ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ

Fakulta Elektrotechnická

Detekce a lokalizace rušení GNSS systémů

Detection and Localization of the GNSS Systems Jamming

Viktor Loužil

Diplomová práce

2017

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Loužil** Jméno: **Viktor** Osobní číslo: **392772**

Fakulta/ústav: **Fakulta elektrotechnická**

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

Studijní program: **Komunikace, multimédia a elektronika**

Studijní obor: **Bezdrátové komunikace**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Detekce a lokalizace rušení GNSS systémů

Název diplomové práce anglicky:

Detection and Localization of the GNSS Systems Jamming

Pokyny pro vypracování:

Vypracujte přehled typů signálů, které mohou potenciálně rušit družicové navigační systémy. Proveďte rešerši metod detekce a lokalizace zdrojů rušení. Zabývejte se možností generování rušení pomocí softwarově definovaných rádiových zařízení (SDR) za účelem testování odolnosti GNSS přijímačů vůči rušení a testování systémů detekce a lokalizace rušení. Vytvořte program pro generování vybraných typů rušivých signálů.

Seznam doporučené literatury:

[1] Kaplan, E.: Understading GPS, Principes and Applicatios, Second Eddition, Artach House 2006, ISBN-10: 1-58053-894-0.
[2] Kovář, P.: Družicová navigace, Od teorie k aplikacím v softwarovém přijímači. ČVUT 2016, ISBN 978-80-01-05989-0.

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: **01.02.2017** Termín odevzdání diplomové práce: **26.05.2017**

Platnost zadání diplomové práce: **25.05.2018**

Podpis vedoucí(ho) práce	Podpis vedoucí(ho) ústavu/katedry	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.

Datum převzetí zadání	Podpis studenta

Abstrakt

Tato práce se zabývá analýzou rušivých signálů negativně ovlivňujících činnost GNSS systémů. Rušivé signály jsou nejprve podrobně klasifikovány. Následuje rozbor metod jejich detekce a lokalizace. Praktická část je věnována generování vybraných rušivých signálů pomocí softwarového prostředí Matlab.

Abstract

This thesis deals with jamming signals which have negative impact on GNSS systems. Jamming signal are researched in detail. An analysis of their detection a localization methods follows. The practical part is devoted to development of Matlab scripts for generating selected jamming signals.

Klíčová slova

GNSS, rušení, spoofing, detekce, lokalizace, Matlab

Keywords

GNSS, jamming, spoofing, detection, localization, Matlab

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 26. května 2017

_____

vlastnoruční podpis autora

Poděkování

Na tomto místě bych rád poděkoval doc. Dr. Ing. Pavlu Kovářovi za cenné připomínky a odborné rady, kterými přispěl k vypracování této diplomové práce.

OBSAH

ÚVOD

Řízení letového provozu České republiky a.s. (dále jen ŘLP) se v současné době potýká s dlouhodobým problémem rádiového rušení GNSS signálů. Kamenem úrazu je v případě ŘLP klíčová závislost multilateračního systému MLAT od pardubické společnosti ERA a.s. na přesné synchronizaci jednotlivých prvků systému. Tato synchronizace je totiž realizována na základě hodinového signálu GNSS družic a v případě aktivního rušení tak věrohodnost polohových údajů dodaných systémem MLAT výrazně klesá. Rušení, které je v současné době zaznamenáváno, zatím nemá pro funkčnost systému fatální následky. Tato situace se však může rázem změnit, a to zejména vlivem rostoucího trendu softwarově definovaných rádií, jejichž cenová dostupnost a uživatelská základna každým dnem roste. Přes bezpečnostní rizika a závažnost možných následků je problematika rušení GNSS signálů v současné době zásadně podceňována.

Cílem této práce je klasifikovat rušivé signály, jež by svým charakterem mohly ohrozit dostupnost GNSS signálů v kritických uzlech infrastruktury ŘLP. Dále analyzovat možné metody detekce potenciálně rušivých signálů a zároveň navrhnout konkrétní metody jejich lokalizace. V rámci praktické části této práce jsou tyto potencionálně rušivé signály vygenerovány pomocí softwarového prostředí Matlab a připraveny k implementaci do softwarově definovaného rádia. V závěru jsou navrženy konfigurace měřícího pracoviště, na jejichž základě je možné provést simulaci reálného útoku a objektivně posoudit vliv na výslednou přesnost určení polohy.

1 RUŠIVÉ SIGNÁLY

Z hlediska GNSS signálů považujeme za rušení takové elektromagnetické záření, které způsobuje narušení jejich integrity a může vést ke krátkodobému výpadku, úplné ztrátě nebo falsifikaci polohových údajů udávaných přijímačem.

