{Aut}} \sqrt{p_m^a}C_{ml}^a(kNT_s)}_{I_{Aut}:\text{rušení ostatními autentickými PRN}} + \underbrace{\sum_{q=1}^{N_{spoof}} \sqrt{p_m^s}C_{ql}^s(kNT_s)}_{I_{spoof}:\text{rušení spoofingem}} + \underbrace{\overline{w}(kNT_s)}_{Gaussovský\ šum} \quad (35)$$

kde:

$$C_{ml}^{a}(kNT_s) = \frac{1}{N}\sum_{n=(k-1)N+1}^{kN} F_m^a(nT_s)\hat{F}_l(nT_s)$$

$$C_{ql}^{s}(kNT_s) = \frac{1}{N}\sum_{n=(k-1)N+1}^{kN} F_q^s(nT_s)\hat{F}_l(nT_s) \tag{36}$$

$$\hat{F}_l(nT_s) = c_l(nT_s - \hat{\tau}_l)e^{-j2\pi\hat{f}_l nT_s}$$

N je koherentní interval integrace a kNT_s je časový okamžik, kdy je výstup korelátoru aktualizován. $C_{ml}^{a}(kNT_s)$ je vzájemná korelace $F_m^a(nT_s)$ a l-té generované repliky PRN signálu $\hat{F}_l(nT_s)$, jejíž Dopplerovský a časový posuv jsou $\hat{f}_l$ a $\hat{\tau}_l$. Pro zjednodušení byl zanedbán vliv datové zprávy. I_{Aut} a I_{Spoof} v rovnici (37) jsou rušení vzniklé vlivem vzájemné korelace jiných autentických a rušivých signálů. $\overline{w}(kNT_s)$ je filtrovaný šum s rozptylem σ^2/N. C/N_0, pro GPS signál, je úměrné poměru odstupu výkonu signálu na výstupu korelátoru, k výkonu šumu a výkonu jiných rušivých signálů (SNR):

$$SNR_l^a = \frac{p_l^a}{|I_{Aut}|^2 + \left|I_{Spoof}\right|^2 + (\sigma^2/N)} \tag{37}$$

GPS signály jsou navrženy tak, že $|I_{Aut}|^2$ je zanedbatelné vůči rozptylu filtrovaného Gaussovského šumu. $\left|I_{Spoof}\right|^2$ se však zvyšuje s narůstajícím celkovým výkonem spoofingu (TSP). TSP je součet výkonů pro různé rušivé PRN ($TSP = \sum_{q=1}^{N_{Spoof}} \sqrt{p_q^s}$). Z toho důvodu může asynchronní zdroj rušení s větším výkonem výrazně snížit C/N_0. Pokud je však rušivý signál zpětně rozprostřen, poměr C/N_0 se jeví jako C/N_0 autentického signálu. Jako důsledek pak může detektor na bázi sledování C/N_0 selhat. [5]

b) Sledování absolutního výkonu signálu

Jelikož útlum vzniklý šířením signálu mezi zdrojem rušení a přijímačem se výrazně mění, je pro zdroj rušení obtížné odhadnout vysílací výkon tak, aby byl dostačující pro ovlivnění přijímače a aby zároveň výrazně nepřesahoval typickou hodnotu výkonu pro autentický GPS signál. Maximální přijatý výkon GPS signálů, přijímaných na zemi, je přibližně – 153 dBW v pásmu L1. Je tedy zřejmé, že příjem signálu s výrazně vyšším absolutním výkonem, než je očekávaný výkon autentického GPS signálu, je jednoduchým prostředkem pro detekci spoofingu. [5]

4.2.2 Metoda pro detekci spoofingu založena na metrice podílového kritéria

Tato metoda se řadí do třídy metod sledování kvality signálu a je zaměřena na detekci útoku ve fázi trackingu, sledováním tvaru korelační funkce.
Jak již bylo zmíněno, existují tři hlavní typy spoofingu, tato metoda je zaměřena především na druhý typ (viz kapitola 3.3). [9]

Metrika podílového kritéria pro detekci spoofingu je definována jako:

$$M_1[k] = \frac{I_e[k] + I_l[k]}{\varepsilon I_p[k]} \tag{38}$$

kde $I_e[k]$, $I_l[k]$ a $I_p[k]$ jsou brzká, pozdní a okamžitá korelace a ε konstanta, která reprezentuje sklon korelační funkce. Například GPS C/A kód a korelátor, během doby trvání jednoho chipu budou mít ε rovno 2. V zásadě může být použito více schémat DLL (Delay Locked Loop). V případě koherentní smyčky DLL jsou $I_e[k]$, $I_l[k]$ a $I_p[k]$ výstupy korelátoru. V případě nekoherentní smyčky DLL jsou k dispozici dvě řešení: buď výstup soufázové větve korelátoru nebo výstup obou větví. Dále budeme pracovat s výstupem soufázové větve nekoherentní smyčky DLL. V tomto případě mohou být $I_e[k]$, $I_l[k]$ a $I_p[k]$ modelovány jako nezávislé a identicky rozložené Gaussovské procesy. Statisticky nezávislý výstup ve skutečnosti generují vzorky bílého šumu přijatého signálu. [9]

Metrika $M_1[k]$ je zašuměná a předpokládáme, že jsme schopni odhadnout její rozptyl, stejně jako výkon původního signálu. Dále aproximujeme $M_1[k]$ jako Gaussovský proces. Přitom je $M_1[k]$ poměr mezi dvěma Gaussovskými procesy $I_{el}[k] = I_l[k] + I_e[k]$ a $I_p[k]$, jež už není Gaussovský. Nicméně pokud je šum na výstupu okamžitého korelátoru zanedbatelný, $I_p[k]$ může být aproximováno jako známá konstanta. Tato aproximace se může zdát riskantní, ale v praxi dobře funguje, zejména v otevřeném prostranství při vysokém poměru C/N_0. Vezmeme-li v potaz tato zjednodušení, můžeme metriku $M_1[k]$ vyjádřit následovně:

$$M_1[k] = \mu_1[k] + N_1[k] \tag{39}$$

kde $\mu_1[k]$ je střední hodnota signálu a $N_1[k]$ je Gaussovský proces s nulou střední hodnotou a známým rozptylem σ_1^2 šumu. [9]

Pokud máme vypočtenou metriku, je třeba zvolit způsob, jak rozhodnout, zda je přítomno rušení, či nikoliv. Jedna z možných metod je Neyman-Pearsonův detektor (NP), což je binární test hypotéz, který vybere jednu z hypotéz H_0 (pouze signál GPS) a H_1 (přítomnost spoofingu). Tyto hypotézy mohou být formulovány následovně:

$$\mu_1[k] = \begin{cases} \mu_{1,0} \rightarrow H_0 \\ \mu_{1,1} \rightarrow H_1 \end{cases} \quad (40)$$

kde $\mu_1[k]$ je hodnota metriky v okamžiku k, $\mu_{1,0}$ je test podílového kritéria při absenci šumu a spoofingu, $\mu_{1,1}$ je test podílového kritéria při absenci šumu a přítomnosti spoofingu. [9]

Nyní můžeme přejít k NP detektoru, ten je založen na poměru pravděpodobností (LR), která se porovnává s rozhodovací úrovní γ. Pro náš případ lze test poměru pravděpodobností (LRT) vyjádřit jako:

$$L(M_1[k]) = \frac{p(M_1[k]\,;\,H_1)}{p(M_1[k]\,;\,H_0)} > \gamma_{L1} \quad (41)$$

kde γ_{L1} je rozhodovací úroveň, $p(M_1[k]\,;\,H_i)$ je hustota pravděpodobnosti náhodné proměnné $M_1[k]$, když je hypotéza H_i pravda, $i = \{0, 1\}$ a $M_1[k]$ je měřená metrika v době k. Lze dokázat, že tento výraz vede na LRT:

$$M_1[k] > \frac{\sigma_1^2 \ln(\gamma_{L1})}{\mu_{1,1} - \mu_{1,0}} + \frac{\mu_{1,1} + \mu_{1,0}}{2} = \gamma_1 \quad (42)$$

tento vztah platí pro $\Delta\mu = \mu_{1,1} - \mu_{1,0} > 0$. Rozhodovací úroveň je nepřímo úměrný poměru:

$$\rho_s = \frac{\Delta\mu}{\sigma_1} \quad (43)$$

γ_1 se blíží k nekonečnu, když se ρ_s blíží k nule (když se $\mu_{1,1}$ blíží k $\mu_{1,0}$). To je dáno tím, že poměrová metrika je efektivní pouze, pokud se hodnoty $\mu_{1,1}$ a $\mu_{1,}$ výrazně liší, jelikož jsou použity pro rozhodnutí mezi H_0 a H_1. Pokud by si byly rovny, nebylo by rozhodnutí možné. Naopak, vysoké hodnoty ρ_s, pokud je $\Delta\mu$ vysoké a šum je zanedbatelný, vede na nízké hodnoty rozhodovací úrovně. [9]

Funkčnost detektoru lze charakterizovat pomocí pravděpodobnosti detekce a pravděpodobnosti falešného alarmu (P_D a P_{FA}). Tyto pravděpodobnosti se vynesou do grafu, pro dané hodnoty rozhodovací úrovně. Takovému grafu se říká ROC charakteristika (Receiver Operating Characteristic) a slouží k návrhu NP detektoru. NP detekce spočívá v určení hodnoty pravděpodobnosti falešného alarmu a následného získání hodnoty rozhodovací úrovně γ_{L1}. [9]

Z rovnic (38) – (42) a z analýzy statistických parametrů $M_1[k]$, lze teoreticky odvodit vztah pro P_{FA} a P_D:

$$P_{FA} = \int_{\gamma_1}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_1} e^{-\frac{(x-\mu_{1,0})^2}{2\sigma_1^2}} dx = \frac{1}{2} erfc\left(\frac{\gamma_1 - \mu_{1,0}}{\sqrt{2}\sigma_1}\right)$$

$$P_D = \int_{\gamma_1}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_1} e^{-\frac{(x-\mu_{1,1})^2}{2\sigma_1^2}} dx = \frac{1}{2} erfc\left(\frac{\gamma_1 - \mu_{1,1}}{\sqrt{2}\sigma_1}\right) \quad (44)$$

dále:

$$\gamma_1 - \mu_{1,0} = \frac{\sigma_1^2 \ln(\gamma_{L1})}{\Delta\mu} + \frac{\Delta\mu}{2}$$

$$\gamma_1 - \mu_{1,1} = \frac{\sigma_1^2 \ln(\gamma_{L1})}{\Delta\mu} - \frac{\Delta\mu}{2} \quad (45)$$

kde $\Delta\mu$ reprezentuje rozhodovací interval mezi dvěma situacemi: přítomnost spoofingu a absence spoofingu. Dosazením získáme:

$$P_{FA} = erfc\left(\frac{\ln(\gamma_{L1})}{\sqrt{2}\rho_s} + \frac{\rho_s}{2\sqrt{2}}\right)$$

$$P_D = erfc\left(\frac{\ln(\gamma_{L1})}{\sqrt{2}\rho_s} - \frac{\rho_s}{2\sqrt{2}}\right) \quad (46)$$

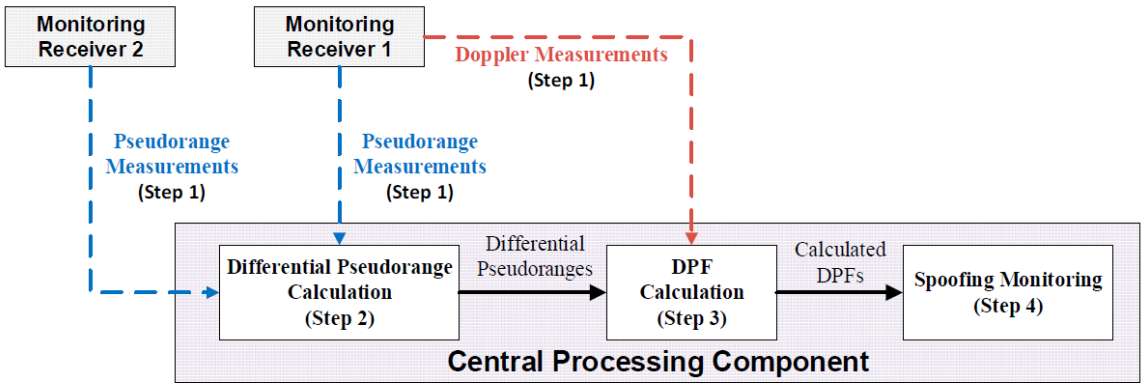
4.2.3 Metoda pro detekci spoofingu založena na monitorování rozdílu pseudovzdálenosti

Tato metoda je založena na principu sítě několika rádiových přijímačů (alespoň dvou) a jedné centrální výpočetní jednotky. Mechanismus pracuje na principu rozdílného TDOA (Time Difference of Arrival) mezi spoofingem a autentickým signálem. TDOA signálů, generovaných stejným spooferem,

jsou běžně identické, zatímco autentické signály z různých směrů se liší. TDOA je měřeno jako poměr rozdílné pseudovzdálenosti k frekvenci nosné vlny (DPF). DPF autentických signálů se liší, zatímco u signálů generovaných spooferem se DPF téměř překrývají. [10]

Architektura monitorovací sítě

Struktura architektury je znázorněna na obrázku 4-2. Skládá se alespoň ze dvou monitorovacích přijímačů a centrální výpočetní jednotky (CPC – Central Processing Component). Monitorovací přijímače jsou určeny k měření pseudovzdálenosti a Dopplerovského posuvu všech přijatých signálů. Tato měření jsou následovně zpracovávána v CPC. CPC se skládá z bloků pro vypočet diferenční pseudovzdálenosti, DPF a vyhodnocování spoofingu. [10]

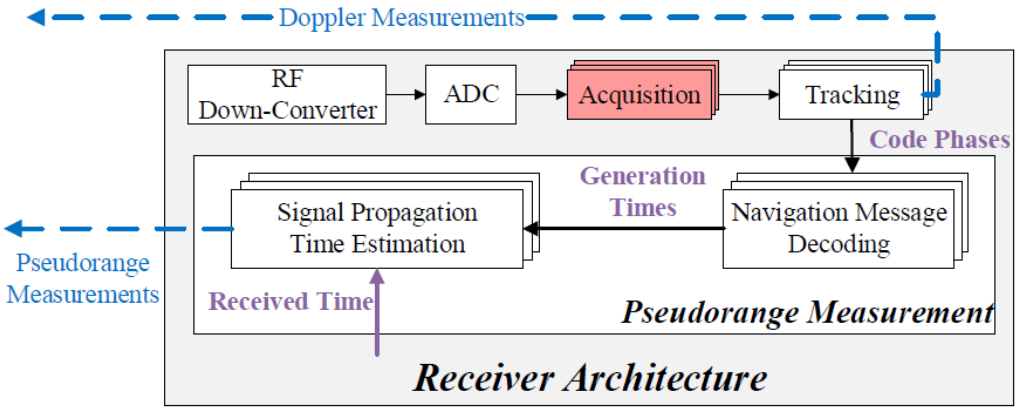


Obrázek 4-2 Architektura monitorovací sítě [10]

Architektura monitorovacího přijímače

V prvním kroku je potřeba určit pseudovzdálenost a Dopplerovský posuv, k tomu slouží monitorovací přijímač, jehož blokové schéma je na obrázku 4-3. Architektura tohoto přijímače je téměř shodná s architekturou klasického GNSS přijímače, až na blok provádějící akvizici. Modifikovaný blok akvizice sleduje všechny signály a následně propouští k dalšímu zpracování signály, které převyšují předem určená rozhodovací úroveň. Následně je potřeba určit odhad Dopplerovského posuvu a fáze kódu přijatých signálů (blok tracking). Fáze kódu je využita pro výpočet pseudovzdálenosti, pomocí rychlosti světla a doby šíření signálu, která je určena jako rozdíl času, kdy je signál vyslán a přijat. Čas vyslání je získán dekódováním navigační zprávy, zatímco čas přijetí je určen pomocí hodin přijímače. V případě přítomnosti spoofingu však není časování GNSS důvěryhodné. To lze vyřešit například použitím NTP (Network Time Protocol). Tato metoda pracuje s přesností v řádu desítek milisekund, což

je pro monitorování spoofingu dostačující. Pseudovzdálenost je společně s Dopplerovskými parametry následovně zpracovávána v CPC. [10]



Obrázek 4-3 Architektura monitorovacího přijímače [10]

Výpočet diferenční pseudovzdálenosti

Diferenční pseudovzdálenost (DP) je učena pomocí pseudovzdáleností získaných z přijímačů. Za přítomnosti spoofingu získáme pseudovzdálenosti jak spoofingu, tak autentického signálu ze všech přijímačů, takže vypočtené DP mohou být dvou nebo tří typů:

- DP mezi spoofingem
- DP mezi autentickými signály
- DP mezi spoofingem a autentickými signály, pokud mají stejné PRN

Tyto tři typy budou popsány později. [10]

Výpočet DPF

DPF se počítá jako poměr mezi DP a frekvencí přijaté nosné vlny. Frekvence přijaté nosné vlny je kombinace frekvence signálu vyslaného ze satelitu a Dopplerovským posuvem, získaným jedním z přijímačů. Z předchozí části vyplývá, že DPF mohou být, stejně jako DP, dvou nebo tří obdobných typů. Tyto tři typy budou rovněž popsány později. [10]

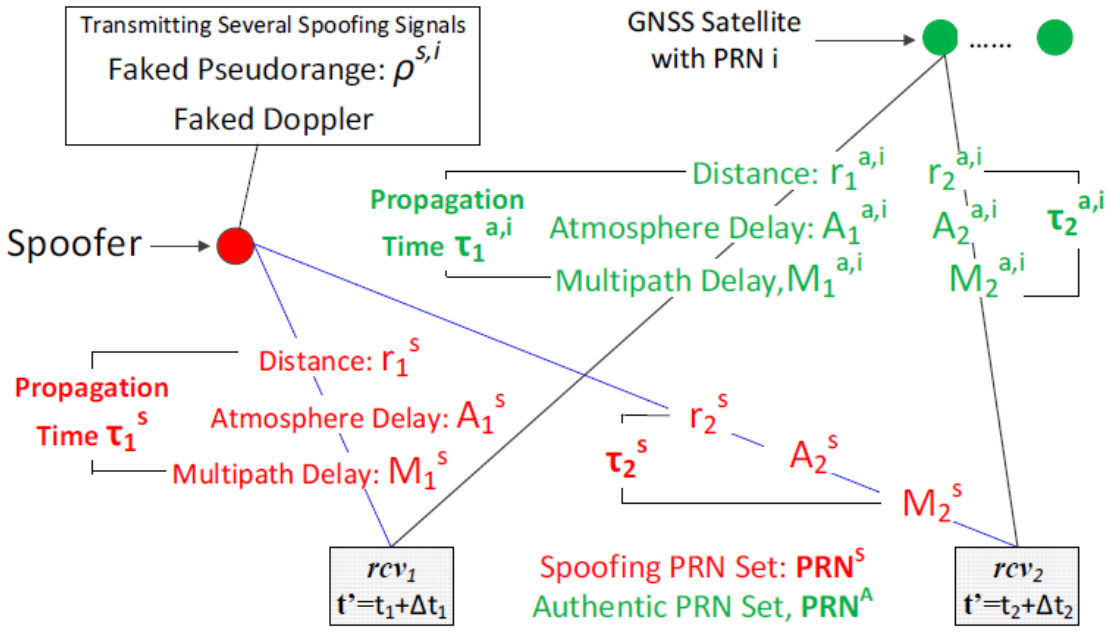
Monitorování spoofingu

V případě nepřítomnosti spoofingu jsou přítomny pouze rozdílné DPF. V případě přítomnosti spoofingu, jak již bylo zmíněno, jsou přítomny i překrývající se DPF. Algoritmus pro monitorování je navržen tak, aby hledal DPF, které se nacházejí v malém předdefinovaném rozsahu. Metoda zahrnuje testování hypotéz a stanovení výše zmíněného malého rozsahu. [10]

DP modely

Nejprve si ukážeme, jak probíhá spoofing. Na obrázku 4-4 je typický scénář spoofingu, který se skládá ze dvou monitorovacích přijímačů, spooferu a několika GNSS satelitů. Předpokládejme, že každý ze dvou přijímačů, rcv_1 a rcv_2, dokáže přijímat oba typy signálu, autentický a spoofing. Chyba hodin přijímače rcv_x je Δt_x. Čas přijímače rcv_x, t' je modelován jako kombinace skutečného času t_x a chyby Δt_x. [10]

$$t' = t_x + \Delta t_x \tag{47}$$



Obrázek 4-4 Scénář spoofingu [10]

Spoofer vysílá několik falešných GNSS signálů s falešným Dopplerovým posuvem a s falešnou fází kódu, která vyústí ve falešnou pseudovzdálenost $\rho^{s,i}$. Předpokládáme, že všechny rušivé signály

jsou generovány společným spooferem, dále předpokládáme, že tyto signály budou alespoň čtyři, aby mohl být přijímač naveden na špatnou lokalitu. PRN množiny pro spoofing a autentický signál jsou označeny jako $\mathbf{PRN^S}$ a $\mathbf{PRN^A}$. Vztah mezi jednotlivými množinami je následující:

$$\mathbf{PRN}^{\mathbf{A}\cap\boldsymbol{S}} = \mathbf{PRN}^{\mathbf{A}} \cap \mathbf{PRN}^{\mathbf{S}}, \mathbf{PRN}^{\mathbf{A-S}} = \mathbf{PRN}^{\mathbf{A}} - \mathbf{PRN}^{\mathbf{S}}, \quad \mathbf{PRN}^{\mathbf{S-A}} = \mathbf{PRN}^{\mathbf{S}} - \mathbf{PRN}^{\mathbf{A}} \tag{48}$$

kde $\mathbf{PRN}^{\mathbf{A}\cap\boldsymbol{S}}$ je průnik $\mathbf{PRN}^{\mathbf{A}}$ a $\mathbf{PRN}^{\mathbf{S}}$, $\mathbf{PRN}^{\mathbf{A-S}}$ náleží $\mathbf{PRN}^{\mathbf{A}}$, ale ne $\mathbf{PRN}^{\mathbf{S}}$, $\mathbf{PRN}^{\mathbf{S-A}}$ náleží $\mathbf{PRN}^{\mathbf{S}}$, ale ne $\mathbf{PRN}^{\mathbf{A}}$. [8]

Když jsou všechny signály zpracovány, pseudovzdálenost pro přijímač rcv_x je:

$$\tilde{\rho}_x = \begin{bmatrix} \tilde{\rho}_x^{a,i}, \tilde{\rho}_x^{s,i} \middle| i \in \mathbf{PRN}^{\mathbf{A}\cap\mathbf{S}} \\ \tilde{\rho}_x^{a,i} \middle| i \in \mathbf{PRN}^{\mathbf{A-S}} \\ \tilde{\rho}_x^{s,i} \middle| i \in \mathbf{PRN}^{\mathbf{S-A}} \end{bmatrix} \tag{49}$$

kde $\tilde{\rho}_x^{a,i}$ a $\tilde{\rho}_x^{s,i}$ jsou autentická pseudovzdálenost a pseudovzdálenost ovlivněná spoofingem v přijímači rcv_x. Index i značí index PRN. $\tilde{\rho}_x^{a,i}$ a $\tilde{\rho}_x^{s,i}$ měřené v čase t' lze vyjádřit jako:

$$\tilde{\rho}_x^{a,i}(t') = \frac{\lambda f^{a,i}}{c}\left[r_x^{a,i}(t') + A_x^{a,i} + M_x^{a,i} + c\Delta t_x\right] + \zeta_x^{a,i} \tag{50}$$

$$\tilde{\rho}_x^{s,i}(t') = \frac{\lambda f^{s,i}}{c}\left[r_x^{s} + A_x^{s} + M_x^{s} + c\Delta t_x\right] + \rho^{s,i}(t') + \zeta_x^{s,i} \tag{51}$$

kde λ je vlnová délka nosné vlny, c je rychlost světla, $f^{s,i}$ ($f^{a,i}$) je přijatá frekvence, kombinace nosné frekvence GNSS a Dopplerova posuvu. r_x^s ($r_x^{a,i}$) je vzdálenost mezi spooferem (satelitem) a rcv_x. A je zpoždění způsobené atmosférou, M je chyba vzniklá vícecestným šířením signálu. $\rho^{s,i}(t')$ je falešná pseudovzdálenost simulovaná spooferem v čase t'. Šum $\zeta_x^{s,i}$($\zeta_x^{a,i}$) bývá modelován jako identická a nezávisle rozdělená (IID – Identical and Independently Distributed) Gaussovská náhodná proměnná s nulovou střední hodnotou a rozptylem σ^2. [10]