1.1 Základní rozdělení rušivých signálů

Na úvod lze rušení rozdělit do dvou elementárních skupin z pohledu povahy jejich původce. První skupinou je rušení neúmyslné, jehož původce nemá žádný zájem o narušení dostupnosti GNSS služeb. Druhou skupinou je rušení úmyslné, jehož původce má jasný záměr o znehodnocení polohových údajů dodávaných systémem. Z pohledu EMC bychom mohli rušení dále rozdělit na přírodní a umělé. Takovéto rozdělení je však pro naši aplikaci nepodstatné.

NEÚMYSLNÉ RUŠENÍ

Neúmyslné rušení může být charakterizováno např. emisním vyzařováním některých elektronických zařízení. Tento typ rušení je v reálném prostředí takřka všudypřítomný a jeho výskyt tak lze s určitou rezervou předpovídat. Výrazně nebezpečnější a na první pohled skrytou hrozbou je rušení, které je způsobeno koexistencí dalších rádiových systémů. Ty mohou svými vyššími harmonickými kmitočty s dotčeným systémem interferovat.

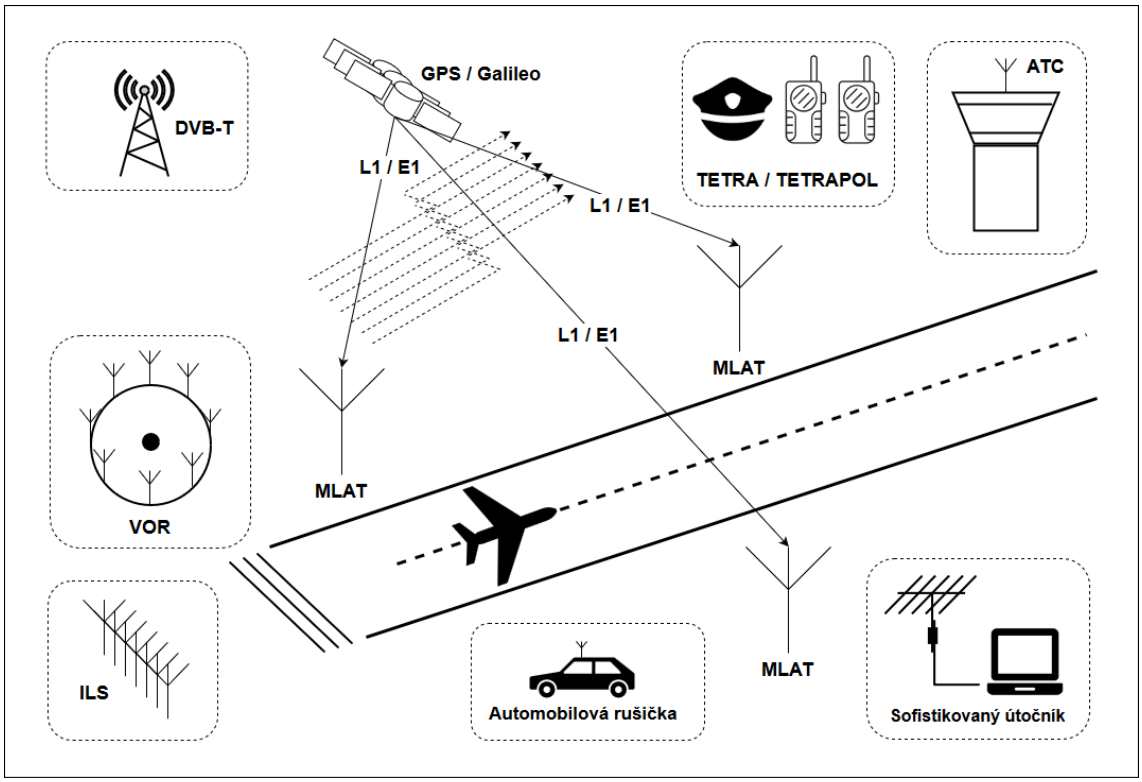
ÚMYSLNÉ RUŠENÍ

Úmyslné rušení má za cíl zcela vyřadit nebo alespoň částečně omezit určitý rádiový systém, a v tom nejhorším případě nad ním zcela nepozorovaně převzít úplnou kontrolu. Tento typ rušení je realizován soustředěním elektromagnetické energie v rámci RF kmitočtů, na kterých cílený systém pracuje a někdy také do směrů, ve kterých se prvky daného systému nacházejí. Tento typ rušení zpravidla generují zařízení k tomu speciálně uzpůsobená.

1.2 Zdroje rušivých signálů

Družice systémů GNSS se nachází ve vzdálenosti přibližně 20 000 *km* od povrchu Země. Vysílací výkony družicových vysílačů se pohybují okolo 20 *W*. Signály družic GNSS jsou tak na Zemi dostupné s velice slabou výkonovou úrovní. Vzhledem k takto nízké úrovni družicových signálů jsou přijímače extrémně náchylné na nejrůznější typy rušení.

Následující obrázek vyjadřuje situační schéma rádiového provozu v okolí letiště. Všechny uvedené rádiové systémy mohou svým vysíláním ovlivnit dostupnost GNSS signálů, na kterých je závislý provoz vybraných letištních aplikací.