Diferenční pseudovzdálenost je počítána jako rozdíl pseudovzdáleností se stejným PRN, které jsou získány dvěma přijímači. Tento rozdíl lze vyjádřit následovně:

$$\Delta\rho = \begin{bmatrix} \Delta\rho^{a,i}, \Delta\rho^{s,i}, \Delta\rho^{a-s,i}, \Delta\rho^{s-a,i,} \middle| i \in \mathbf{PRN}^{\mathbf{A}\cap\mathbf{S}} \\ \Delta\rho^{a,i} \middle| i \in \mathbf{PRN}^{\mathbf{A-S}} \\ \Delta\rho^{s,i} \middle| i \in \mathbf{PRN}^{\mathbf{S-A}} \end{bmatrix} \tag{52}$$

kde:

$$\Delta\rho^{s,i} = \tilde{\rho}_1^{s,i} - \tilde{\rho}_2^{s,i},\ \ \Delta\rho^{a,i} = \tilde{\rho}_1^{a,i} - \tilde{\rho}_2^{s,i}, \Delta\rho^{a-s,i} = \tilde{\rho}_1^{a,i} - \tilde{\rho}_2^{s,i},$$
$$\Delta\rho^{s-a,i} = \tilde{\rho}_1^{s,i} - \tilde{\rho}_2^{a,i} \tag{53}$$

V případě přítomnosti spoofingu může mít vypočtená DP tři typy, DP autentických signálů $\Delta\rho^{a,i}$, DP signálů generovaných spooferem $\Delta\rho^{s,i}$ a DP autentického signálu a signálu generovaným spooferem $\Delta\rho^{a-s,i}$ a $\Delta\rho^{s-a,i}$. Tento typ existuje jen, pokud je $\mathbf{PRN}^{\mathbf{A}\cap\mathbf{S}}$ neprázdná množina. Dosazením rovnic (50) a (51) do rovnice (53) dostaneme vztah pro $\Delta\rho^{s,i}$ a $\Delta\rho^{a,i}$:

$$\Delta\rho^{s,i} = \lambda f^{s,i}(\Delta\tau^s + \Delta M^s + \Delta t) + \Delta\zeta^{s,i} \tag{54}$$

$$\Delta\rho^{a,i} = \lambda f^{a,i}\left(\Delta\tau^{a,i} + \Delta M^{a,i} + \Delta t\right) + \Delta\zeta^{a,i} \tag{55}$$

kde:

$$\Delta\tau^s = \frac{[r_1^s - r_2^s]}{c}, \Delta M^s = M_1^s - M_2^s, \Delta\zeta^{s,i} = \zeta_1^{s,i} - \zeta_2^{s,i}, \Delta t = \Delta t_1 - \Delta t_2,$$
$$\Delta\tau^{a,i} = \frac{\left[r_1^{a,i} - r_2^{a,i}\right]}{c}, \Delta M^{a,i} = M_1^{a,i} - M_2^{a,i}, \Delta\zeta^{a,i} = \zeta_1^{a,i} - \zeta_2^{a,i} \tag{56}$$

V rovnicích (51) a (52) pro $\Delta\rho^{s,i}$ ($\Delta\rho^{a,i}$) je $\Delta\tau^s$ ($\Delta\tau^{a,i}$) vlastně TDOA spoofingu (autentického signálu). Rozdíl zpoždění, vlivem atmosféry, je zanedbatelný pro krátkou výchozí diferenční pseudovzdálenost, což je náš případ, takže jej můžeme zanedbat jak pro $\Delta\rho^{s,i}$, tak pro $\Delta\rho^{a,i}$. Jelikož IID Gaussovský šumy v obou přijímačích ($\zeta_1^{s,i}$ a $\zeta_2^{s,i}$) jsou nekorelovány, $\Delta\zeta^{s,i}$ a $\Delta\zeta^{a,i}$ mohou být modelovány jako IID Gaussovská náhodná proměnná s nulovou střední hodnotou a rozptylem $2\sigma^2$:

$$\Delta\zeta^{s,i} \sim \mathbf{N}\left[0, \sqrt{2}\sigma\right], \Delta\zeta^{a,i} \sim \mathbf{N}\left[0, \sqrt{2}\sigma\right] \tag{57}$$

kde **N**[a, b] značí Gaussovské rozdělení se střední hodnotou *a* a směrodatnou odchylkou *b*. [10]

DPF

DPF jednotlivých signálů se počítá jako poměr diferenční pseudovzdálenosti a přijaté frekvence nosné vlny. Přijatá frekvence je kombinace frekvence původní nosné vlny a Dopplerovského posuvu. Dopplerovský posuv je určen jedním z přijímačů s určitou chybou, která je zanedbatelná, pokud je výrazně menší než frekvence nosné vlny. Pokud budeme vycházet z výpočtu DP (52), dojdeme k tvaru DPF:

$$\mathbf{k} = \begin{bmatrix} k^{a,i}, k^{s,i}, k^{a-s,i}, k^{s-a,i} \middle| i \in \mathbf{PRN}^{\mathbf{A}\cap\mathbf{S}} \\ k^{a,i} \middle| i \in \mathbf{PRN}^{\mathbf{A}-\mathbf{S}} \\ k^{s,i} \middle| i \in \mathbf{PRN}^{\mathbf{S}-\mathbf{A}} \end{bmatrix} \tag{58}$$

kde $k^{s,i} = \frac{\Delta\rho^{s,i}}{\lambda f^{s,i}}$, $k^{a,i} = \frac{\Delta\rho^{a,i}}{\lambda f^{a,i}}$, $k^{a-s,i} = \frac{\Delta\rho^{a-s,i}}{\lambda f^{a,i}}$, $k^{s-a,i} = \frac{\Delta\rho^{s-a,i}}{\lambda f^{s,i}}$. [10]

V případě přítomnosti spoofingu může mít DPF tři typy: DPF mezi autentickými signály: $k^{a,i}$, DPF mezi signály generovanými spooferem: $k^{s,i}$ a DPF mezi autentickým signálem a signálem generovaným spooferem (AS DPF): $k^{s-a,i}$ a $k^{a-s,i}$. Dosazením rovnic (51) a (52) získáme:

$$k^{s,i} = \underbrace{\Delta\tau^s + \Delta M^s + \Delta t}_{identické\ pro\ signály\ generované\ spooferem} + \delta^{s,i} \tag{59}$$

$$k^{a,i} = \underbrace{\Delta\tau^{a,i} + \Delta M^{a,i}}_{liší\ se\ pro\ autentické\ signály} + \Delta t + \delta^{a,i} \tag{60}$$

kde

$$\delta^{s,i} = \frac{\Delta\zeta^{s,i}}{\lambda f^{s,i}}, \qquad \delta^{a,i} = \frac{\Delta\zeta^{a,i}}{\lambda f^{a,i}} \tag{61}$$

lze odvodit [10], že:

$$\delta^{s,i} = \frac{\Delta\zeta^{s,i}}{c}, \qquad \delta^{s,i} \sim \mathbf{N}[0, \sigma_\delta]$$

$$\delta^{a,i} = \frac{\Delta\zeta^{a,i}}{c}, \qquad \delta^{a,i} \sim \mathbf{N}[0, \sigma_\delta] \tag{62}$$

kde $\sigma_\delta = \sqrt{2}\sigma/c$. [10]

Bylo ukázáno, že jak autentická DPF, tak DPF spoofingu se sestává ze čtyř částí: TDOA, vícecestné šíření, rozdíl hodin a odhad šumu DPF. První tři části jsou pro spoofing identické, jelikož

jsou signály vysílány ze stejného zdroje, je tedy patrné, že nebýt šumu, DPF spoofingu by se kompletně překrývaly. Naproti tomu TDOA a rozdíly vícecestným šířením jsou u autentického signálu rozdílné, jelikož signály přichází k přijímači z jiných směrů. [10]

Složky $k^{s-a,i}$ a $k^{a-s,i}$ jsou z hlediska monitorovací techniky, použité v této metodě nezajímavé, proto nebyly dále rozvedeny. [10]

Jelikož $\Delta\zeta^{s,i}$ je IID Gaussovská náhodná proměnná, šum DPF $\delta^{s,i}$ je také IID. Potom DPF $k^{s,i}$ sestávající se z identických $\Delta\tau^s$, ΔM^s, Δt a IID Gaussovských náhodných proměnných $\delta^{s,i}$, jsou identicky a nezávisle Gaussovsky rozložené:

$$k^{s,i} \sim \mathbf{N}[\Delta\tau^s + \Delta M^s + \Delta t, \sigma_\delta] \tag{63}$$

Metodika monitorování spoofingu

a) Testování hypotéz

Monitorování spoofingu je založeno na vypočtených DPF. V případě absence spoofingu vypočtené DPF obsahují pouze rozdílné autentické DPF. V případě přítomnosti spoofingu obsahují DPF jak autentické DPF, tak téměř se překrývající DPF spoofingu. Již bylo řečeno, že se předpokládá přítomnost alespoň čtyř signálů generovaných spooferem. Tedy v případě přítomnosti spoofingu musí být přítomny, alespoň čtyři, téměř se překrývající DPF s různými PRN. Monitorování spoofingu je navrženo jako hledání, alespoň čtyř, téměř se překrývajících DPF s rozdílnou PRN v malém předdefinovaném rozsahu. Nulová hypotéza H_0 zastupující možnost absence spoofingu a alternativní hypotéza H_1 zastupující možnost přítomnosti spoofingu jsou formulovány následovně:

$$\begin{aligned} H_0 &: N(R) < 4 \\ H_1 &: N(R) \geq 4 \end{aligned} \tag{64}$$

kde $N(R)$ reprezentuje počet DPF (s rozdílnou PRN), které jsou v předdefinovaném rozsahu R. Správné určení R je klíčové pro fungování tohoto procesu. Chybné určení R vyústí v malou pravděpodobnost detekce nebo naopak ve vysokou pravděpodobnost falešného alarmu. [10]

b) Dolní hranice pravděpodobnosti detekce

Založeno na testování hypotéz, pravděpodobnost detekce P_d je definována jako pravděpodobnost jevu, kdy alespoň čtyři DPF spoofingu budou v předdefinovaném rozsahu *R*:

$$P_d = \Pr\{N(R) \geq 4\} \tag{65}$$

kde Pr{x} značí pravděpodobnost jevu x. P_d roste s počtem přijatých signálů spoofingu, *m*. Jelikož *m* nelze na straně přijímače nijak ovlivnit, budeme dále uvažovat nejhorší možný případ, tedy $m = 4$. P_d se v takovém případě označuje jako dolní hranice pravděpodobnosti detekce $\tilde{P}_d$:

$$P_d \geq \tilde{P}_d = \Pr\{N(R) \geq 4 | m = 4\} = Pr\{N(R) = 4 | m = 4\} \tag{66}$$

Druhá rovnost uvažuje v potaz, že *N*(*R*) nemůže být větší než 4, protože *N*(*R*) je vždycky rovno nebo menší než celkový počet DPF, *m*. Dále je dáno, že čtyři DPF spoofingu budou v rozsahu *R* jen a pouze, když rozsah těchto čtyř DPF bude menší než *R*, $\tilde{P}_d$ je potom:

$$\tilde{P}_d = \Pr\{\max(DPF) - \min(DPF) \leq R\} = Pr\{r(4) \leq R\} \tag{67}$$

kde *r*(*x*) značí rozsah *x* DPF spoofingu, což je rozdíl mezi maximálním a minimálním prvkem DPF. Kumulativní distribuční funkce (cdf) rozsahu *r*(*4*), $F_{r(4)}$, je odvozena v [8] a má tvar:

$$F_{r(4)}(R) = \Pr\{r(4) \leq R\} = 4 \int_{-\infty}^{\infty} g'(x) \left[G'\left(x + \frac{R}{\sigma_\delta}\right) - G'(x) \right]^3 dx \tag{68}$$

kde g' a G' je hustota pravděpodobnosti a cdf Gaussovského procesu s nulovou střední hodnotou a jednotkovým rozptylem. Pokud vyjdeme z rovnic (67) a (68) můžeme vyjádřit $\tilde{P}_d$ jako :

$$\tilde{P}_d = F_{r(4)}(R) \tag{69}$$

Z rovnice (69) můžeme vyjádřit *R* v závislosti na požadované pravděpodobnosti detekce: [10]

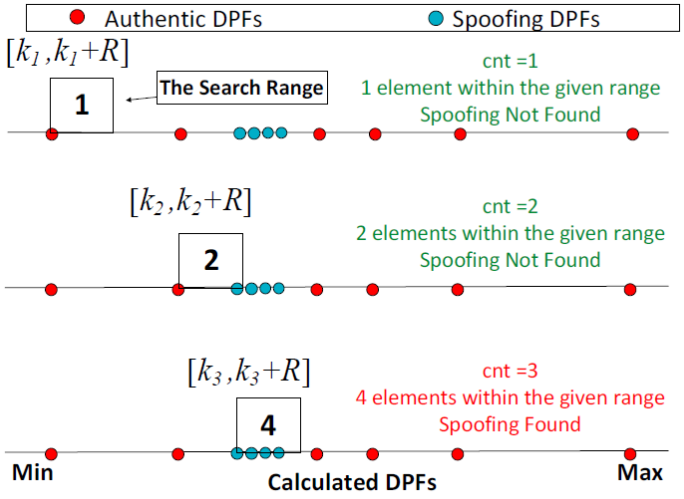
$$R = F_{r(4)}^{-1}(\tilde{P}_d) \tag{70}$$

c) Algoritmus pro testování hypotéz

Algoritmus se skládá ze šesti kroků:

- Definování *R* podle rovnice (70)
- Seřazení vypočtených DPF od nejmenší po největší: $[k_1 \leq k_2 \ldots \leq k_n]$
- Vytvoření čítače *cnt* a přiřazení hodnoty 1
- Vytvoření vyhledávacího rozsahu $[k_{cnt}, k_{cnt} + R]$ a výpočet počtu prvků v tomto rozsahu
- Pokud je počet prvků roven nebo vetší než čtyři, spoofing je přítomen. Jinak se postupuje ke kroku 6
- Inkrementace čítače *cnt*: *cnt* = *cnt* + 1. Opakování od kroku 4 [10]

Na obrázku 4-5 je ilustrace výše popsaného algoritmu. V prvním případě, kdy je *cnt* = 1, je ve vyhledávacím rozsahu pouze jeden prvek, což znamená, že spoofing nebyl nalezen. Ve druhém případě, *cnt* = 2, jsou ve vyhledávacím rozsahu 2 prvky, takže spoofing opět nebyl nalezen. Ve třetím kroku, *cnt* = 3, jsou ve vyhledávacím rozsahu 4 prvky, je přijata alternativní hypotéza H_1, tedy že je přítomen spoofing. [10]



Obrázek 4-5 Ilustrace algoritmu pro testování hypotéz [10]

5. Lokalizace zdroje rušení

5.1 Přehled základních technik pro lokalizaci rádiových signálů

Pokud chceme zjistit polohu zdroje signálu, je třeba odhadnout parametry vztažené k energii, úhlu, času nebo frekvenci signálu. V případě rušení je tato situace ještě komplikovanější, jelikož nemáme žádné informace o zdroji, který signál vysílá. [11]

Konkrétní metody pro lokalizaci rušení používají následující techniky, nebo jejich určitou modifikaci, či kombinaci [11]:

- RSS (Received Signal Strength) – úroveň přijatého signálu
- AOA (Angle Of Arrival) – úhel přijetí signálu
- TDOA – rozdíl času při přijetí signálu
- FDOA (Frequency Difference Of Arrival) – rozdíl frekvencí při přijetí signálu

a) RSS

Systémy pracující s technikou RSS využívají síť přijímačů, každý z přijímačů vyhodnotí sílu přijatého signálu. Ve většině případů je vzdálenost zdroje rušení určena pomocí modelu pro ztráty šířením signálu (path-loss):

$$\mathrm{RSS_i} = P_0 - 10n\, log_{10}\left(\frac{d_i}{d_0}\right) + \sigma_i \tag{71}$$

kde RSS_i je RSS *i*-tého přijímače, P_0 je přijatý výkon v referenční vzdálenosti d_0 od vysílače, n je koeficient útlumu, d_i je hledaná vzdálenost a σ_i je směrodatná odchylka pro pomalé úniky. Pro výpočet vzdálenosti pomocí RSS potřebujeme znát P_0 a d_0 a n a σ_i známe pouze pokud předem známe místo měření, a i potom jde jen o hrubé odhady. Alternativou může být použití modelu, který místo P_0 využívá vysílaný výkon, ten je ovšem také neznámý. To lze využit modifikací této techniky na DRSS (Difference Received Signal Strength), kdy je problém neznámého vysílacího výkonu vyřešen odečtením dvou RSS [11]:

$$\mathrm{DRSS_{i-j}} = \mathrm{RSS}_i - \mathrm{RSS}_j = 10n\, log_{10}\left(\frac{d_j}{d_i}\right) + \sigma_i + \sigma_j \tag{72}$$

b) AOA

Systémy, využívající AoA, k určení polohy zdroje rušení využívají informaci o směru příchodu signálu. Ve většině případů tuto informaci získají pomocí anténní řady, je však možné použít jednu rotující a pohybující se anténu. My se však budeme zabývat první variantou. Pro tangens úhlu fixní anténní řady, ve 2D platí vztah:

$$\tan(\theta_i) = \frac{y_i - y}{x_i - x} \tag{73}$$

kde θ_i je změřený úhel i-tým senzorem ve směru podle hodinových ručiček, vztaženo k severu, pro každý senzor. Například $\theta_1 = 315°$, (x, y) reprezentuje polohu zdroje a (x_i, y_i) je poloha senzoru. Protože metrikou pro tento systém jsou úhly, čím dál od zdroje se senzor nachází, tím větší je chyba určení polohy. [11]

c) TDOA

Tato technika funguje na principu snímání signálu senzory rozloženými v prostoru a měření časového rozdílu přijetí signálu. Časový rozdíl je přepočten na rozdíl ve vzdálenosti. V případě lokalizace rušení se přijímá signál v každém uzlu sítě senzorů a počítá se vzájemná korelace přijatých signálů, pro zjištění rozdílu času, kdy byl signál přijat. To vyžaduje precizní synchronizaci mezi jednotlivými senzory. Ve 2D jsou křivky polohy hyperboly, ve 3D se jedná o hyperboloidy. Pro 2D platí:

$$\Delta t_{i,j} c = \sqrt{(x_i - x)^2 + (y_i - y)^2} - \sqrt{(x_j - x)^2 + (y_j - y)^2} \tag{74}$$

kde (x, y) reprezentuje polohu zdroje rušení, (x_i, y_i), (x_j, y_j) reprezentuje polohu dvojice přijímačů i a j, $i = 1, \dots, M-1$ a $j = 2, \dots, M$, kde M je počet přijímačů a $i \neq j$. c je rychlost světla a $\Delta t_{i,j}$ jsou měření TDOA mezi přijímači. [11]

d) FDOA

Pro úplnost je třeba zmínit i techniku FDOA. Základním principem fungování této metody je předpoklad, že se buď zdroj rušení, nebo systém, který jej má lokalizovat pohybuje, což způsobuje rozdílný Dopplerův posuv, který se následovně vyhodnocuje a slouží k určení polohy.[11]

5.2 Algoritmy pro odhad AoA využívající signálového podprostoru

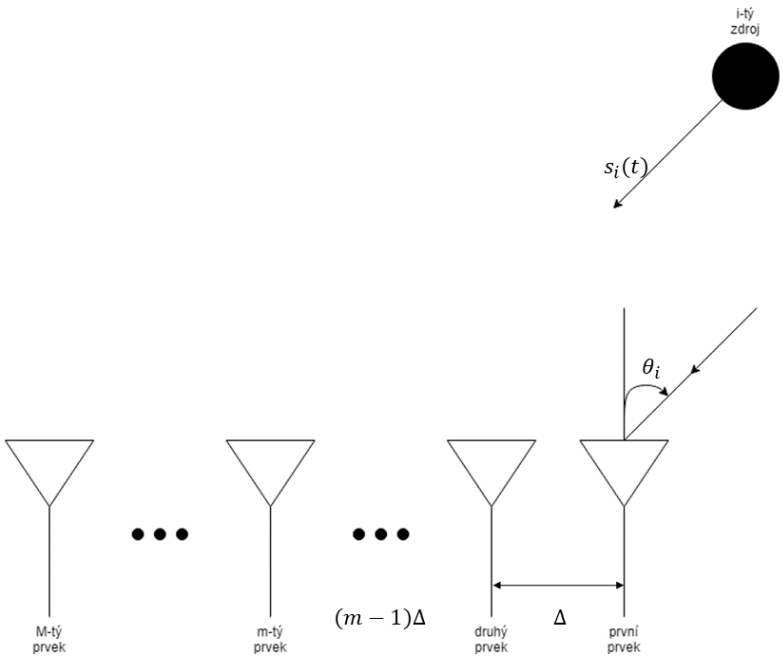
V této podkapitole budou představeny dva algoritmy, MUSIC (Multiple Signal Classification) a ESPRIT (Estimation of Signal Parameters via Rotational Invariance). Nejprve si definujeme model signálu pro výše zmíněné algoritmy, poté si předvedeme samotné algoritmy MUSIC a ESPRIT a následně některé algoritmy pro předzpracování signálu.

5.2.1 Model signálu

Pro algoritmy, v této kapitole, budeme uvažovat následující předpoklady:

- Izotropní a lineární prostředí: fyzikální vlastnosti prostředí jsou stejné ve všech možných směrech, signály mohou být v libovolném bodě lineárně superponovány.
- Předpoklad vzdáleného pole: všechny zdroje signálu jsou dostatečně daleko od anténní řady, takže vlna dopadající na anténní řadu může být považována za rovinnou.
- Předpoklad úzkopásmovosti.
- AWGN kanál.

Jako anténní řadu budeme předpokládat uniformní lineární řadu (ULA), sestávající se z M identických a všesměrových prvků, které jsou rozprostřeny v přímce se stejnou vzdáleností mezi prvky. Vzdálenost mezi dvěma prvky budeme označovat Δ. Úhel, pod kterým bude signál dopadat na i-tý prvek řady, budeme označovat θ_i, viz obrázek 5-1. [12]



Obrázek 5-5.1 Model signálu

Předpokládejme, že rovinná vlna, generovaná zdrojem *i* dopadá na řadu pod úhlem θ_i a signál generovaný zdrojem *i* je úzkopásmový signál $s_i(t)$. Ten pak urazí vzdálenost *d*, rychlostí *c* a dopadne na první prvek (zprava), signál dopadající na první prvek řady, je tedy zpožděná verze signálu $s_i(t)$ se zpožděním $\tau = d/c$. Tedy:

$$s_{i1}(t) = s_i(t-\tau) = \alpha_i(t-\tau)\cos[2\pi f_c(t-\tau) + \beta_i(t-\tau)] = \mathcal{R}\{s_i(t)\} \qquad (75)$$

kde $\alpha_i(t)$ a $\beta_i(t)$ jsou pomalu se měnící amplituda a fáze signálu a f_c je frekvence nosné vlny. Protože jsou prvky v ULA za sebou v přímce, signál dopadající na *m*-tý prvek urazí větší vzdálenost v porovnání s prvkem vpravo od něj. Tato vzdálenost může být vyjádřena jako:

$$\Delta_{mi} = (m-1)\Delta\sin\theta_i \qquad (76)$$

Je zřejmé, že signál, který dopadne na *m*-tý prvek nabere zpoždění:

$$\tau_{mi} = \frac{\Delta_{mi}}{c} = (m-1)\frac{\Delta\sin\theta_i}{c} \qquad (77)$$

Signál přijatý *m*-tým prvkem je potom zpožděnou verzí signálu $s_{i1}(t)$, který je přijat prvním prvkem, se zpožděním τ_{mi}:

$$
\begin{aligned}
&s_{im} = s_i(t - \tau_{mi}) = s_i(t - \tau - \tau_{mi}) \\
&= \alpha_i(t - \tau - \tau_{mi})cos[2\pi f_c(t - \tau - \tau_{mi}) + \beta_i(t - \tau - \tau_{mi})] \\
&\approx \alpha_i(t - \tau)cos[2\pi f_c(t - \tau) + \beta_i(t - \tau) - (m-1)\mu_i] \\
&= \mathcal{R}\{s_i(t)e^{j(m-1)\mu_i}\}
\end{aligned}
\tag{78}
$$

kde $\mu_i = -\frac{2\pi f_c}{c}\Delta sin\theta_i = -\frac{2\pi}{\lambda}\Delta sin\theta_i$ je prostorová frekvence. Z rovnice (78) plyne, že signál přijatý *m*-tým prvkem z *i*-tého zdroje je stejný jako signál přijatý prvním prvkem a liší se pouze posuvem fáze, daným členem $e^{j(m-1)\mu_i}$. Tento člen je závislý pouze na prostorové frekvence a na pozici daného prvku vztažené k prvnímu prvku řady. Pro každý úhel θ_i daným zdrojem, existuje odpovídající prostorová frekvence μ_i. Cílem úlohy určení úhlu dopadu signálu je tedy získat prostorovou frekvenci ze signálů přijatých anténní řadou. [12]

K tomu aby bylo možné určit θ_i z μ_i, musí být ve vztahu jedna k jedné, v důsledku čehož musí být prostorové frekvence omezeny v intervalu $-\pi \leq \mu_i \leq \pi$ a úhly dopadu signálu jsou omezeny na intervalu $-90° \leq \theta_i \leq 90°$. Toho dosáhneme, pokud od sebe budou jednotlivé prvky anténní řady vzdáleny $\Delta = \lambda/2$. Pokud bychom tuto podmínku nedodrželi, vznikl by prostorový aliasing, analogický k aliasingu vznikajícím při nedodržení vzorkovacího teorému. [12]

Všechny signály generovány z *d* zdrojů signálu, $s_i(t)$, $1 \leq i \leq d$, včetně šumu, přijaty m-tým prvkem v okamžiku *t* mohou být vyjádřeny následovně:

$$
\begin{aligned}
&x_m = \sum_{i=1}^{d} s_i(t) + n_m(t) = \sum_{i=1}^{d} s_i(t)e^{j(m-1)\mu_i} + n_m(t) \\
&s_i(t)\sum_{i=1}^{d} e^{j(m-1)\mu_i} + n_m(t) \\
&m = 1,2,\dots,M
\end{aligned}
\tag{79}
$$

Rovnice (79) může být přepsána do maticového zápisu následovně:

$$
\boldsymbol{x}(t) = [\boldsymbol{a}(\mu_1), \boldsymbol{a}(\mu_2), \dots, \boldsymbol{a}(\mu_d)\,]\begin{bmatrix} s_1(t) \\ s_2(t) \\ \vdots \\ s_d(t) \end{bmatrix} + \boldsymbol{n}(t) = \mathbf{A}\boldsymbol{s}(t) + \boldsymbol{n}(t) \tag{80}
$$

kde $\mathbf{x}(t) = [x_1(t), x_2(t), \dots, x_M(t)]^T$ je sloupcový vektor přijatých dat, $\boldsymbol{s}(t) = [x_1(t), x_2(t), \dots, x_M(t)]^T$ je sloupcový vektor signálů, generovaných zdrojem signálu, $\mathbf{n}(t)$ je

prostorově nekorelovaný aditivní šum, s nulovou střední hodnotou a s prostorovou kovarianční maticí rovnou $\sigma_N^2\mathbf{I}_M$ ($\mathbf{I}_M$ je jednotková matice o rozměru *M*x*M*). Řídící vektor řady $\boldsymbol{a}(\mu_i)$ je definován jako:

$$\boldsymbol{a}(\mu_i) = \left[1\ e^{j\mu_i}\ e^{j2\mu_i}\ \ldots\ e^{j(M-1)\mu_i}\right]^T \tag{81}$$

Jsou to funkce neznámé prostorové frekvence μ_i a tvoří sloupce řídící matice **A** o rozměru *M*x*d*: [12]

$$\mathbf{A} = [\boldsymbol{a}(\mu_1)\ \ldots\ \boldsymbol{a}(\mu_i)\ \ldots\ \boldsymbol{a}(\mu_d)] \tag{82}$$
$$= \begin{bmatrix} 1 & 1 & \cdots & 1 \\ e^{j\mu_1} & e^{j\mu_2} & \cdots & e^{j\mu_d} \\ \cdots & \cdots & \cdots & \cdots \\ e^{j(M-1)\mu_1} & e^{j(M-1)\mu_2} & \ldots & e^{j(M-1)\mu_d} \end{bmatrix}$$

5.2.2 MUSIC

MUSIC je jednou z nejpopulárnějších a zároveň nejstarších technik pro zjištění úhlu příchodu signálu s vysokým rozlišením. [12]

Prvním krokem algoritmu bude zjištění odhadu kovarianční matice vstupního signálu, ta má, vzhledem k definovanému modelu signálu, následující tvar:

$$\mathbf{R}_{xx} = \mathbf{A}\mathbf{R}_{ss}\mathbf{A}^H + \boldsymbol{\sigma}_N^2\mathbf{I}_M \tag{83}$$

kde $\mathbf{R}_{ss}$ je kovarianční matice signálu generovaného zdrojem, $\boldsymbol{\sigma}_N^2$ je rozptyl šumu, $\mathbf{I}_M$ je jednotková matice o rozměru *M*x*M*. Předpokládejme, že vlastní čísla matice $\mathbf{R}_{xx}$ jsou $\{\lambda_1, \ldots, \lambda_M\}$, takže:

$$|\mathbf{R}_{xx} - \lambda_i\mathbf{I}_M| = 0 \tag{84}$$

poté získáme substitucí:

$$\left|\mathbf{A}\mathbf{R}_{ss}\mathbf{A}^H + \boldsymbol{\sigma}_N^2\mathbf{I}_M - \lambda_i\mathbf{I}_M\right| = 0 \tag{85}$$

nechť má $\mathbf{A}\mathbf{R}_{ss}\mathbf{A}^H$ vlastní čísla e_i, potom: [12]

$$e_i = \lambda_i - \sigma_N^2 \tag{86}$$

Jelikož je matice **A** složená z řídících vektorů řady, které jsou lineárně nezávislé, má plnou sloupcovou hodnost a kovarianční matice $\mathbf{R}_{ss}$ je nesingulární, pokud nejsou dopadající signály silně korelované. [12]

Lze dokázat, že plná hodnost **A** a nesingularita $\mathbf{R}_{ss}$ zajišťují, že pokud je počet dopadajících signálů *d* menší než počet prvků *M*, matice $\mathbf{A}\mathbf{R}_{ss}\mathbf{A}^H$ bude pozitivně semidefinitní s hodností *d*. Z toho plyne, že *M* – *d* vlastních čísel e_i bude rovno nule. Z rovnice (86) vyplývá, že *M* – *d* vlastních čísel $\mathbf{R}_{xx}$ bude odpovídat rozptylu šumu σ_N^2 a zároveň to budou vlastní čísla nejmenší:

$$\lambda_{d+1} = \dots \lambda_M = \lambda_{min} = \sigma_N^2 \tag{87}$$

Pokud tedy určíme násobnost nejmenšího vlastního čísla *k*, jsme schopni odhadnout počet signálů jako $d = M - k$. [12]

V praxi je ovšem kovarianční matice pouze odhadnuta z konečného počtu vzorků, v důsledku čehož si nebudou všechny vlastní čísla, odpovídající šumovému prostoru, rovna. V podkapitole 5.3.4 budou představeny techniky pro odhad počtu signálů, v této kapitole budeme pro jednoduchost uvažovat teoretické hodnoty vlastních čísel. [12]

Vlastní vektory odpovídající příslušnému vlastnímu číslu λ_i, označované $\mathbf{q}_i$ splňují:

$$(\mathbf{R}_{xx} - \lambda_i \mathbf{I}_M)\mathbf{q}_i = 0, \qquad i = d+1, d+2, \dots, M \tag{88}$$

pro t vlastní vektory, které odpovídají *M* – *d* nejmenším vlastním číslům platí:

$$(\mathbf{R}_{xx} - \lambda_i \mathbf{I}_M)\mathbf{q}_i = \mathbf{A}\mathbf{R}_{ss}\mathbf{A}^H\mathbf{q}_i + \boldsymbol{\sigma}_N^2\mathbf{I}_M\mathbf{q}_i - \boldsymbol{\sigma}_N^2\mathbf{q}_i = \mathbf{A}\mathbf{R}_{ss}\mathbf{A}^H\mathbf{q}_i = 0 \tag{89}$$

Jelikož **A** má plnou hodnost a $\mathbf{R}_{ss}$ je nesingulární, tak:

$$\mathbf{A}^H\mathbf{q}_i = 0 \tag{90}$$

to znamená, že vlastní vektory odpovídající *M* – *d* nejmenším vlastním číslům jsou ortogonální na *d* řídící vektory z **A**: [12]

$$\{\boldsymbol{a}(\theta_d), \dots, \boldsymbol{a}(\theta_d)\} \perp \{\boldsymbol{q}_1, \dots, \boldsymbol{q}_M\} \tag{91}$$

To znamená, že můžeme odhadnout řídící vektory odpovídající přijatým signálům tak, že najdeme řídící vektory, které jsou ortogonální k $M - d$ vlastním vektorům odpovídajícím vlastním číslům $\mathbf{R}_{\boldsymbol{xx}}$, která jsou přibližně rovna σ_N^2. [12]

Vlastní vektory kovarianční matice $\mathbf{R}_{\boldsymbol{xx}}$ patří do jednoho ze dvou na sebe ortogonálních podprostorů, jedním je hlavní podprostor (signálový) a druhý je vedlejší podprostor (šumový). Řídící vektory odpovídající AoA signálu, leží v signálovém podprostoru a jsou tedy ortogonální na šumový podprostor. AoA může být nalezeno hledáním, přes všechny možně řídící vektory řady, těch vektorů které jsou kolmé vlastní vektory z vedlejšího, šumového podprostoru. [12]

Pro zformování šumového podprostoru musíme nejdřív vytvořit matici obsahující vlastní vektory odpovídající šumu:

$$\mathbf{V}_n = [\boldsymbol{q}_{d+1}, \dots, \boldsymbol{q}_M] \tag{92}$$

Jelikož řídící vektory ze signálového podprostoru jsou ortogonální na vlastní vektory ze šumového podprostoru, $\boldsymbol{a}^H(\theta)\mathbf{V}_n\mathbf{V}_n^H\boldsymbol{a}(\theta) = 0$ pro $\theta = \theta_i$ odpovídající dopadajícímu signálu. Poté můžeme zavést spektrum MUSIC následovně:

$$P(\theta) = P_{MUSIC}(\theta) = \frac{1}{\boldsymbol{a}^H(\theta)\mathbf{V}_n\mathbf{V}_n^H\boldsymbol{a}(\theta)} \tag{93}$$

AoA získáme hledáním *d* největších vrcholů v MUSIC spektru. [12]

5.2.3 ESPRIT

Algoritmus ESPRIT předpokládá, že se anténní řada skládá ze dvou identických řad. Ty se mohou překrývat, ve smyslu, že prvek jedné řady může být i prvkem druhé řady. Každý prvek může mít libovolnou polarizaci, směrovost, pokud bude mít každý identické „dvojče“ v druhé komplementární řadě. Prvky každého páru identických senzorů jsou fyzicky odděleny fixním translačním vektorem. Celá řada poté má translační invarianci (prvky řady jsou v párech se stejnými translačními vektory). [12]

Předpokládejme, že *d* signálů dopadá na anténní řadu. Nechť $\boldsymbol{x}_1(t)$ a $\boldsymbol{x}_2(t)$ reprezentují signál přijatý dvěma komplementárními řadami společně s aditivními šumy $\boldsymbol{n}_1(t)$ a $\boldsymbol{n}_2(t)$. Každá z komplementárních řad má *m* prvků. Přijaté signály můžeme zapsat jako:

$$\boldsymbol{x}_1(t) = [\boldsymbol{a}(\mu_1), \dots, \boldsymbol{a}(\mu_d)] \begin{bmatrix} s_1(t) \\ s_2(t) \\ \vdots \\ s_d(t) \end{bmatrix} + \boldsymbol{n}(t) = \mathbf{A}\boldsymbol{s}(t) + \boldsymbol{n}_1(t) \tag{94}$$

$$\boldsymbol{x}_2(t) = \left[\boldsymbol{a}(\mu_1)e^{j\mu_1}, \dots, \boldsymbol{a}(\mu_d)e^{j\mu_d}\right] \begin{bmatrix} s_1(t) \\ s_2(t) \\ \vdots \\ s_d(t) \end{bmatrix} + \boldsymbol{n}(t) = \mathbf{A}\boldsymbol{\Phi}\boldsymbol{s}(t) + \boldsymbol{n}_2(t) \tag{95}$$

kde $\boldsymbol{x_1}(t)$ a $\boldsymbol{x_2}(t)$ jsou vektory *m* x 1 reprezentující data přijatá anténními řadami, $\boldsymbol{n_1}(t)$ a $\boldsymbol{n_2}(t)$ jsou vektory *m* x 1 reprezentující šumy. **A** je řídící vektor *m* x *d*. $\boldsymbol{\Phi} = diag\left[e^{j\mu_1}, \dots, e^{j\mu_d}\right]$ je diagonální matice *d* x *d*, která uvádí do souvislosti signály z obou komplementárních řad a říká se jí rotační operátor. Rovnice (94) a (95) lze přepsat do tvaru pro celkovou řadu: [12]

$$\boldsymbol{x}(t) = \begin{bmatrix} \boldsymbol{x}_1(t) \\ \boldsymbol{x}_2(t) \end{bmatrix} = \begin{bmatrix} \mathbf{A} \\ \mathbf{A}\boldsymbol{\Phi} \end{bmatrix} \boldsymbol{s}(t) + \begin{bmatrix} \boldsymbol{n}_1(t) \\ \boldsymbol{n}_2(t) \end{bmatrix} = \widetilde{\mathbf{A}}\boldsymbol{s}(t) + \boldsymbol{n}(t) \tag{96}$$

Cílem algoritmu ESPRIT je určit odhad AoA pomocí odhadu μ_i určením **Φ.** To je možné ve dvou krocích, určit odhad signálového podprostoru a poté určit rotační operátor.[12]

Nechť jsou $\boldsymbol{E}_1$ a $\boldsymbol{E}_2$ množiny vektorů patřící do signálového podprostoru, který je ideálně rozložen do sloupců **A**. Signálový podprostor lze získat pomocí kovarianční matice, která má tvar:

$$\mathbf{R}_{\boldsymbol{xx}} = \widetilde{\mathbf{A}}\mathbf{R}_{\boldsymbol{ss}}\widetilde{\mathbf{A}}^{\boldsymbol{H}} \tag{97}$$

Předpokládáme, že $\mathbf{R}_{ss}$ i $\widetilde{\mathbf{A}}$ mají plnou hodnost *d*. Signálový prostor je rozložen jako $\mathbf{E}_s = [\mathbf{e}_1, \dots, \mathbf{e}_d]$. Jelikož má $\mathbf{R}_{ss}$ má plnou hodnost, je $\mathbf{E}_s$ ve stejném prostoru jako $\widetilde{\mathbf{A}}$. Jako důsledek musí jednoznačně existovat nesingulární matice **T** taková:

$$\mathbf{E}_s = \widetilde{\mathbf{A}}\mathbf{T} \tag{98}$$

Signálový podprostor $\mathbf{E}_s$ můžeme rozdělit na $\mathbf{E}_1$ a $\mathbf{E}_2$, tedy signálové podprostory jednotlivých anténních řad:

$$\mathbf{E}_s = \begin{bmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{AT} \\ \mathbf{A\Phi T} \end{bmatrix} \tag{99}$$

Signálový podprostor $\mathbf{E}_s$ lze z kovarianční matice získat pomocí zobecněného rozkladu na vlastní čísla a vektory a následnému určení d vlastních vektorů $[\boldsymbol{e}_1, \dots, \boldsymbol{e}_d\ ]$ odpovídajícím d největším vlastním číslům $[\boldsymbol{\lambda}_1, \dots, \boldsymbol{\lambda}_d\ ]$:[12, 13]

$$\mathbf{R}_{xx}\mathbf{E} = \mathbf{IE\Lambda} \tag{100}$$

$$\mathbf{E}_s = [\boldsymbol{e}_1, \dots, \boldsymbol{e}_d\ ] = \begin{bmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{bmatrix} \tag{101}$$

kde $\mathbf{\Lambda}$ je diagonální matice, která má na diagonále vlastní čísla kovarianční matice $\mathbf{R}_{xx}$.

Protože jsou obě anténní řady identicky konfigurovány, sdílejí stejný signálový podprostor a mají stejnou dimenzi, z čehož vyplývá, že lze nalézt nesingulární matici d x d značenou $\mathbf{\Psi}$:

$$\mathbf{E}_1\mathbf{\Psi} = \mathbf{E}_2 \rightarrow \mathbf{AT\Psi} = \mathbf{A\Phi T} \tag{102}$$

rovnici (102) lze vyřešit pomocí metody nejmenších čtverců nebo pomocí metody úplných nejmenších čtverců (TLS) poté získáme: [12, 15]

$$\mathbf{\Psi} = \mathbf{T}^{-1}\mathbf{\Phi T} \tag{103}$$

Je patrné, že $\mathbf{\Psi}$ a $\mathbf{\Phi}$ jsou svázány přes vlastní čísla. Diagonální prvky vlastní čísla $\mathbf{\Phi}$ jsou rovny vlastním číslům $\mathbf{\Psi}$**,** která rotuje m rozměrný signálový podprostor matice $\mathbf{E}_1$ spojenou s první anténní řadou, na m rozměrný signálový podprostor matice $\mathbf{E}_2$ spojenou s druhou anténní řadou. Algoritmus ESPRIT tedy nehledá přímo $\mathbf{\Phi}$, ale hledá $\mathbf{\Psi}$ a následně jeho vlastní čísla $[\phi_1, \dots, \phi_d]$. Pak lze určit prostorovou frekvenci:

$$\mu_i = arg(\phi_i) \tag{104}$$

a následně: [12]

$$\theta_i = arcsin\left(-\frac{\lambda}{2\pi\Delta}\mu_i\right) \tag{105}$$

5.2.4 Předzpracování signálu, odhad řádu modelu

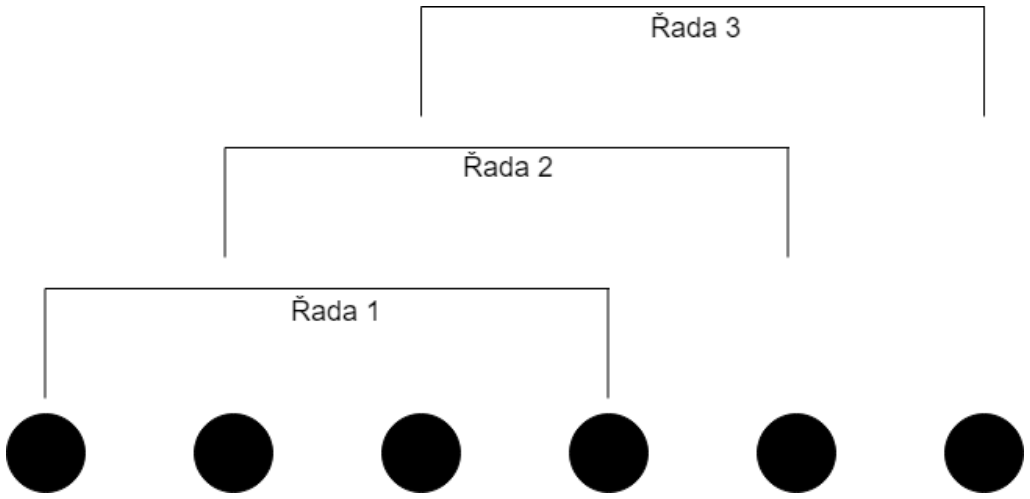
Dopředné a zpětné průměrování

Dopředné a zpětné průměrování je oblíbená metoda, která spoléhá na to, že řídící vektor ULA zůstává stejný, i když se prvky řady zamění a komplexně sdruží. Kovarianční matice, na kterou bylo aplikováno dopředné a zpětné průměrování má hodnost d, i když jsou dva signály koherentní nebo vysoce korelované, to umožňuje rozlišení koherentních nebo vysoce korelovaných signálů. V praxi lze zpětně a dopředně průměrovanou kovarianční matici spočítat jako: [12]

$$\mathbf{R}_{xx}^{fb} = \frac{1}{2N}(\mathbf{R}_{xx} + \mathbf{\Pi}_M(\mathbf{R}_{xx}^*)^H\mathbf{\Pi}_M) \tag{106}$$

Prostorové vyhlazení

Uvažujme ULA anténní řadu o M prvcích, tu rozdělíme na L menších řad obsahujících $M_L = M - L + 1$ prvků, například jako na obrázku 5-2.



Obrázek 5-5.2 Příklad rozdělení anténní řady na L řad pro prostorové vyhlazení

Prostorové vyhlazení se provede tak, že se určí L kovariančních matic a ty se následně zprůměrují:

$$\mathbf{R}_{xx}^{ss} = \frac{1}{L}\sum_{l=1}^{L}\mathbf{R}_l \tag{107}$$

Cenou za prostorové vyhlazení je zmenšení počtu prvků z M na M_L při podmínce $M_L \geq d + 1$ pro správné určení AoA. [12]

Odhad řádu modelu

Pro odhadnutí počtu signálů dopadajících na anténní řadu si představíme dvě techniky odhadu řádu modelu, MDL (Minimum Descriptive length Criterion) a AIC (Akaike Information Theoretic Criterion). Počet dopadajících signálu pomocí MDL najdeme tak, že hledáme takové $d \in \{0, 1, \dots, M-1\}$, které minimalizuje kritérium: [14]

$$MDL(d) = -Nln\left\{\frac{\prod_{i=d+1}^{M}\lambda_i}{\left(\frac{1}{M-d}\sum_{i=d+1}^{M}\lambda_i\right)^{M-d}}\right\} + \frac{1}{2}d(2M-d)ln\,N \tag{108}$$

kde M je počet prvků v anténní řadě, N je počet vzorků a λ_i jsou vlastní čísla kovarianční matice.
Při použití AIC minimalizujeme kritérium: [14]

$$AIC(d) = -2Nln\left\{\frac{\prod_{i=d+1}^{M}\lambda_i}{\left(\frac{1}{M-d}\sum_{i=d+1}^{M}\lambda_i\right)^{M-d}}\right\} + 2d(2M-d) \tag{109}$$

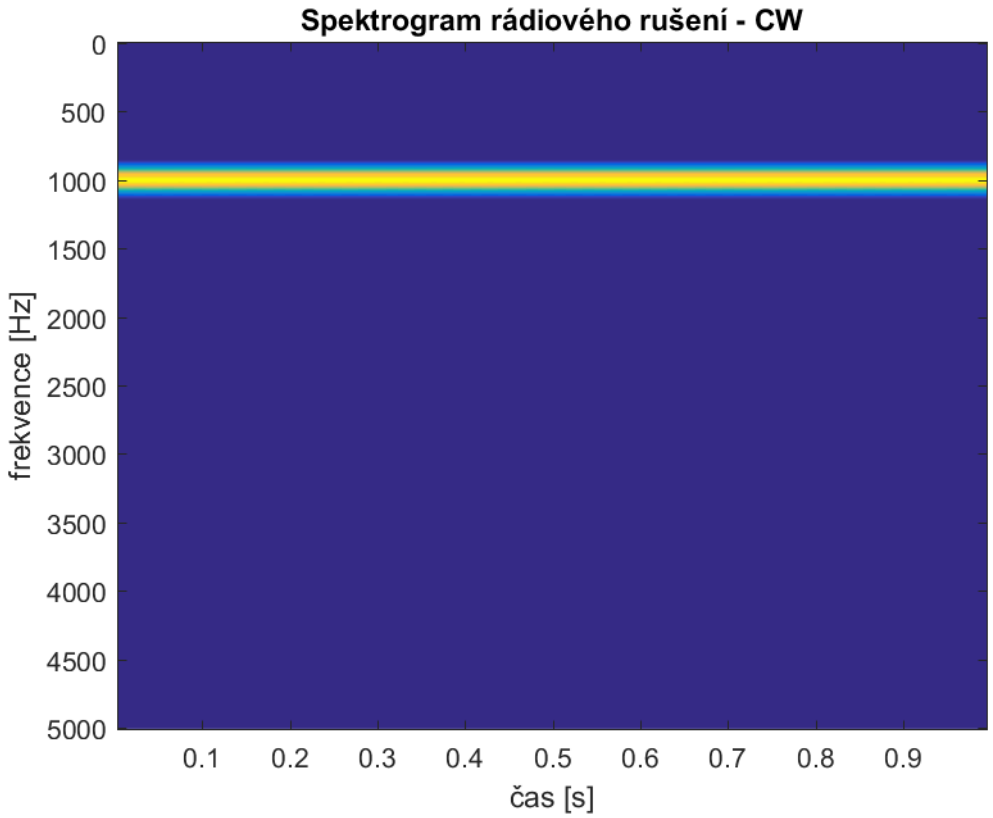
6. Simulace a výsledky

V této kapitole si představíme výsledky simulací, kterým byly podrobeny metody vybrané pro implementaci. V první části si ukážeme výsledky simulací metod pro detekci rušení, v části druhé výsledky simulací pro lokalizaci rušení. Všechny metody byly implementovány a simulovány v prostředí MATLAB.

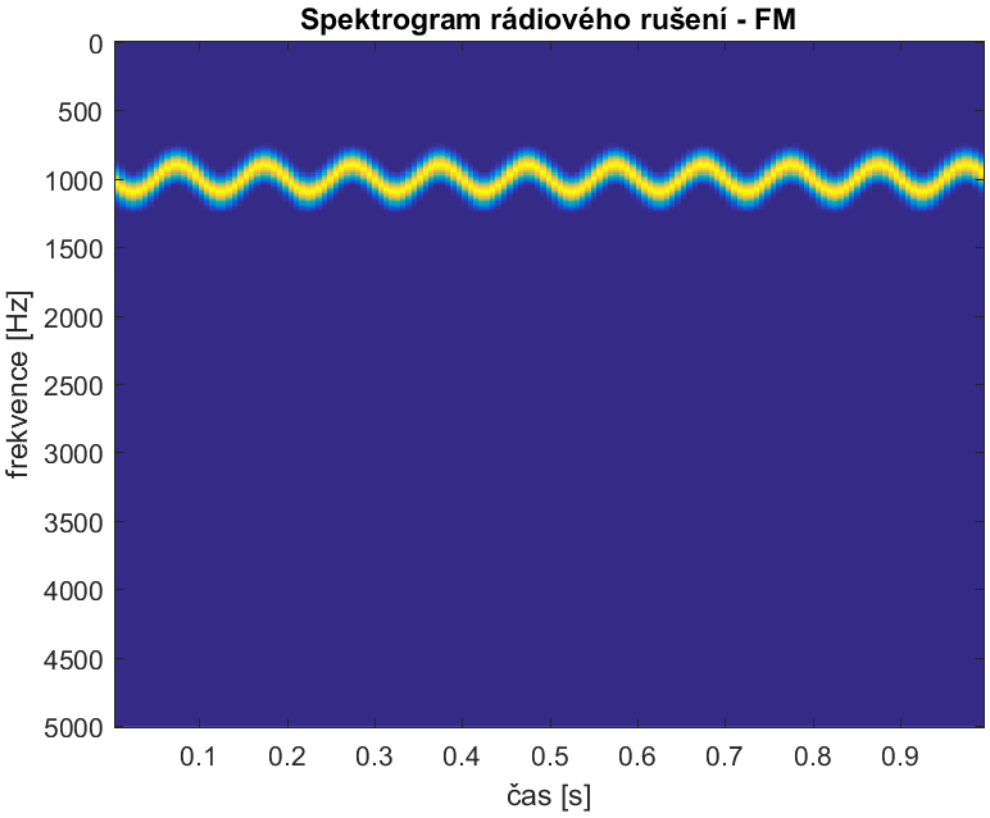
6.1 Simulace vybraných metod pro detekci rušení

Pro detekci rušení byly vybrány tři metody, a to: Metoda využívající sledování spektrální výkonové hustoty, metoda využívající sledování poměru C/N_0 a metoda detekce rušení v časově-frekvenční oblasti.

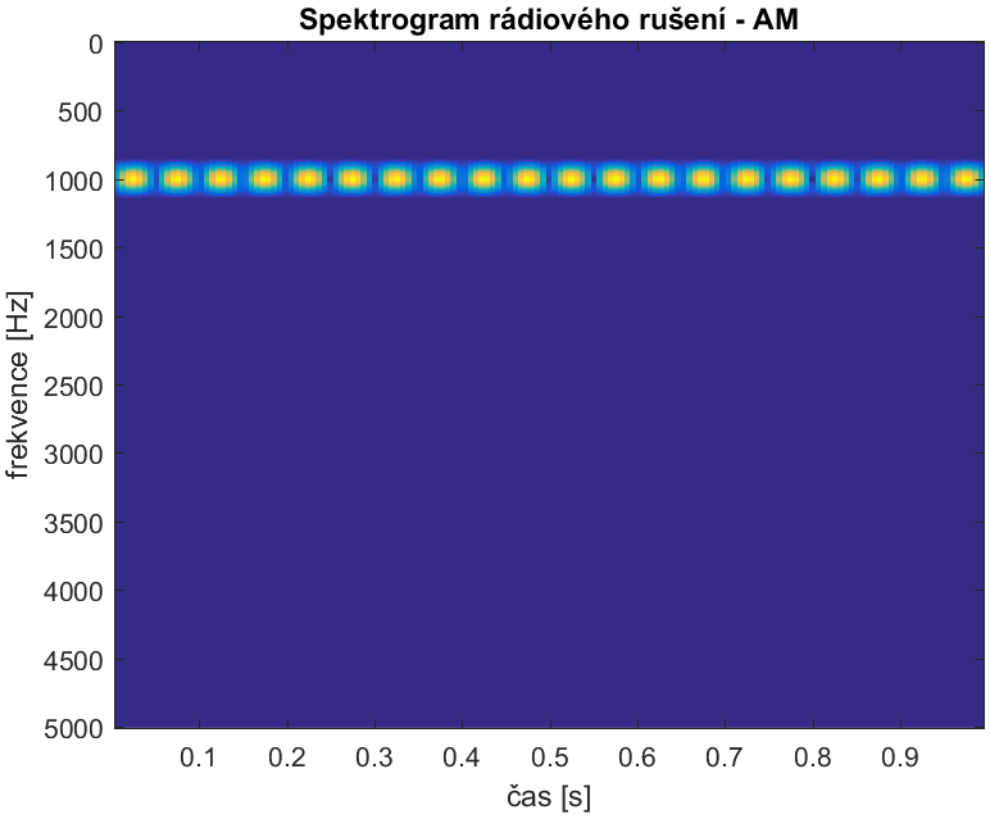
Všechny metody byly v simulacích otestovány stejnými druhy rušivých signálů – kontinuální sinusovou vlnou - CW, amplitudově modulovaným sinusovým signálem - AM, frekvenčně modulovaným sinusovým signálem - FM a čtyřmi druhy chirp signálu (lineární monotónní chirp, dva lineární nemonotónní chirp signály a logaritmický chirp) – chirp 1 – chirp 4. Spektrogramy jednotlivých signálů jsou zobrazeny na obrázcích 6-1 – 6-7.



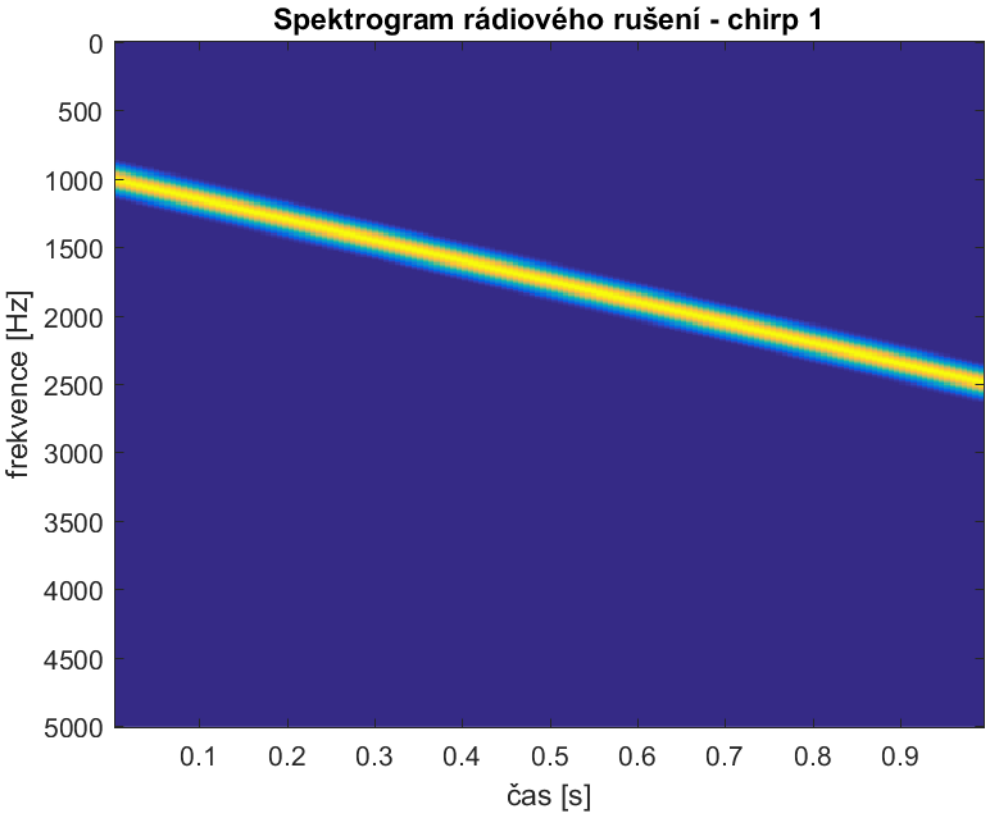
Obrázek 6.1 Spektrogram rádiového rušení - kontinuální sinusová vlna



Obrázek 6.2 Spektrogram rádiového rušení - frekvenčně modulovaný sinusový signál

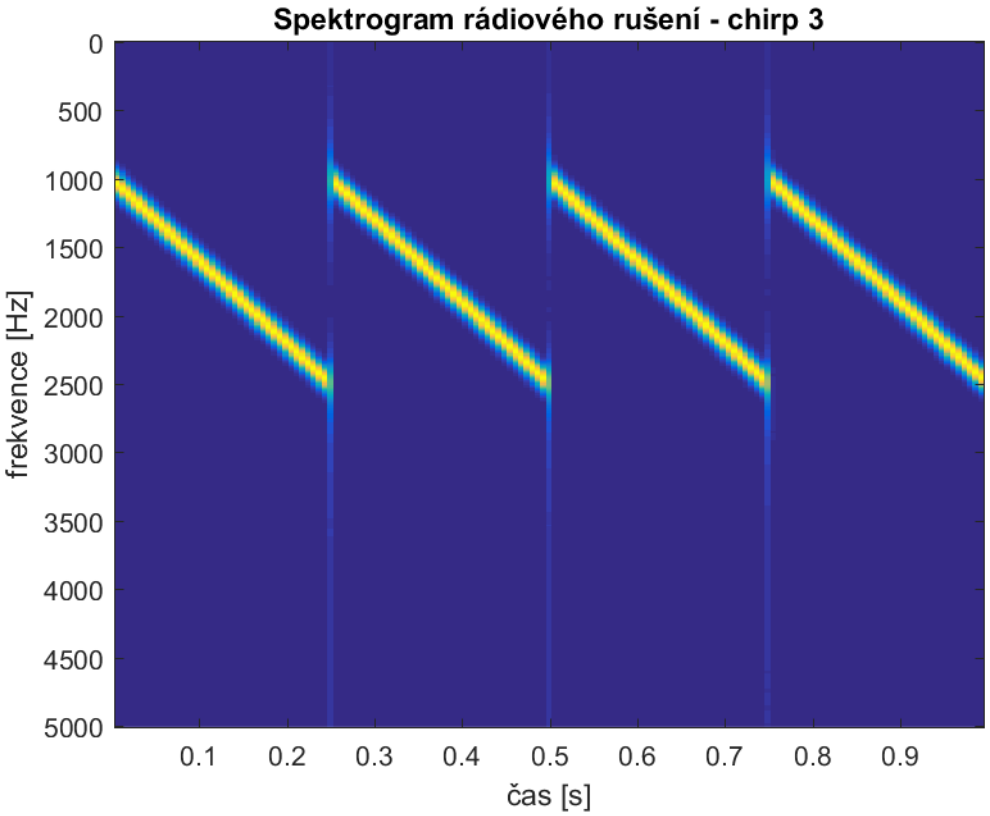


Obrázek 6.3 Spektrogram rádiového rušení - amplitudově modulovaný sinusový signál

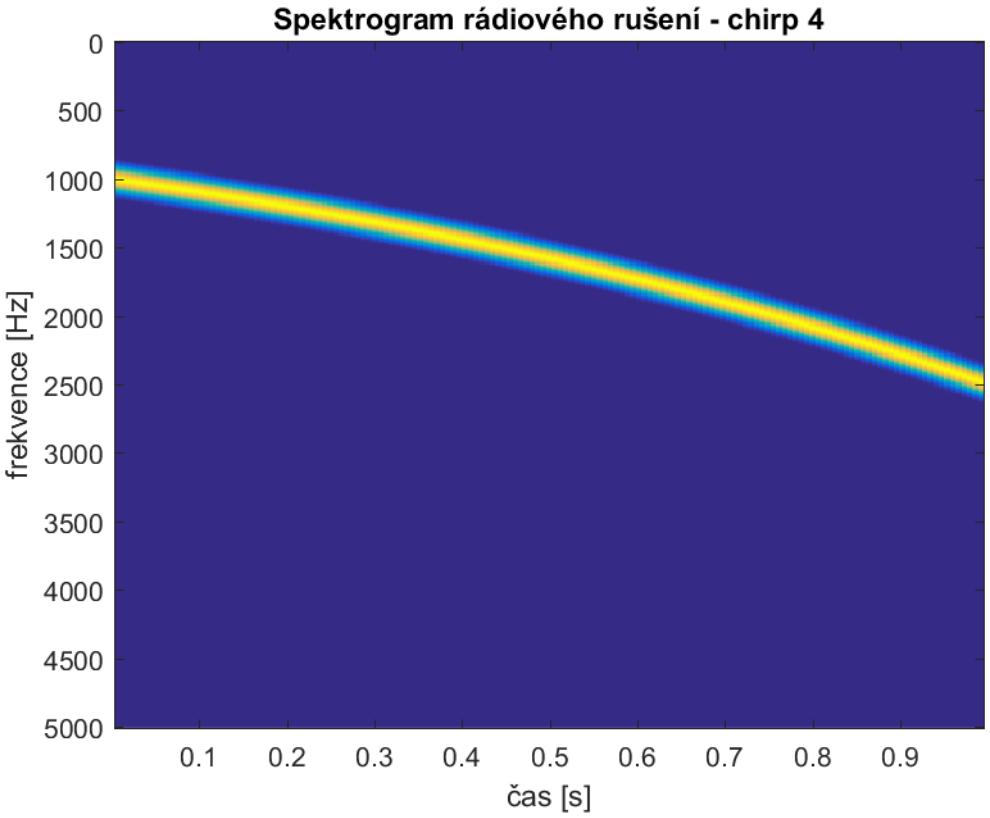


Obrázek 6.4 Spektrogram rádiového rušení - chirp 1

Obrázek 6.5 Spektrogram rádiového rušení - chirp 2



Obrázek 6.6 Spektrogram rádiového rušení - chirp 3



Obrázek 6.7 Spektrogram rádiového rušení - chirp 4

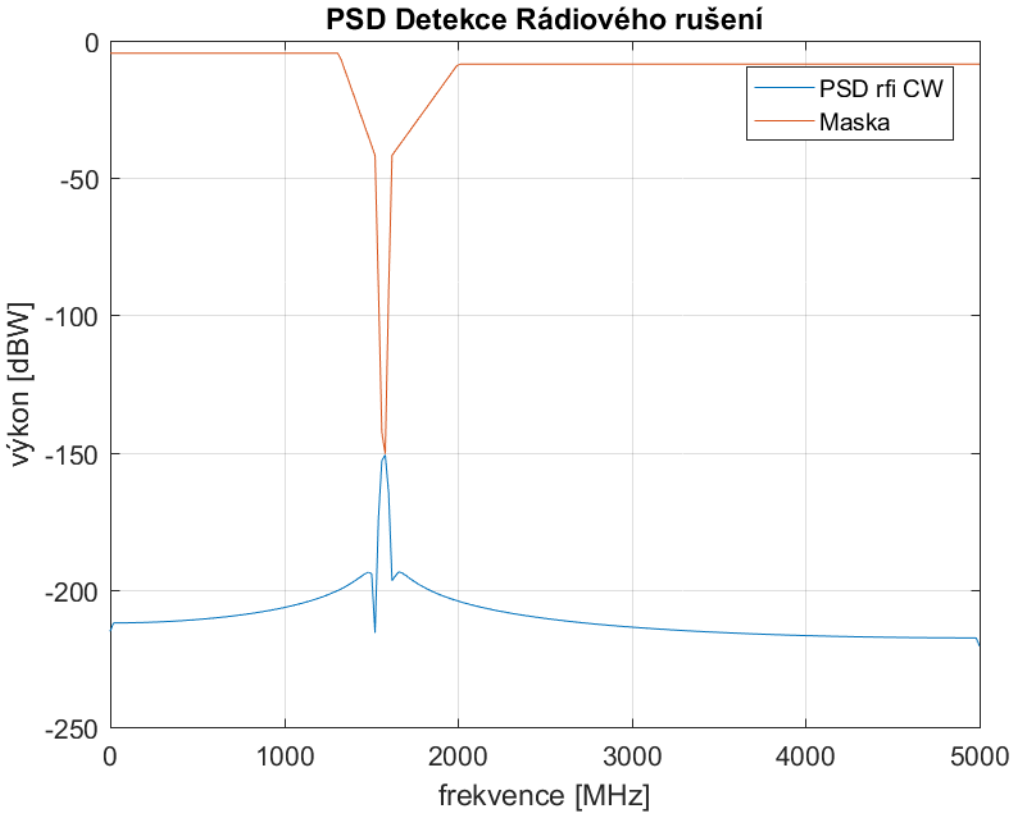
6.1.1 Simulace metody využívající sledování spektrální výkonové hustoty

Pro simulaci byly signály generovány vždy dvakrát, o dvou různých výkonech. Jednou s výkonem, který by měl být pod úrovní spektrální masky a následovně s výkonem, který by měl masku přesahovat. Vzorkovací frekvence byla u všech signálů 10 MHz, ostatní parametry jsou uvedeny zde:

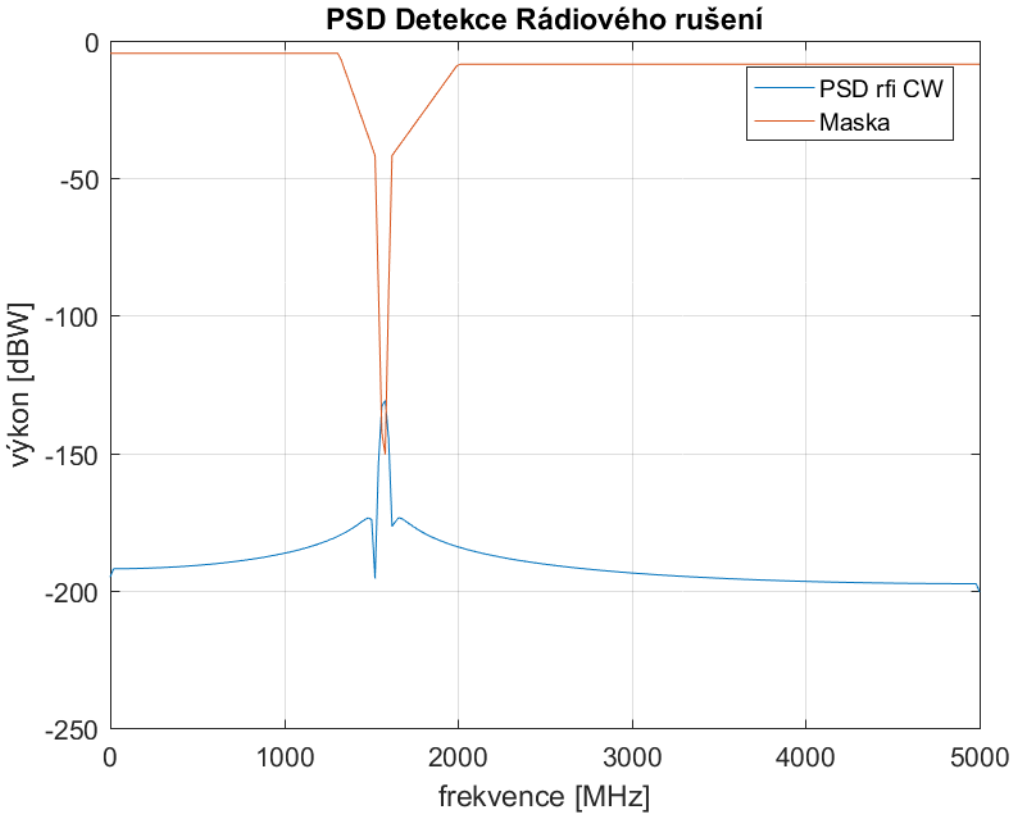
- Sinusový signál – výkon: -150 dBW a -130 dBW, frekvence: 1575 MHz.
- Frekvenčně modulovaný sinusový signál: výkon: -150 dBW a -130 dBW, frekvence nosné vlny: 1575 MHz, frekvenční zdvih: 5 MHz.
- Amplitudově modulovaný sinusový signál: výkon: -150 dBW a -130 dBW, frekvence nosné vlny: 1575 MHz.
- Chirp 1-4: výkon: -150 dBW a -130 dBW, počáteční frekvence: 1570 MHz, konečná frekvence 1580 MHz.

Pro výpočet spektrální výkonové hustoty signálu byla použita Welchova metoda s Hammingovým oknem o délce 512 vzorků.

Na obrázku 6-8 je zobrazen průběh spektrální výkonové hustoty sinusového signálu pod úrovní spektrální masky, na obrázku 6-9 je případ, kdy je signál naopak nad úrovní této masky a je tedy detekován jako rádiové rušení. Ostatní průběhy jsou v příloze A.



Obrázek 6.8 PSD sinusového signálu pod úrovní spektrální masky



Obrázek 6.9 PSD sinusového signálu nad úrovní spektrální masky

6.1.2 Simulace metody sledování poměru C/N_0

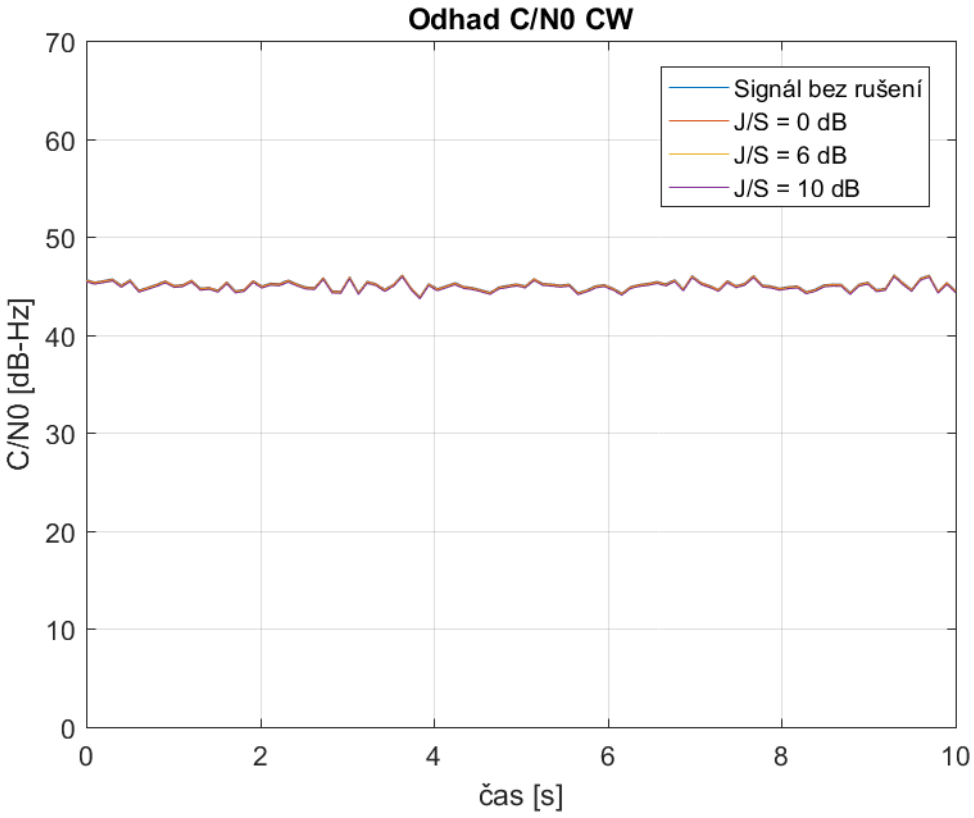
Detekce rušení založená na sledování poměru C/N0 nemohla být testována stejným způsobem jako ostatní metody, jelikož využívá post-korelační přístup. Nejdříve tedy musel být vygenerován C/A kód, který byl následně modulován modulací BPSK, generováno bylo deset period kódu, při vzorkovacím kmitočtu 20 MHz. K tomuto signálu byl následně přidán rušivý signál. Parametry testovaných signálů byly následující:

- Vzorkovací frekvence 20 MHz, výkon v závislosti na požadovaném odstupu rušivého signálu od signálu užitečného - J/S pro všechny signály
- Sinusový signál – frekvence: 4 MHz.
- Frekvenčně modulovaný sinusový signál: frekvence nosné vlny: 4 MHz, frekvenční zdvih: 1 MHz.
- Amplitudově modulovaný sinusový signál: frekvence nosné vlny: 4 MHz.
- Chirp 1-4: počáteční frekvence: 0,5 MHz, konečná frekvence 6 MHz.

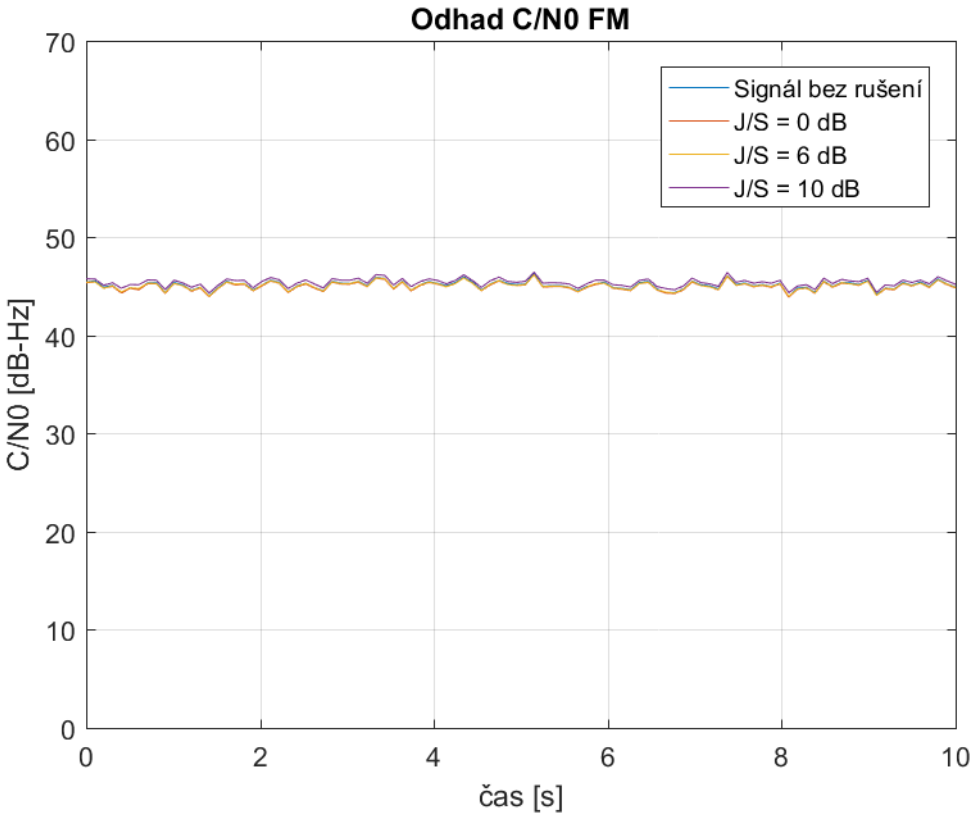
Na obrázcích 6-10 – 6-13 jsou průběhy odhadů poměru C/N_0 pro sinusový signál, frekvenčně modulovaný sinusový signál, amplitudově modulovaný sinusový signál a pro signál typu chirp1, při různých hodnotách *J/S*. Zbylé průběhy odhadu poměru C/N_0 jsou v příloze B.

Z obrázků je patrné, že tato metoda není vhodná pro detekci rušení sinusovým signálem, frekvenčně modulovaným sinusovým signálem a amplitudově modulovaným sinusovým signálem, jelikož se průběhy odhadu C/N_0 téměř překrývají pro všechny hodnoty odstupu *J/S*. Pro signály typu chirp je zřetelně vidět znatelný pokles C/N_0 pro všechny hodnoty odstupu *J/S*.

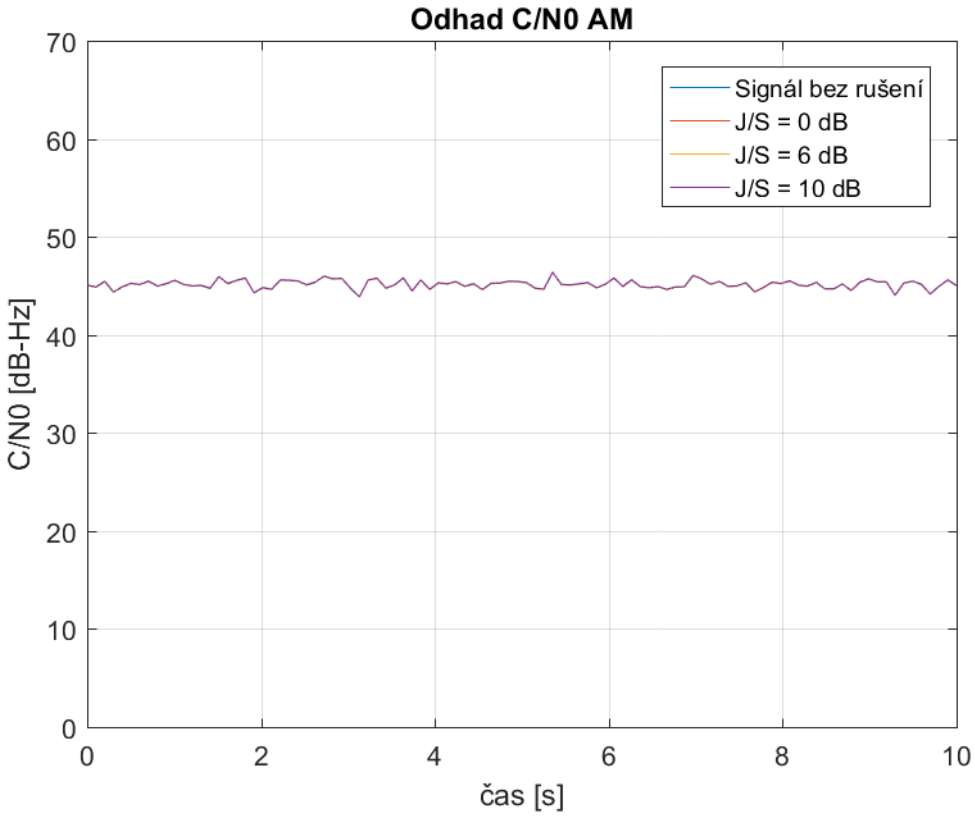
Jak již bylo zmíněno v kapitole 4.1.2, poměr C/N_0 je ovlivněn mnoha faktory a nelze jej považovat za konstantní, aby tedy bylo možné rozhodnout, zda je případný pokles úrovně C/N_0 skutečně způsobený rádiovým rušením, bylo by nutné dlouhodobě sledovat průběhy C/N_0 a s nimi následovně porovnávat současný, vypočtený odhad.



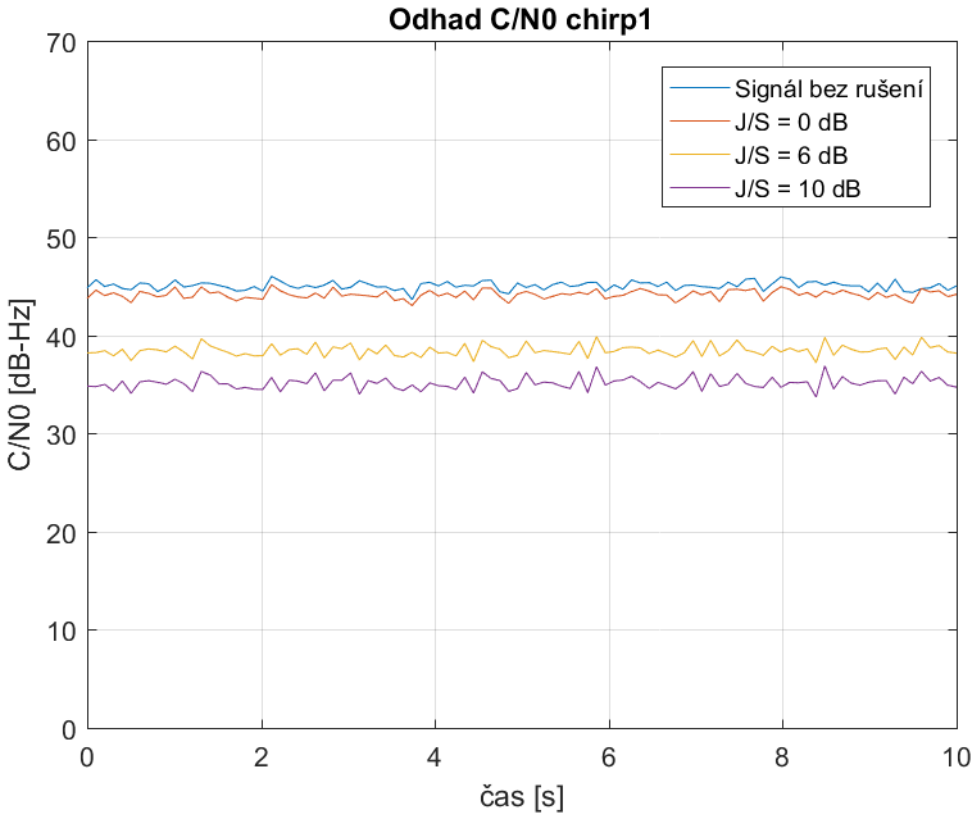
Obrázek 6.10 Odhad poměru C/N0 pro sinusový signál při různých hodnotách J/S



Obrázek 6.11 Odhad poměru C/N0 pro frekvenčně modulovaný sinusový signál při různých hodnotách J/S



Obrázek 6.12 Odhad poměru C/N0 pro amplitudově modulovaný sinusový signál při různých hodnotách J/S



Obrázek 6.13 Odhad poměru C/N0 pro signál typu chirp 1 při různých hodnotách J/S

6.1.3 Simulace metody detekce rušení v časově-frekvenční a statistické doméně

Metoda detekce rušení v časově-frekvenční a statistické doméně byla testována signály, které byly generovány jako signály konvertované do nižšího pásma s následujícími parametry:

- Vzorkovací frekvence 16 MHz, výkon v závislosti na požadovaném *jnr* pro všechny signály
- Sinusový signál – frekvence: 4 MHz.
- Frekvenčně modulovaný sinusový signál: frekvence nosné vlny: 4 MHz, frekvenční zdvih: 1 MHz.
- Amplitudově modulovaný sinusový signál: frekvence nosné vlny: 4 MHz.
- Chirp 1-4: počáteční frekvence: 0,5 MHz, konečná frekvence 6 MHz.

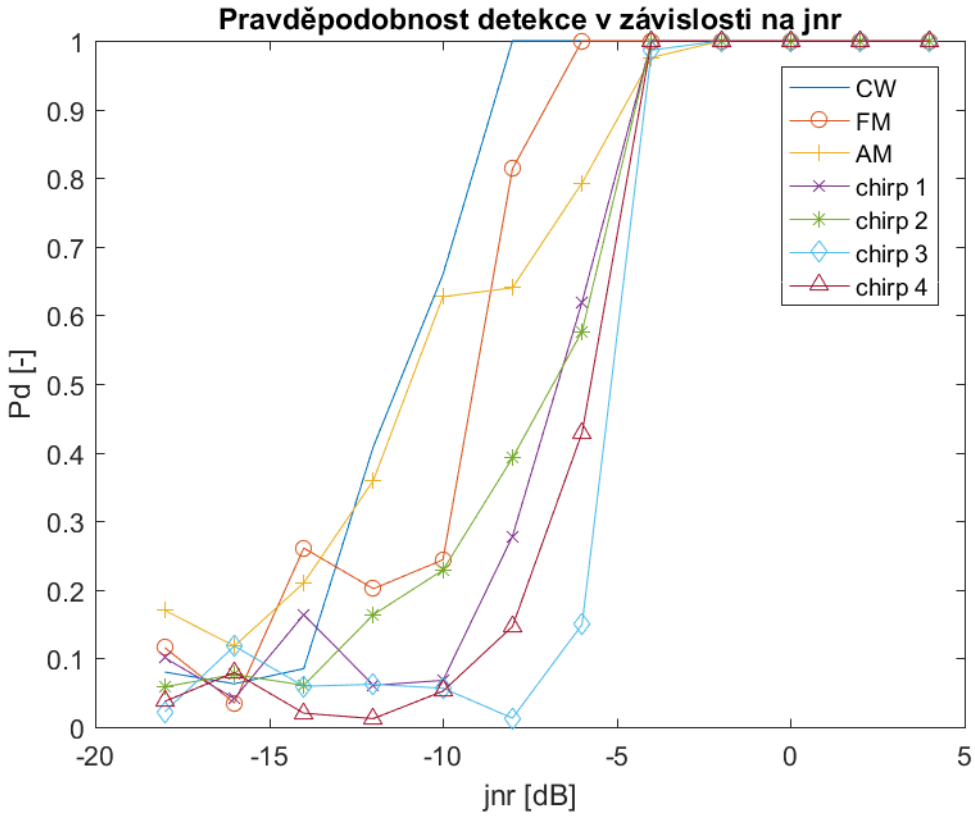
Sledované metriky byly následující:

- Závislost pravděpodobnosti detekce různých druhů rušení na *jnr*, při fixní úrovni signifikance a velikosti rozhodovacího a vyhodnocovacího okna. $jnr \in \{-18, -16, \dots, 4\}\ dB$, α = 0,0001, N = 2048 vzorků.
- Závislost pravděpodobnosti detekce na velikosti rozhodovacího a vyhodnocovacího okna, při fixní úrovni signifikance a různých úrovních *jnr* pro sinusový signál a chirp 1. $N = \{128, 256, 512, 1024, 2048, 4096\}$ vzorků, α = 0,0001, $jnr \in \{-6, -2\}\ dB$.
- Závislost pravděpodobnosti falešného alarmu na velikosti rozhodovacího a vyhodnocovacího okna. $N = \{128, 256, 512, 1024, 2048, 4096\}$.

Proběhlo vždy 200 realizací pro každý parametr metriky. Například 200 realizací detekce pro sinusový signál, při *jnr* = -18 dB, α = 0,0001 a N = 2048 vzorků.

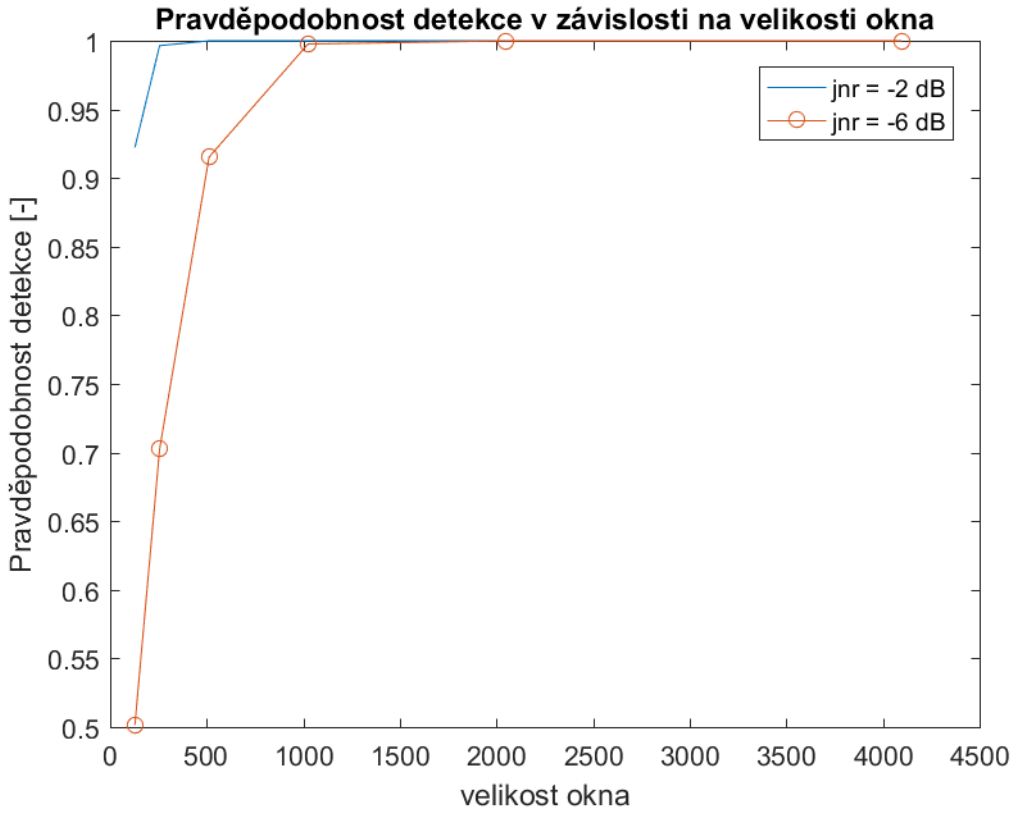
Pro výpočet Pseudo Wigner Villeho distribuce byl použit volně šiřitelný toolbox: *Time Frequency Toolbox*, dostupný na webové adrese http://tftb.nongnu.org/.

Na obrázku 6-10 můžeme vidět průběhy pravděpodobnosti detekce na různých hodnotách *jnr*. V grafu je vidět, že navrhovanou metodou lze nejlépe detekovat sinusový signál (CW) a naopak nejhůře signál typu chirp 3. Od úrovně odstupu výkonu rušení od šumu -2 dB byly všechny druhy rušení detekovány s pravděpodobností blízkou jedné.

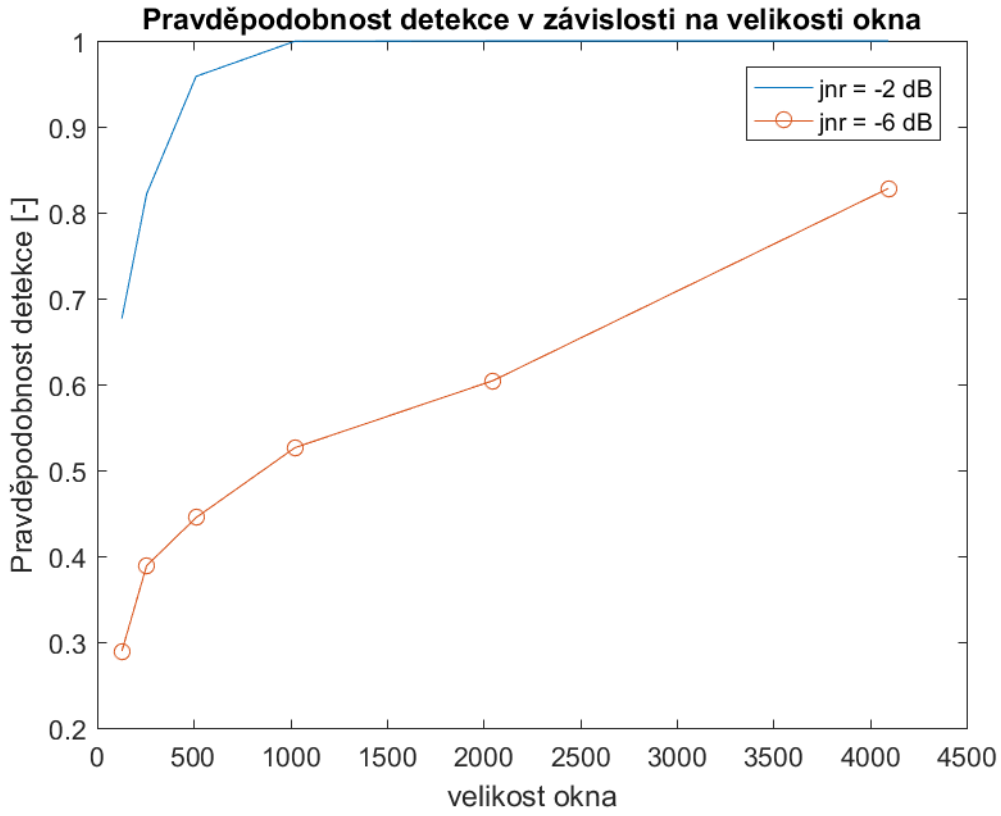


Obrázek 6.14 Závislost pravděpodobnosti detekce v závislosti na různých hodnotách jnr pro různé druhy rušení

Na obrázcích 6-15 a 6-16 jsou zobrazeny průběhy závislosti pravděpodobnosti detekce na velikosti rozhodovacího a posuzovacího okna, pro různé hodny *jnr*, pro sinusový signál a pro signál typu chirp 1. Je patrné, že s rostoucí velikostí okna roste i pravděpodobnost detekce i pro různé hodnoty *jnr*. Pro sinusový signál bylo dosaženo jednotkové pravděpodobnost pro obě úrovně *jnr* při velikosti oken N = 1024 vzorků. Pro signál typu chirp 1, bylo jednotkové pravděpodobnosti dosaženo pouze pro úroveň *jnr* = -2 dB, rovněž při velikosti oken N = 1024 vzorků.

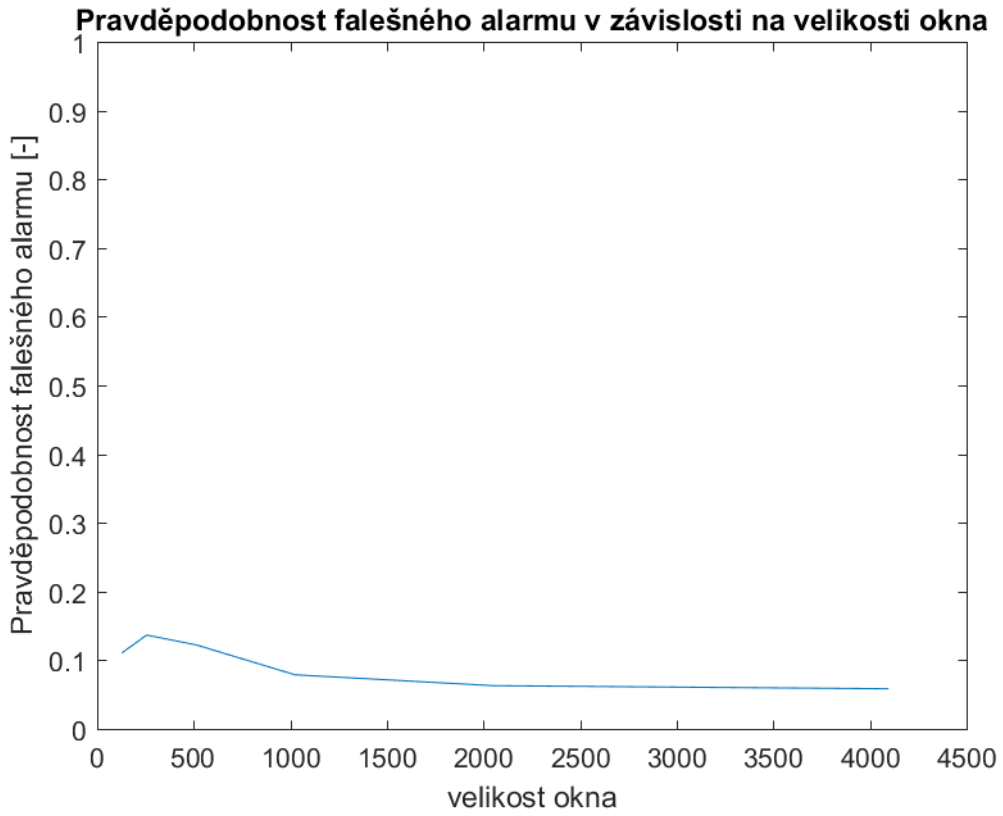


Obrázek 6.15 Pravděpodobnost detekce v závislosti na velikosti rozhodovacího a posuzovacího okna pro sinusový signál



Obrázek 6.16 Pravděpodobnost detekce v závislosti na velikosti rozhodovacího a posuzovacího okna pro signál chirp 1

Dalším předmětem zkoumání byla závislost pravděpodobnosti falešného alarmu na velikosti rozhodovacího a posuzovacího okna. Ta je znázorněna na obrázku 6-17.



Obrázek 6.17 Pravděpodobnost falešného alarmu v závislosti na velikosti rozhodovacího a posuzovacího okna

Lze vypozorovat, že s rostoucí velikostí okna pravděpodobnost falešného alarmu klesá. Nejvyšší hodnoty nabyla pravděpodobnost falešného alarmu při velikosti oken $N = 256$ vzorků a to přibližně $P_f = 0{,}14$. Naopak nejnižší hodnotu jsme zaznamenali při velikosti oken $N = 4096$, $P_f = 0{,}06$.

6.2 Simulace vybraných metod pro lokalizaci rušení

Pro lokalizaci rušení byly k implementaci vybrány algoritmy MUSIC a ESPRIT. Obě metody byly testovány sinusovým signálem a chirp signálem. Výsledky simulací jsou shrnuty v následujících podkapitolách.

6.2.1 Simulace algoritmu MUSIC

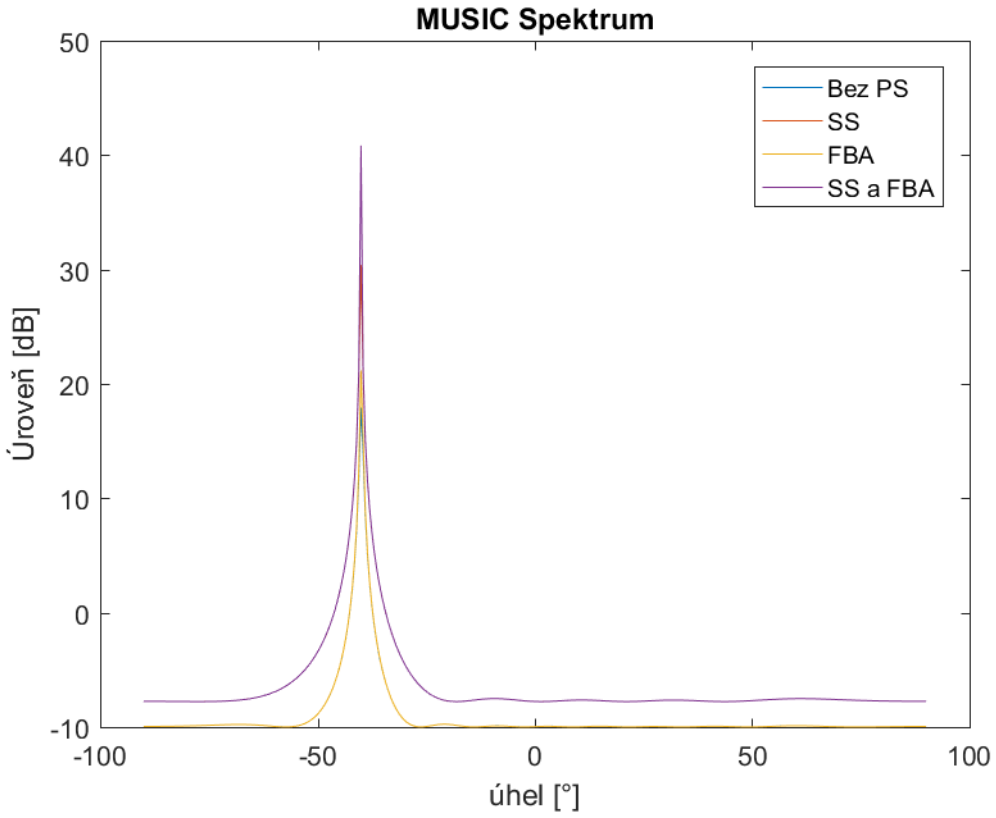
Algoritmus MUSIC byl při simulaci testován sinusovým a chirp signálem o různém AoA. Simulace proběhla pro jeden a pro tři rušivé signály dopadající na anténní řadu bez použití technik pro předzpracování signálu (PS), za použití prostorového vyhlazení (SS), dopředného a zpětného průměrování (FBA) a obou technik najednou, pro tento případ proběhla navíc simulace pro různé hodnoty odstupu výkonu rušivého signálu od výkonu šumu. Střední frekvence pásmového signálu byla určena jako f_c = 1575 MHz, tomu odpovídá vlnová délka λ = 0,1905 m. Anténní řada měla počet prvků M = 10 a vzdálenost mezi jednotlivými prvky byla stanovena na polovinu vlnové délky $\lambda/2$.
Rušivé signály měly následující parametry

- počet snapshotů (úseků): N = 500
- frekvence sinusového signálu pro jeden signál: f = 1575 MHz
- frekvence sinusového signálu pro tři signály: $f_1 = 1570$ MHz, $f_2 = 1575$ MHz a $f_3 = 1580$ MHz
- počáteční a konečná frekvence chirp signálů: $f_0 = 1570$ MHz, $f_1 = 1580$ MHz

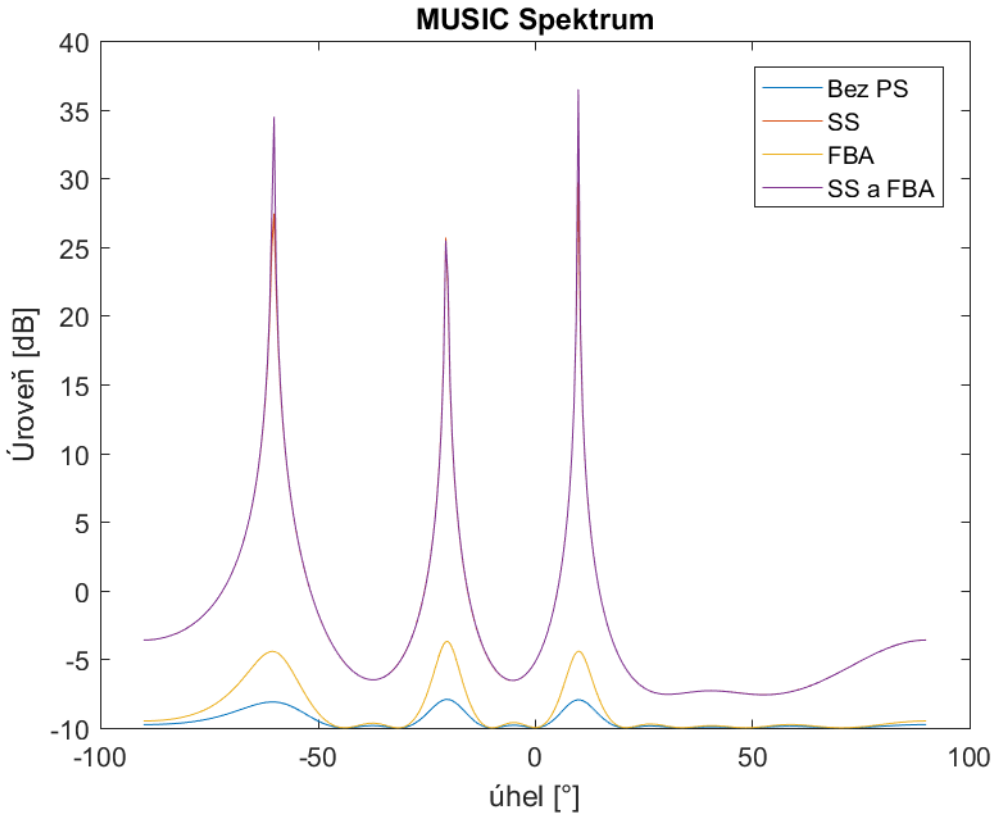
Na obrázku 6-18 vidíme průběhy MUSIC spektra pro úhel dopadu sinusového signálu -40°. Jelikož se jedná o jediný signál, není zde patrný rozdíl mezi výpočtem s použitím technik pro předzpracování signálu a bez nich.

Obrázek 6-19 zobrazuje spektrum pro tři sinusové signály. Zde je již rozdíl patrný, z průběhu spektra bez použití technik pro předzpracování signálu téměř není možné určit úhel příchodu signálu.

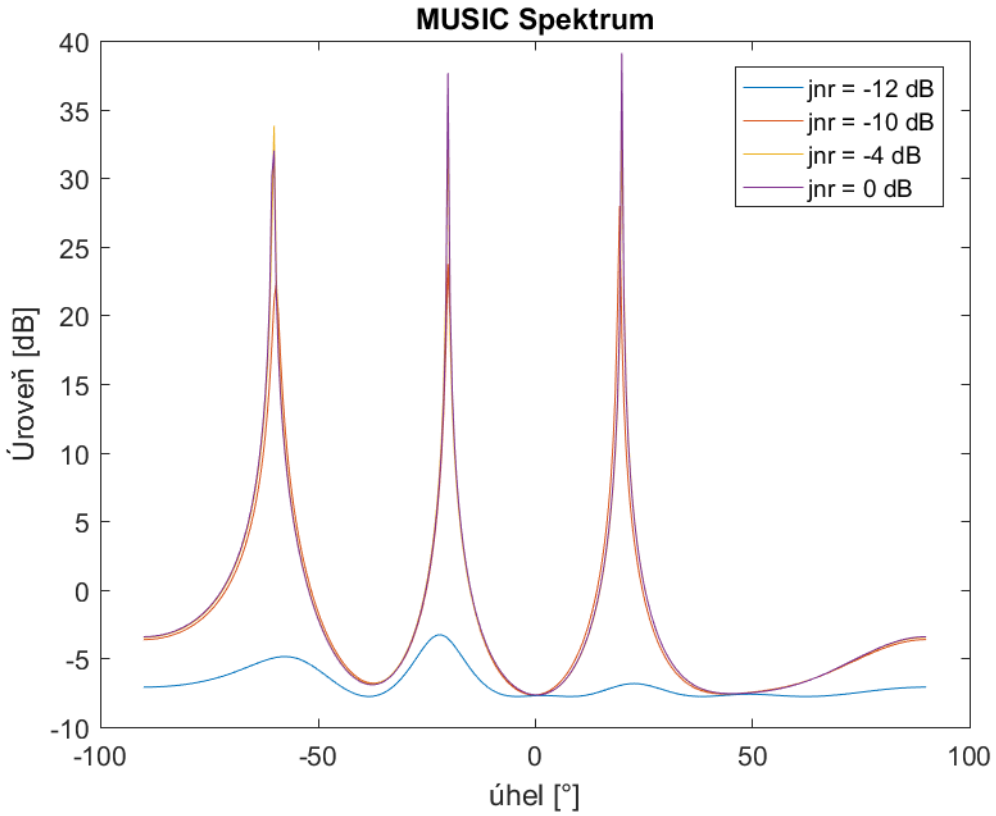
Graf na obrázku 6-20 vykresluje průběhy spektra při použití prostorového vyhlazení i dopředného a zpětného průměrování pro různé hodnoty *jnr*. Z tohoto grafu plyne, že pro hodnoty *jnr* rovny -12 dB a menší algoritmus není schopen určit úhel příchodu signálu. Simulace pro chirp signál dopadly obdobně a jsou k dispozici v příloze C.



Obrázek 6.18 MUSIC spektrum pro jeden sinusový signál, AoA = -40°, jnr = -5 dB



Obrázek 6.19 MUSIC spektrum pro tři sinusové signály, AoA = -60°, -20°, 10°, jnr = -5 dB



Obrázek 6.20 MUSIC spektrum pro tři sinusové signály, AoA = -60°, -20°, 20°, jnr = -12 dB, -10 dB, -4 dB, 0 dB

6.2.2 Simulace algoritmu ESPRIT

Algoritmus ESPRIT byl rovněž testován sinusovým signálem a chirp signálem o stejných parametrech jako algoritmus MUSIC, muselo ovšem dojít k modifikaci, protože pro více než 2 signály dopadající na anténní řadu algoritmus selhal. Konfigurace anténní řady zůstala totožná. Rušivé signály tedy měly následující parametry:

- Počet snapshotů (úseků): $N = 500$
- frekvence sinusového signálu pro jeden signál: $f = 1575$ MHz
- frekvence sinusového signálu pro tři signály: $f_1 = 1570$ MHz a $f_2 = 1580$ MHz
- počáteční a konečná frekvence chirp signálů: $f_0 = 1570$ MHz, $f_1 = 1580$ MHz

V simulaci proběhlo 200 realizací určení odhadu AoA pro oba druhy signálu, při jednom a dvěma dopadajícími signály, bez dopředného a zpětného průměrování i s ním a následně byla zjišťována závislost přesnosti odhadu na různých hodnotách *jnr*. Výsledný odhad AoA byl vždy určen jako aritmetický průměr dílčích odhadů. Výsledky simulací jsou v tabulkách 6-1 a 6-2. x značí selhání algoritmu.

AoA [°]	počet signálů	FBA	typ rušení	odhad AoA [°]
-40,00	1	Ne	sinus	-40,04
-40,00	1	Ano	sinus	-39,98
10,00; 45,00	2	Ne	sinus	x
10,00; 45,00	2	Ano	sinus	9,67; 44,80
-40,00	1	Ne	chirp	x
-40,00	1	Ano	chirp	-40,00
10,00; 45,00	2	Ne	chirp	x
10,00; 45,00	2	Ano	chirp	9,99; 44,99

Tabulka 6.1 Výsledky simulace algoritmu ESPRIT

AoA [°]	typ rušení	odhad AoA [°]	jnr [dB]
-30,00; 50,00	sinus	-30,08; 50,24	-12,00
-30,00; 50,00	sinus	-29,97; 49,97	-10,00
-30,00; 50,00	sinus	-29,99; 49,99	-4,00
-30,00; 50,00	sinus	-30,03; 49,98	0,00
-30,00; 50,00	chirp	-30,19; 49,78	-12,00
-30,00; 50,00	chirp	-30,11; 50,05	-10,00
-30,00; 50,00	chirp	-29,94; 50,06	-4,00
-30,00; 50,00	chirp	-29,98; 49,99	0,00

Tabulka 6.2 Závislost přesnosti odhadu AoA na jnr

V případech, kdy nebylo použito dopředné a zpětné průměrování byl algoritmus schopen určit AoA pouze, pokud na anténní řadu dopadal pouze jeden sinusový signál, v ostatních případech vždy selhal. Dále si můžeme všimnout, že algoritmus téměř není ovlivněn úrovní *jnr*.

7. Závěr

Cílem práce bylo provést rešerši metod pro detekci a lokalizaci záměrného, nezáměrného a inteligentního rádiového rušení globálních družicových navigačních systémů, vybrané metody implementovat v prostředí MATLAB, ověřit simulací a změřenými daty. Změřená data však bohužel nebyla k dispozici, implementované metody tak byly otestovány na simulacích.

Pro detekci záměrného rušení, jammingu a nezáměrného rušení byly zpracovány metody detekce založené na sledování spektrální výkonové hustoty, sledování poměru C/N_0 a využití statistické analýzy časově-frekvenčních charakteristik signálu.

K detekci inteligentního rušení byly vybrány metody detekce založené na monitorování výkonu signálu, metrice podílového kritéria a rozdílu pseudovzdáleností.

Problematika lokalizace rádiových signálů byla nejprve probrána obecněji, byly představeny základní techniky lokalizace a následně byly detailně představeny metody využívající rozklad signálu do signálových podprostorů, MUSIC a ESPRIT.

Implementovány byly všechny metody detekce jammingu a nezáměrného rušení, společně s algoritmy MUSIC a ESPRIT pro lokalizaci rušení.

Simulace metod pro detekci rušení pomocí sledování spektrální výkonové hustoty a statistické analýzy v časově-frekvenční oblasti proběhly úspěšně pro všechny typy simulovaných signálů. Druhá zmiňovaná metoda byla navíc podrobena analýzám pravděpodobnosti detekce v závislosti na úrovni odstupu rušivého signálu od šumu, pravděpodobnosti detekce v závislosti na velikosti posuzovacího a vyhodnocovacího okna a pravděpodobnosti falešného alarmu na velikosti posuzovacího a vyhodnocovacího okna. Detekce signálu proběhla úspěšně i pro signály s úrovní nižší než úroveň šumu. Dále byla zjištěna zvyšující se pravděpodobnost detekce se zvyšující se velikostí posuzovacího a vyhodnocovacího okna. Pravděpodobnost falešného alarmu se s narůstající velikostí okna naopak zmenšovala.

Při simulaci detekce založené na sledování poměru C/N_0 bylo zjištěno, že je tato metoda nevhodná pro rušivé signály typu: sinusový signál, frekvenčně modulovaný sinusový signál a amplitudově modulovaný sinusový signál.

V simulacích metod lokalizace rádiového rušení si vedl lépe algoritmus MUSIC, jelikož algoritmus ESPRIT selhal při pokusu lokalizovat více než dva signály dopadající na anténní řadu. Při analýze vlivu technik pro předzpracování signálu byla demonstrována důležitost těchto technik, které jsou nezbytné pro lokalizaci více signálů. Zajímavé bylo zjištění, že odstup úrovní rušivých signálů a šumu téměř nemá vliv na přesnost určení směru příchodu signálu u algoritmu ESPRIT.

Stanovené cíle byly splněny, pro další zkoumání by bylo zajímavé se zabývat například efektivní implementací pseudo Wigner Villeho distribuce, vzhledem k výpočetní náročnosti tohoto algoritmu.

Pozornost může být věnována také modifikacím algoritmů MUSIC a ESPRIT (Root MUSIC, Unitary ESPRIT a další).

8. Seznam použité literatury

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

[2] Misra, P., Enge, P.: Global Positioning System. Ganga Jamuna Press 2006. ISBN: 0-9709544-7.

[3] "GNSS Signal Authenticity Verification in the Presence of Structural Interference By ALI JAFARNIA JAHROMI A THESIS SUBMITTED TO THE FACULTY OF GRADUATE STUDIES IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY." (2013).

[4] S. Bartl, P. Berglez and B. Hofmann-Wellenhof, "GNSS interference detection, classification and localization using Software-Defined Radio," 2017 European Navigation Conference (ENC), Lausanne, 2017,pp.159-169.doi:10.1109/EURONAV.2017.7954205
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7954205&isnumber=7954157

[5] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," International Journal of Navigation and Observation, vol. 2012, Article ID 127072, 16 pages, 2012. https://doi.org/10.1155/2012/127072.

[6] https://ccrma.stanford.edu/~jos/sasp/Welch_s_Method.html

[7] ICAO Aeronautical Telecomunication, Volume I Radio Navigation Aids, Sixth edition July 2006, Dostupné na: http://cockpitdata.com/Software/ICAO%20Annex%2010%20Volume%201

[8] P. Wang, E. Cetin, A. G. Dempster, Y. Wang and S. Wu, "Time Frequency and Statistical Inference Based Interference Detection Technique for GNSS Receivers," in IEEE Transactions on Aerospace and Electronic Systems, vol. 53, no. 6, pp. 2865-2876, Dec. 2017. doi:10.1109/TAES.2017.2718278
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7954649&isnumber=8167337

[9] Huang, Jie & Lo Presti, Letizia & Motella, Beatrice & Pini, Marco. (2016). GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky. ICT Express. 2. 10.1016/j.icte.2016.02.006.

[10] Zhang, Zhenjun and Xingqun Zhan. "GNSS Spoofing Network Monitoring Based on Differential Pseudorange." Sensors (2016).

[11] A. G. Dempster and E. Cetin, "Interference Localization for Satellite Navigation Systems," in Proceedings of the IEEE, vol. 104, no. 6, pp. 1318-1326, June 2016. doi:10.1109/JPROC.2016.2530814
URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7439734&isnumber=7471392

[12] CHEN, Zhizhang, Gopal GOKEDA a Yiqiang YU. Introduction to direction-of-arrival estimation. Boston: Artech House, c2010. Artech House signal processing library. ISBN 978-1-59693-089-6.

[13] R. Roy and T. Kailath, "ESPRIT-estimation of signal parameters via rotational invariance techniques," in IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 37, no. 7, pp. 984-995,July1989.doi:10.1109/29.32276
URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=32276&isnumber=1399

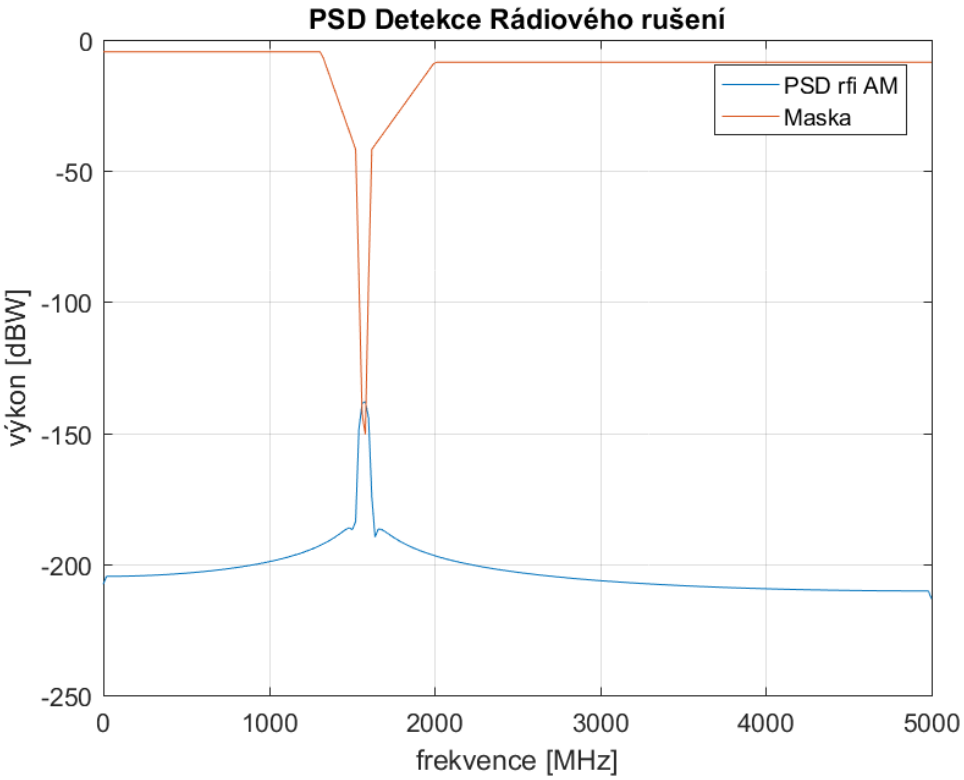
[14] Williams, D.B. “Detection: Determining the Number of Sources” Digital Signal Processing Handbook Ed. Vijay K. Madisetti and Douglas B. Williams Boca Raton: CRC Press LLC, 1999

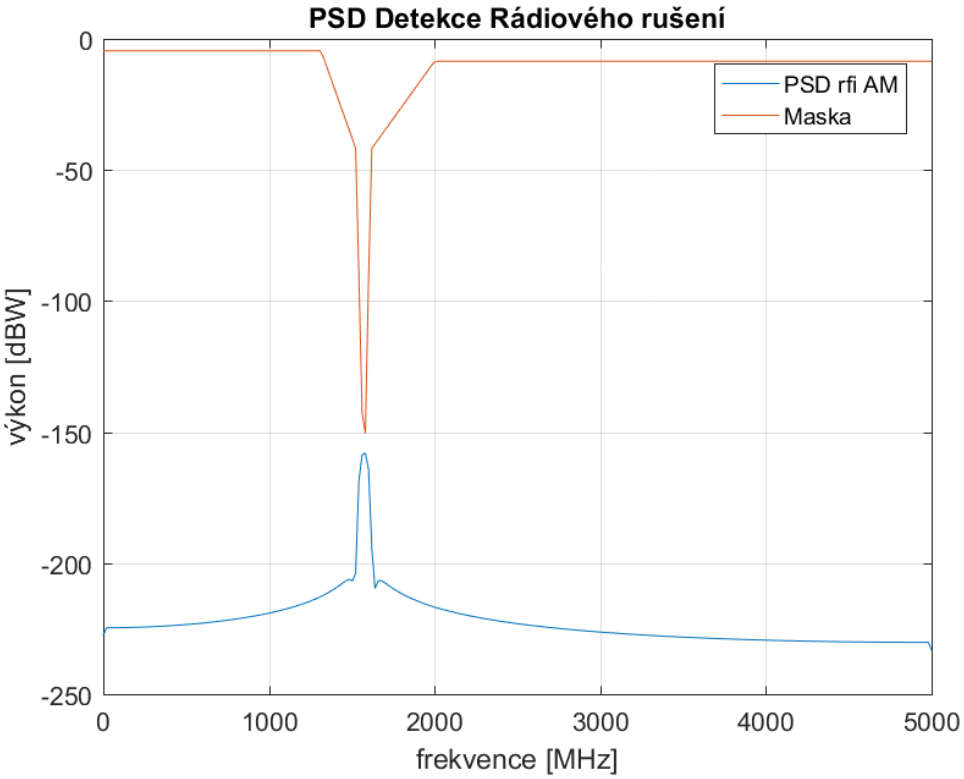
[15] Golub, G. H., and C. F. van Loan, Matrix Computations, 3rd ed., Baltimore, MD: John Hopkins University Press, 1996.

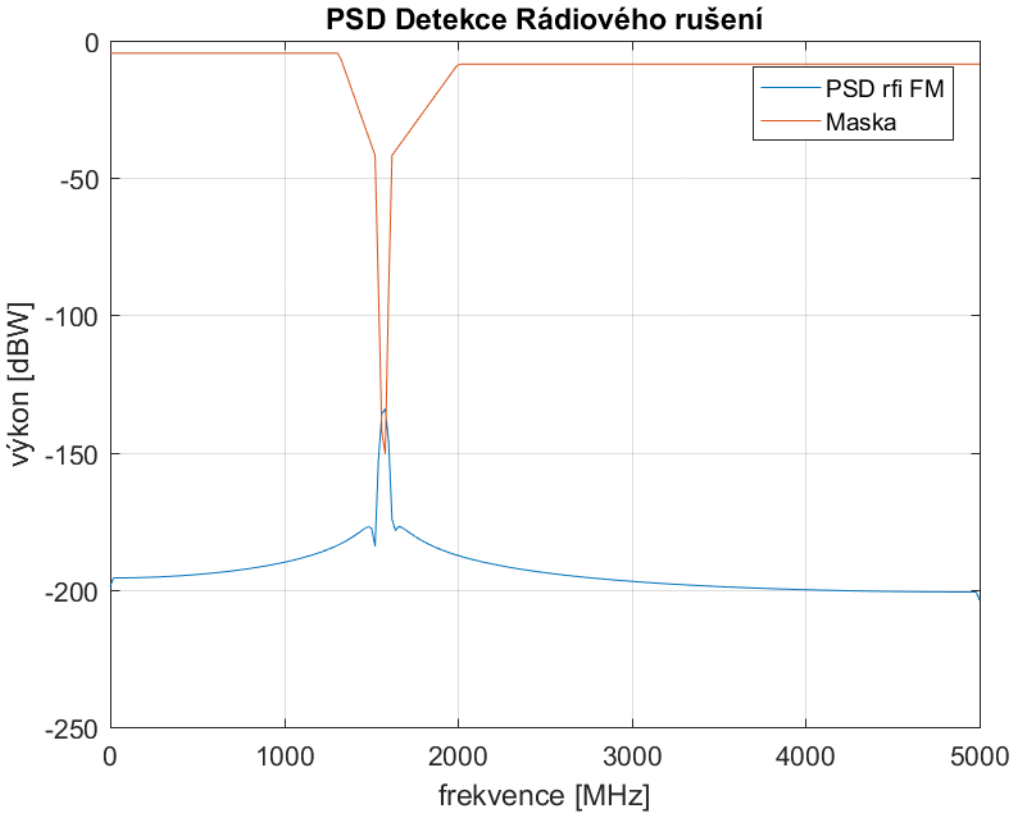
9. Seznam obrázků

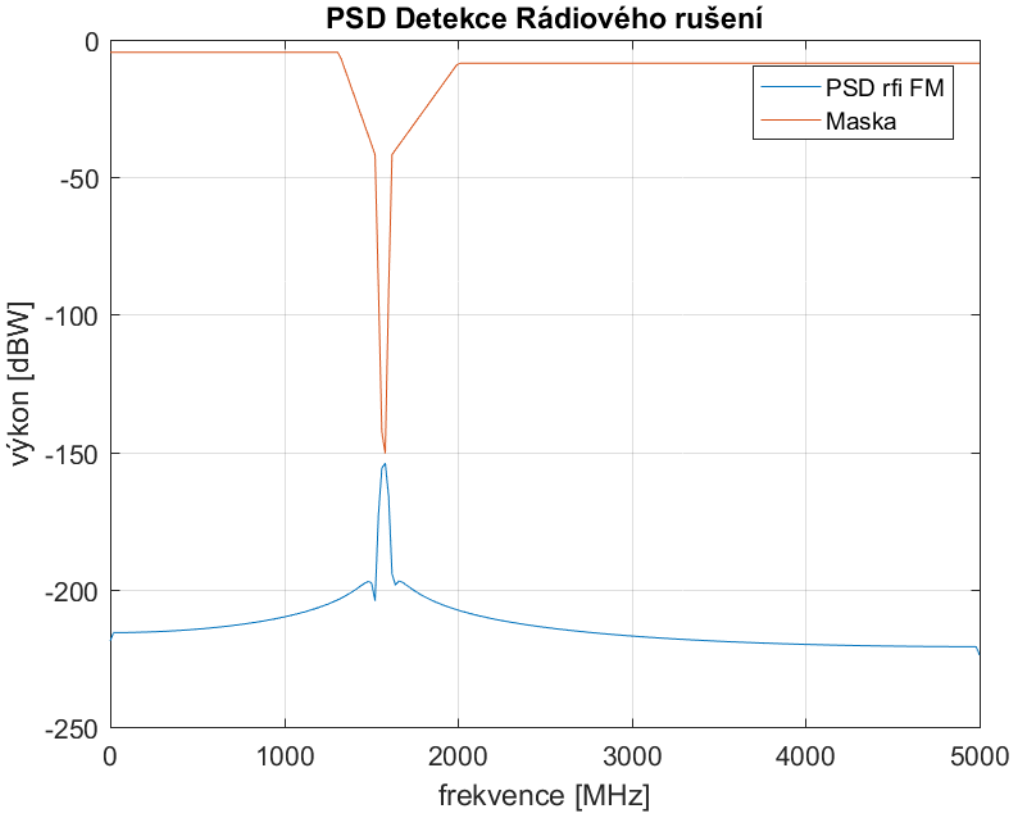
10. Přílohy

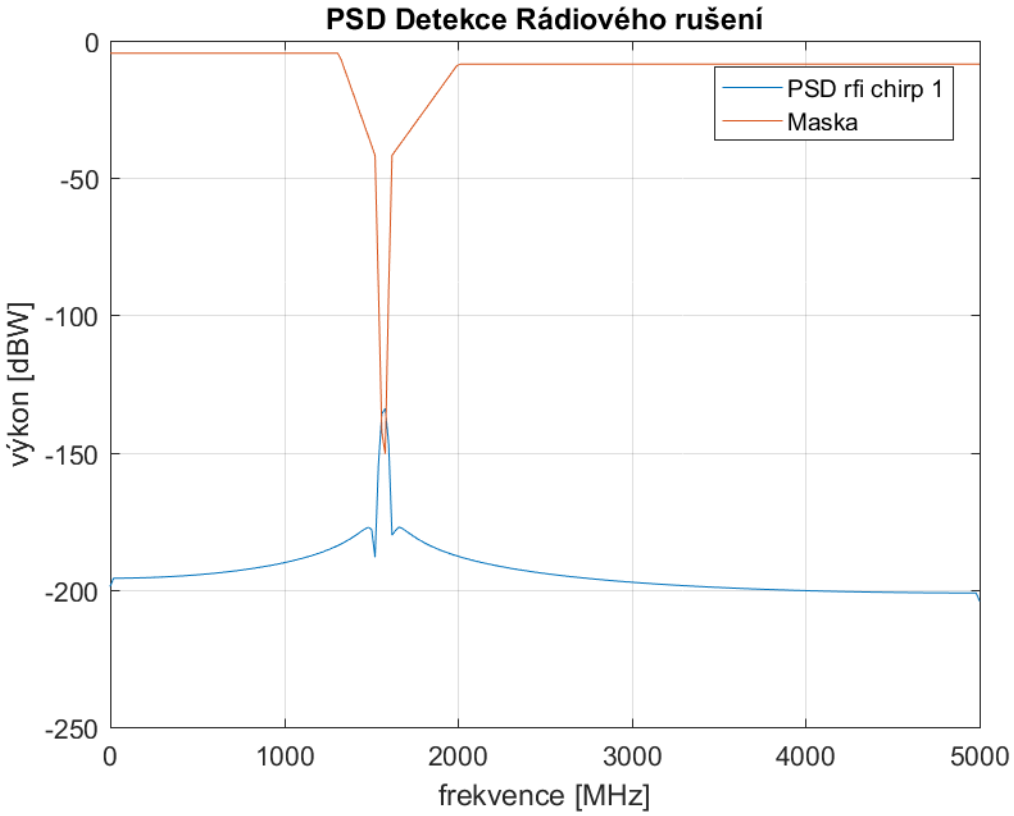
Příloha A

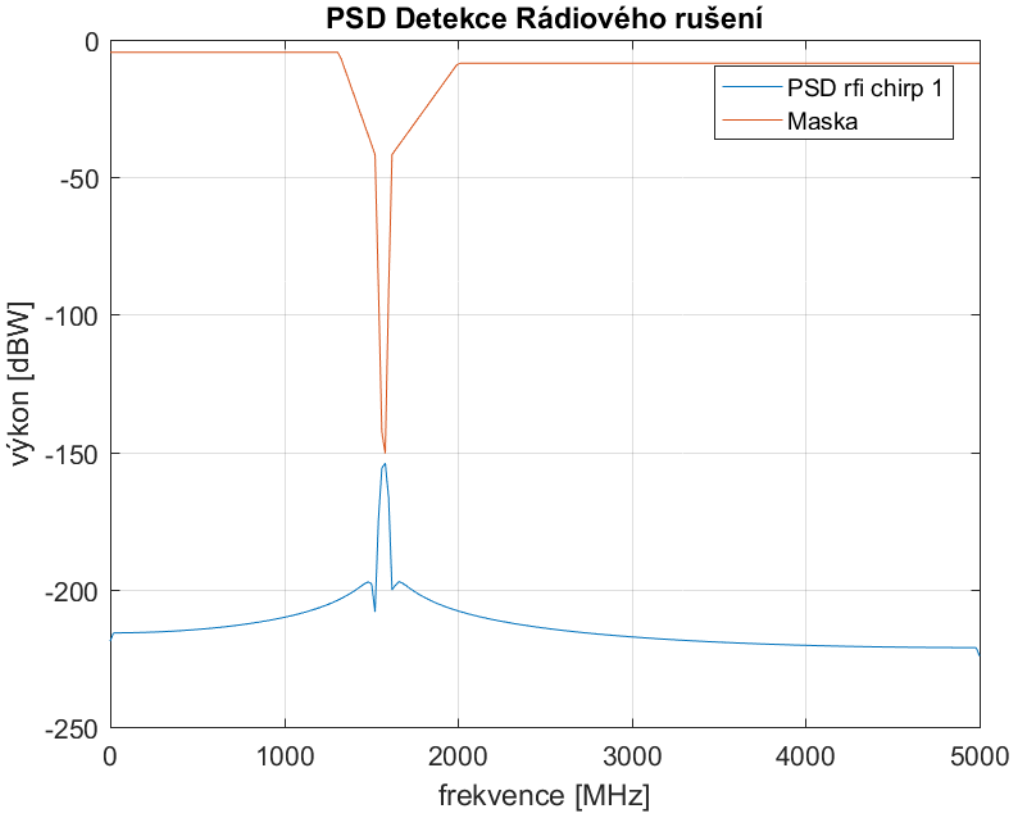


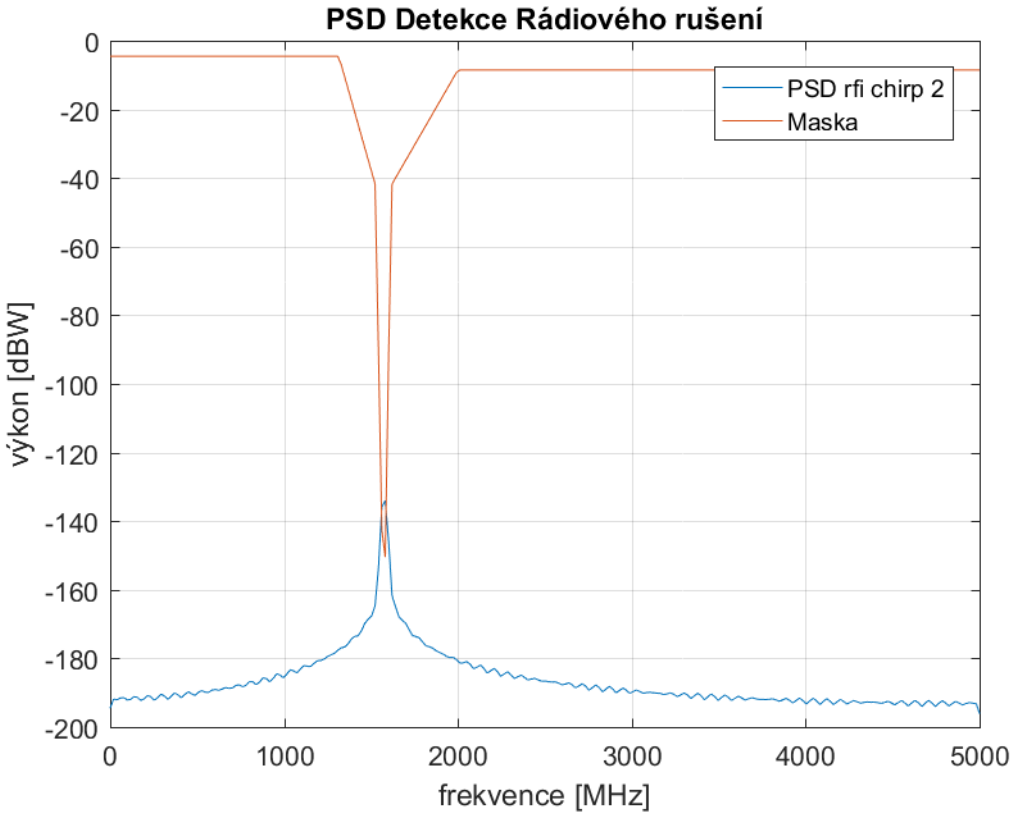


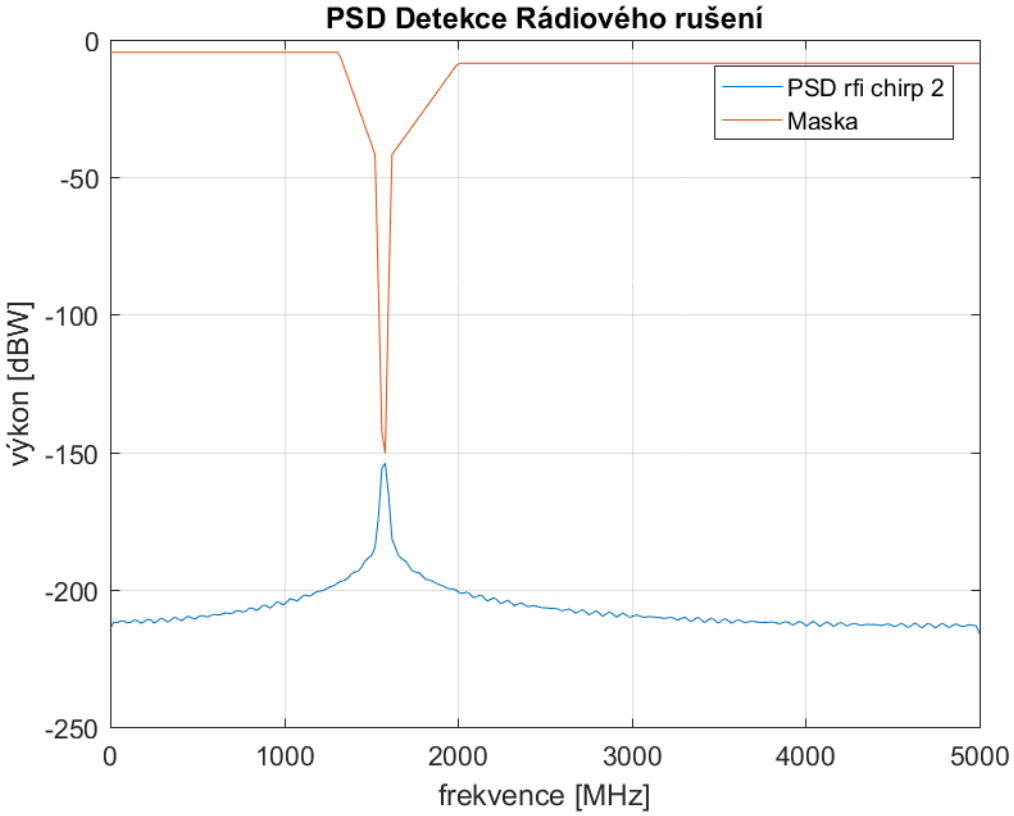

PSD Detekce Rádiového rušení
PSD rfi FM
Maska
výkon [dBW]
frekvence [MHz]
0
-50
-100
-150
-200
-250
0
1000
2000
3000
4000
5000

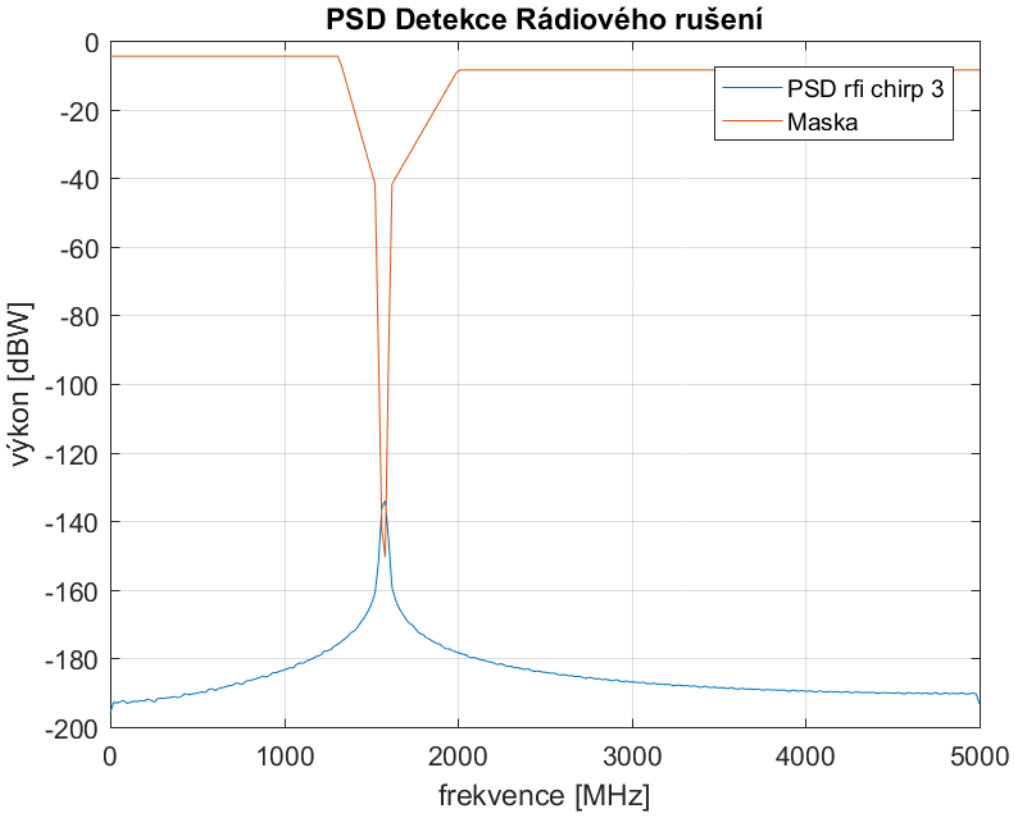

PSD Detekce Rádiového rušení
PSD rfi FM
Maska
výkon [dBW]
frekvence [MHz]
0
-50
-100
-150
-200
-250
0
1000
2000
3000
4000
5000

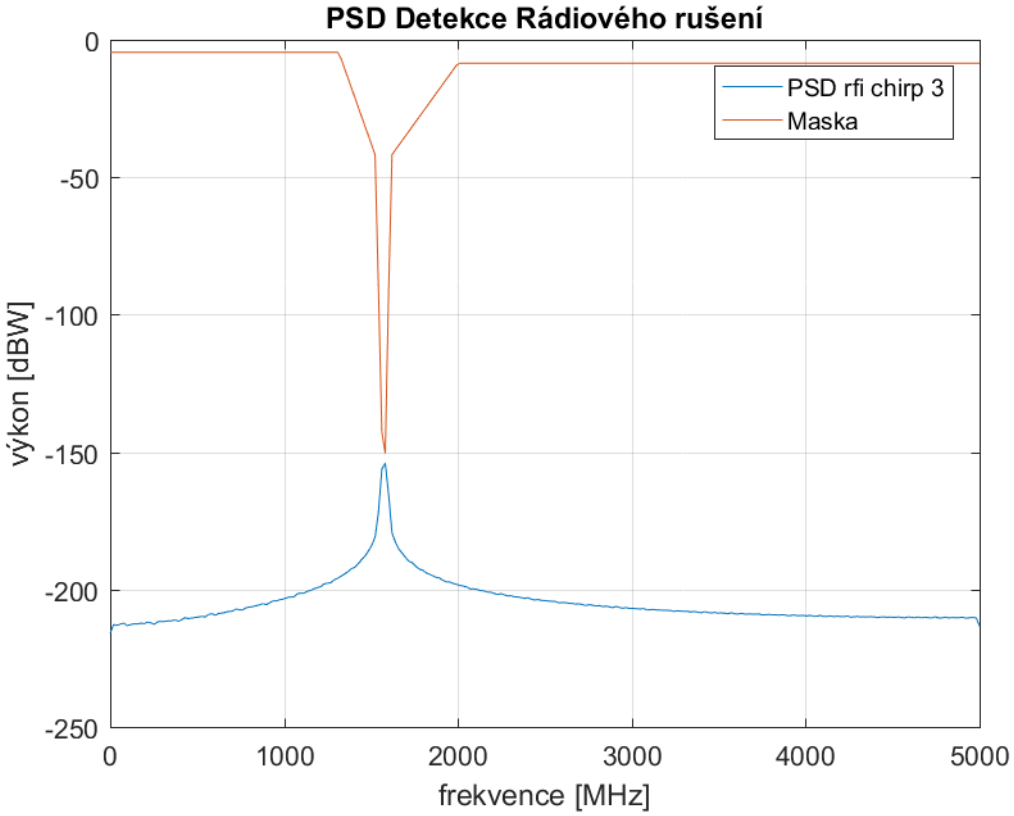

PSD Detekce Rádiového rušení
PSD rfi chirp 1
Maska
výkon [dBW]
frekvence [MHz]
0
-50
-100
-150
-200
-250
0
1000
2000
3000
4000
5000

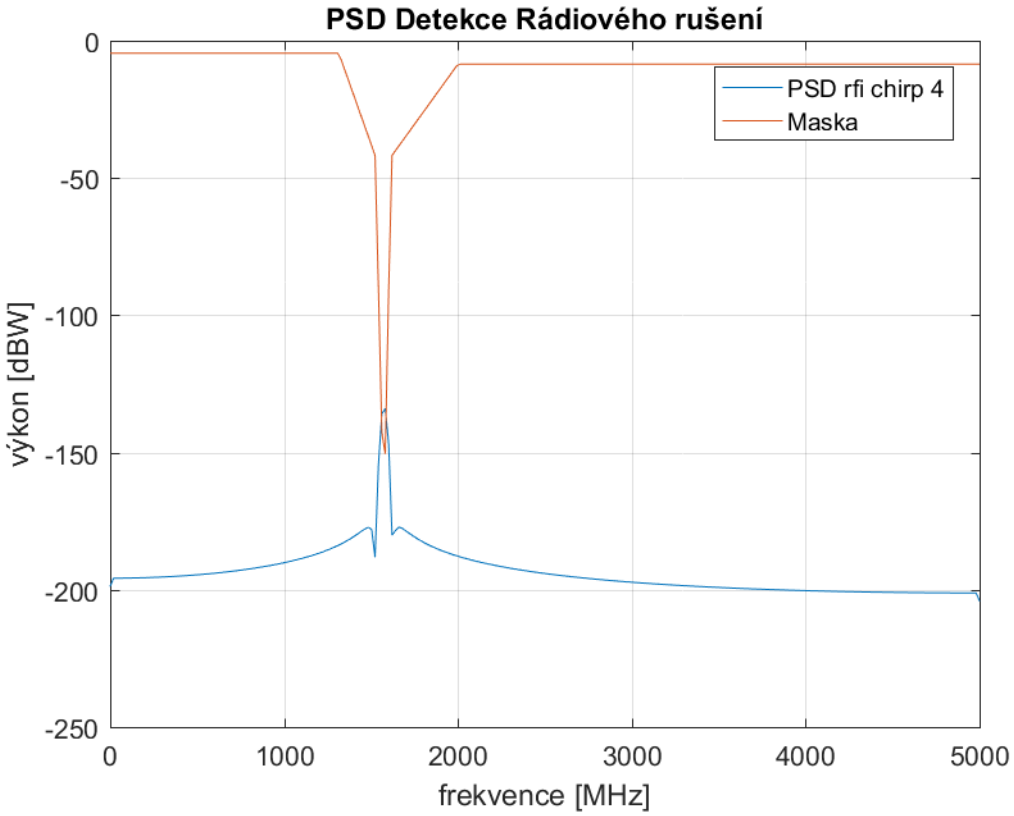

PSD Detekce Rádiového rušení
PSD rfi chirp 1
Maska
výkon [dBW]
frekvence [MHz]
0
-50
-100
-150
-200
-250
0
1000
2000
3000
4000
5000

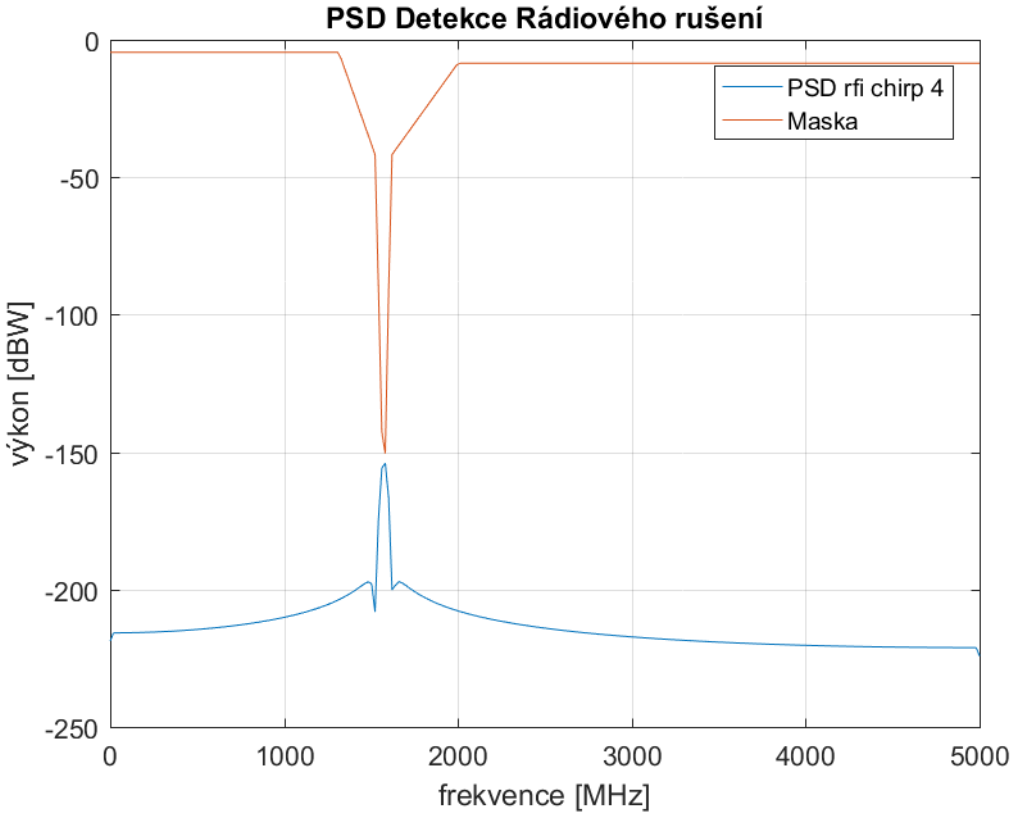

PSD Detekce Rádiového rušení
PSD rfi chirp 2
Maska
výkon [dBW]
frekvence [MHz]
0
-20
-40
-60
-80
-100
-120
-140
-160
-180
-200
0
1000
2000
3000
4000
5000


PSD Detekce Rádiového rušení
PSD rfi chirp 2
Maska
výkon [dBW]
frekvence [MHz]
0
-50
-100
-150
-200
-250
0
1000
2000
3000
4000
5000

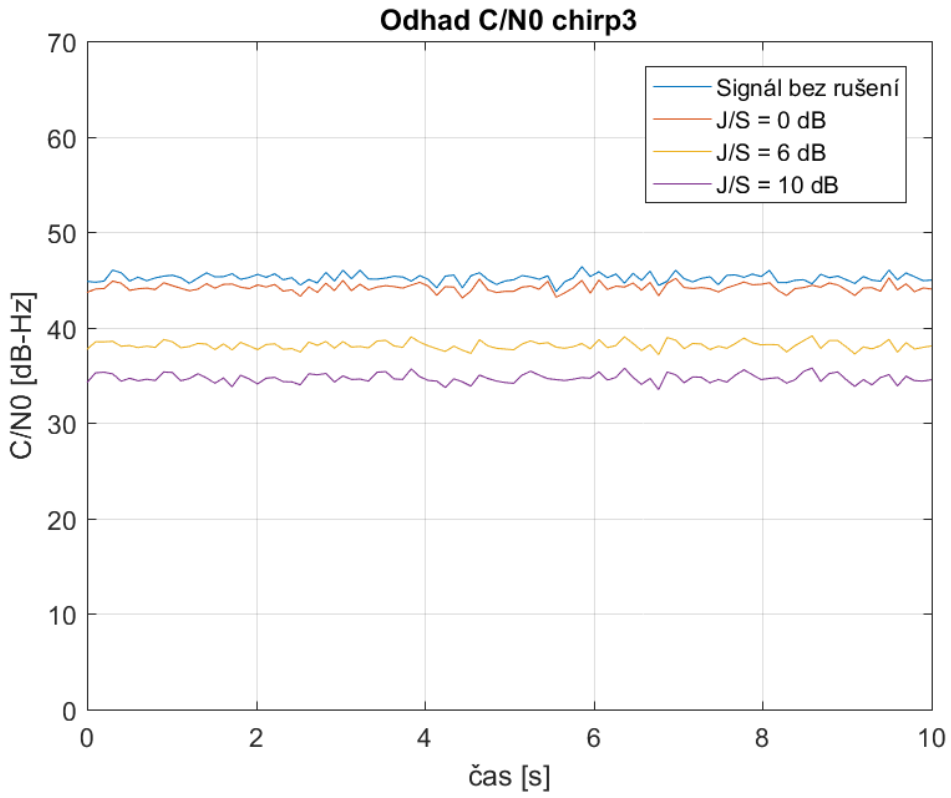

PSD Detekce Rádiového rušení
PSD rfi chirp 3
Maska
výkon [dBW]
frekvence [MHz]
0
-20
-40
-60
-80
-100
-120
-140
-160
-180
-200
0
1000
2000
3000
4000
5000

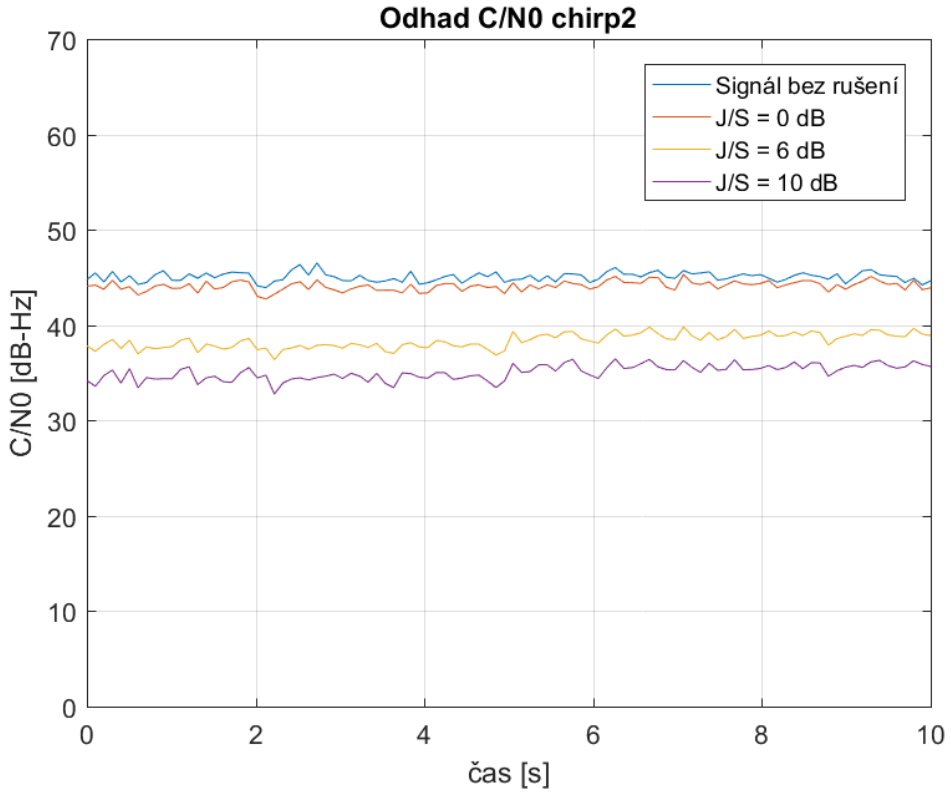

PSD Detekce Rádiového rušení
PSD rfi chirp 3
Maska
výkon [dBW]
frekvence [MHz]
0
-50
-100
-150
-200
-250
0
1000
2000
3000
4000
5000

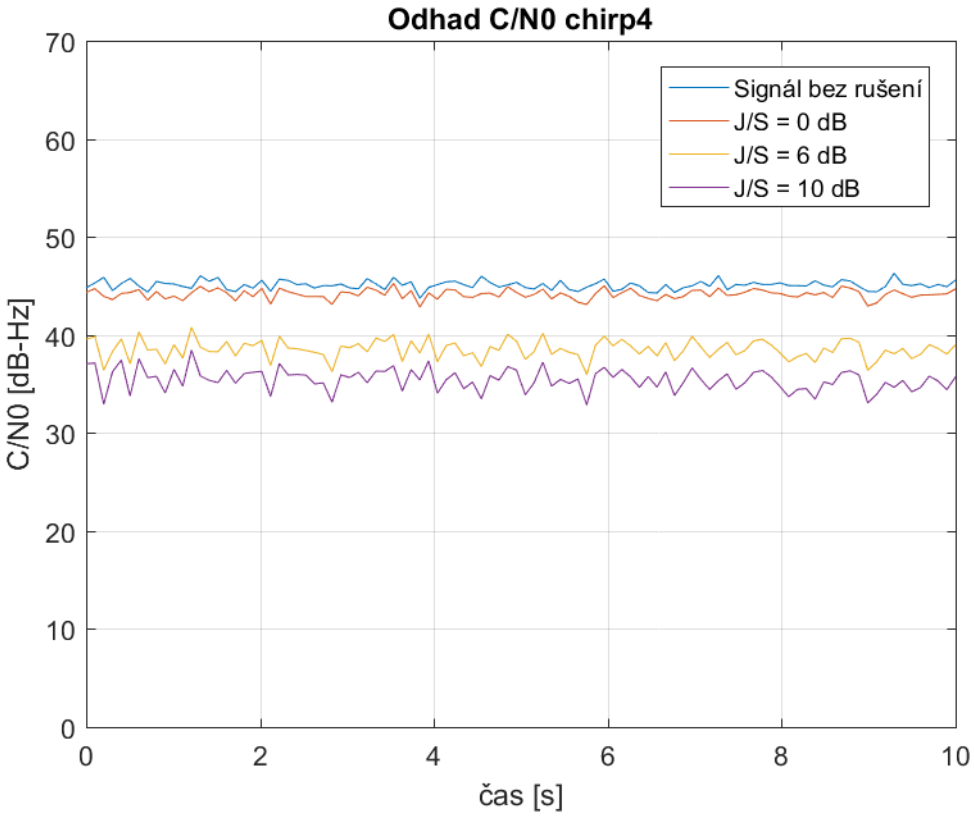

PSD Detekce Rádiového rušení
PSD rfi chirp 4
Maska
výkon [dBW]
frekvence [MHz]
0
-50
-100
-150
-200
-250
0
1000
2000
3000
4000
5000


PSD Detekce Rádiového rušení
PSD rfi chirp 4
Maska
výkon [dBW]
frekvence [MHz]
0
-50
-100
-150
-200
-250
0
1000
2000
3000
4000
5000

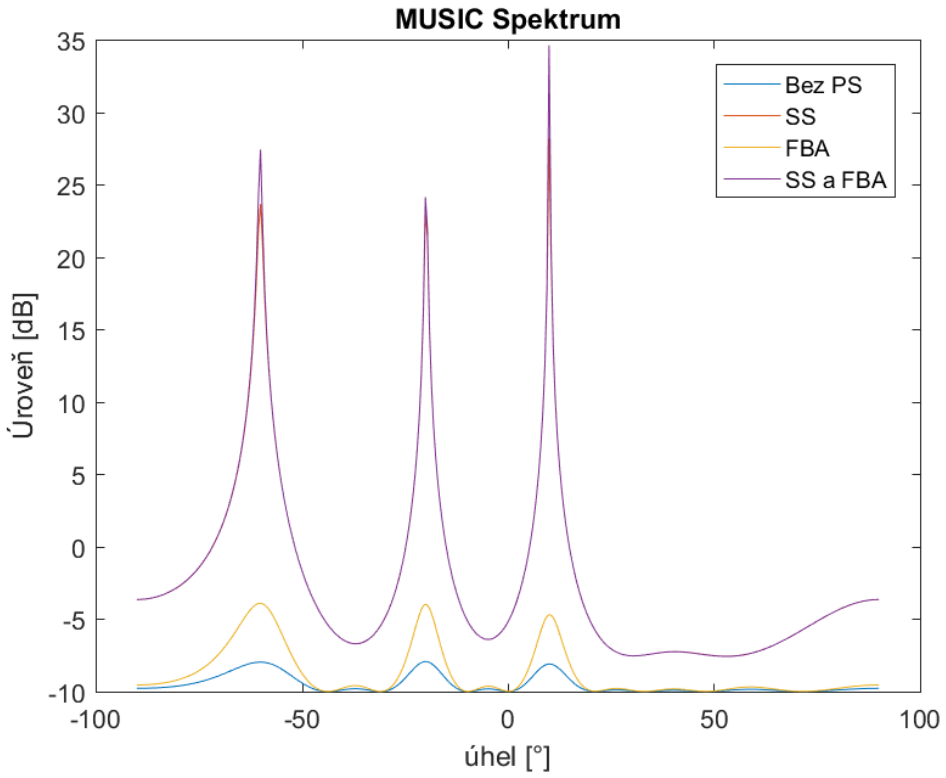
Příloha B

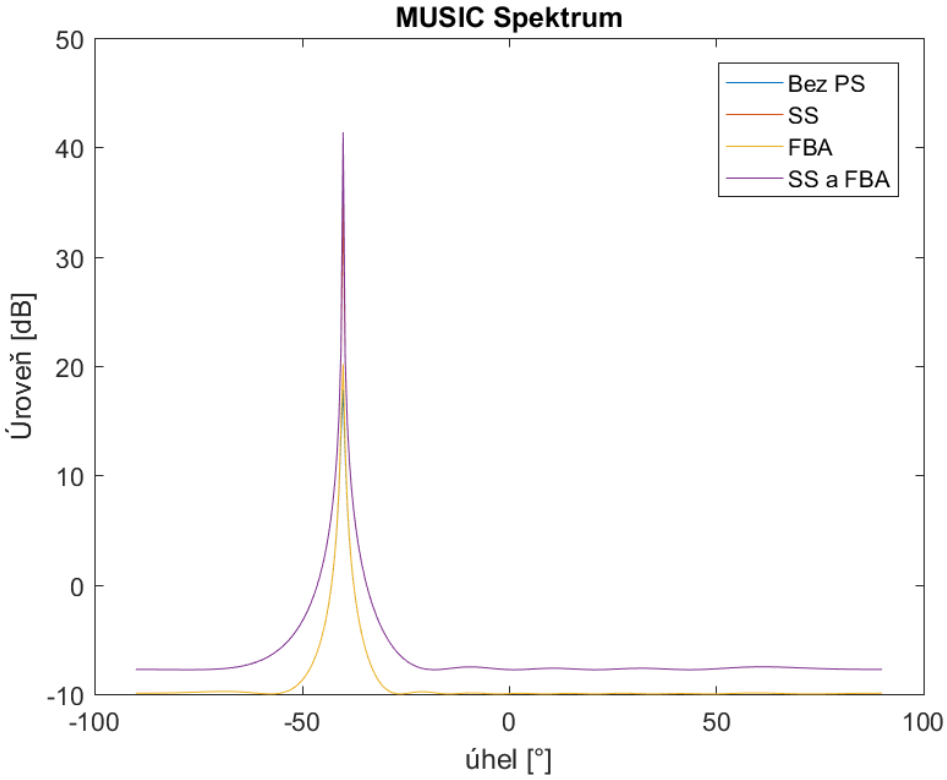

Odhad C/N0 chirp3
Signál bez rušení
J/S = 0 dB
J/S = 6 dB
J/S = 10 dB
C/N0 [dB-Hz]
čas [s]
0
10
20
30
40
50
60
70
0
2
4
6
8
10

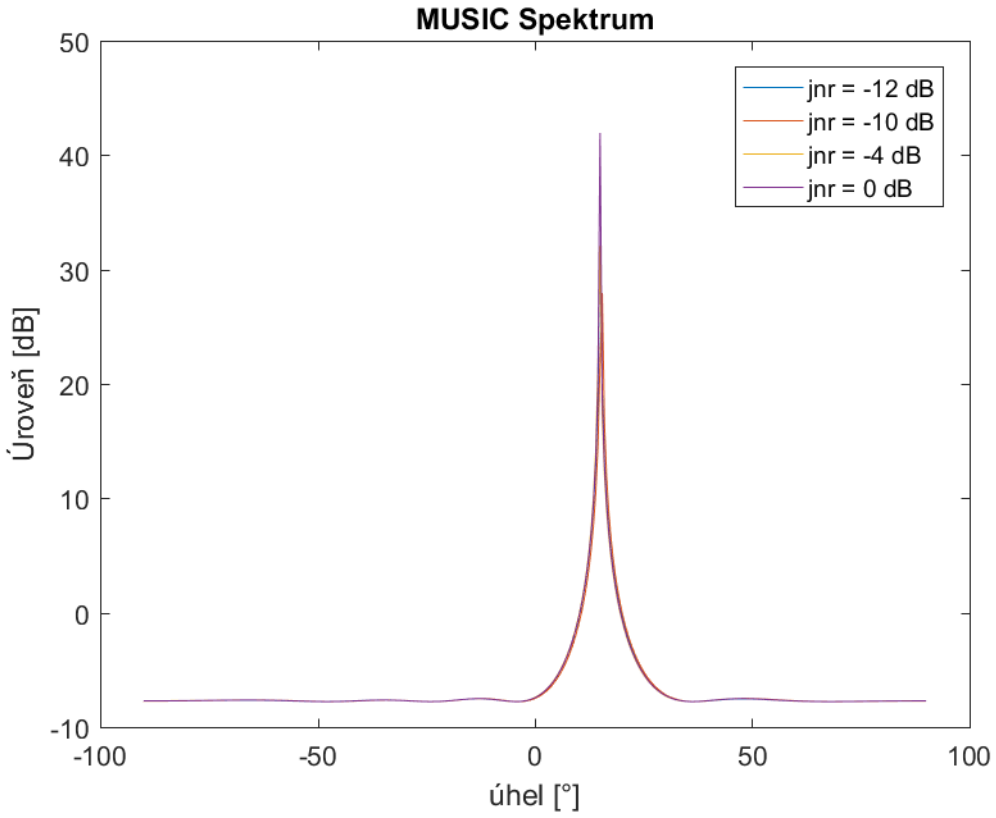

Odhad C/N0 chirp2
Signál bez rušení
J/S = 0 dB
J/S = 6 dB
J/S = 10 dB
C/N0 [dB-Hz]
čas [s]
0
10
20
30
40
50
60
70
0
2
4
6
8
10


Odhad C/N0 chirp4
Signál bez rušení
J/S = 0 dB
J/S = 6 dB
J/S = 10 dB
C/N0 [dB-Hz]
čas [s]
0
10
20
30
40
50
60
70
0
2
4
6
8
10

Příloha C


MUSIC Spektrum
Bez PS
SS
FBA
SS a FBA
Úroveň [dB]
úhel [°]
35
30
25
20
15
10
5
0
-5
-10
-100
-50
0
50
100


MUSIC Spektrum
Bez PS
SS
FBA
SS a FBA
Úroveň [dB]
úhel [°]
50
40
30
20
10
0
-10
-100
-50
0
50
100


MUSIC Spektrum
jnr = -12 dB
jnr = -10 dB
jnr = -4 dB
jnr = 0 dB
Úroveň [dB]
úhel [°]
50
40
30
20
10
0
-10
-100
-50
0
50
100