Obrázek 1: Situační schéma rádiového provozu v okolí letiště

2 NEÚMYSLNÉ RUŠENÍ

V rámci této kapitoly se budeme zabývat především případem neúmyslného rušení způsobeného koexistentními rádiovými systémy a jejich harmonickými kmitočty. Jedná se zejména o úzkopásmové signály digitálních trunkových systémů TETRA či TETRAPOL, širokopásmové signály televizního vysílání DVB-T, komunikační kanály řízení letového provozu ATC nebo letecké radionavigační služby VOR a ILS. Vzhledem k alokaci v rámci kmitočtového spektra a výkonům, na kterých tyto systémy vysílají, mohou jejich signály na svých vyšších harmonických kmitočtech interferovat s GNSS systémy a negativně ovlivňovat jejich dostupnost. V následujících kapitolách je z těchto důvodů podrobně vyšetřeno, kde by v rámci kmitočtového spektra mohlo k těmto „kmitočtových konfliktům“ docházet. Faktor neúmyslného rušení způsobeného emisním vyzařováním konkrétních elektronických zařízení je v této kapitole zcela zanedbán.

2.1 Digitální trunkové systémy

Všeobecné oprávnění č. VO-R5/07.2005-18 vydané Českým telekomunikačním úřadem stanovuje podmínky k provozování uživatelských terminálů rádiových sítí standardů TETRA (*Terrestrial Trunked Radio*) a TETRAPOL (*Terrestrial Trunked Radio Police)* [9]. Toto všeobecné oprávnění dedikuje pásmo 380-385 *MHz* pro uplink provoz systému TETRAPOL. V tomto pásmu je alokováno celkem 400 kanálů o šířce 12,5 *kHz*. Ve směru downlink je systému TETRAPOL dedikováno pásmo 390-395 *MHz*, kde je rovněž alokováno 400 kanálů o šířce 12,5 *kHz*. Dále toto všeobecné oprávnění dedikuje pásmo 410-415 *MHz* pro uplink provoz systému TETRA. V tomto pásmu je alokováno celkem 800 kanálů o šířce 6,25 *kHz*. Ve směru downlink je systému TETRA dedikováno pásmo 420-425 *MHz*, kde je rovněž alokováno 800 kanálů o šířce 6,25 *kHz*.

2.1.1 Rušení systému GPS

Následující tabulka znázorňuje, na jakých kmitočtech dochází k potencionálnímu konfliktu harmonických složek úzkopásmových komunikačních kanálů systému TETRAPOL a nosných kmitočtů systému GPS. Konfliktní kmitočty se nacházejí pouze v pásmu TETRAPOL 390-395 *MHz*. V pásmech TETRAPOL 380-385 *MHz*, TETRA 410-415 *MHz* a TETRA 420-425 *MHz* nebyly zaznamenány žádné konfliktní kmitočty, jejichž provoz by mohl negativně ovlivňovat provoz systému GPS.

	GPS L1 1575,42 *MHz*	**GPS L2** 1227,60 *MHz*	**GPS L5** 1176,45 *MHz*
TETRAPOL 390-395 *MHz*	④.		③. ③.

Tabulka 2.1: Rušení GPS signálů systémem TETRAPOL

Kmitočet L1 je potencionálně rušen ④. harmonickou složkou 309. kanálu systému TETRAPOL, který je alokován na kmitočtu f_c = 393,85625 *MHz*. Kmitočet L5 je potencionálně rušen ③. harmonickou složkou 172. kanálu systému TETRAPOL, který je alokován na kmitočtu f_c = 392,14375 *MHz*. Dále je kmitočet L5 potencionálně rušen ③. harmonickou složkou vedlejšího 173. kanálu systému TETRAPOL, který je alokován na kmitočtu f_c = 392,15625 *MHz*.

2.1.2 Rušení systému Galileo

Stejně jako v předchozím případě následující tabulka znázorňuje, na jakých kmitočtech dochází k potencionálnímu konfliktu harmonických složek úzkopásmových komunikačních kanálů systému TETRAPOL a nosných kmitočtů systému Galileo. Konfliktní kmitočty se nacházejí pouze v pásmu TETRAPOL 390-395 *MHz*. Stejně jako v případě systému GPS nebyly v pásmech TETRAPOL 380-385 *MHz*, TETRA 410-415 *MHz* a TETRA 420-425 *MHz* zaznamenány žádné konfliktní kmitočty, jejichž provoz by mohl negativně ovlivňovat provoz systému GPS.

	Galileo E1 1575,42 *MHz*	**Galileo E6** 1278,75 *MHz*	**Galileo E5** 1191,79 *MHz*
TETRAPOL 390-395 *MHz*	④.		

Tabulka 2.2: Rušení Galileo signálů systémem TETRAPOL

Kmitočet E1 je potencionálně rušen ④. harmonickou složkou 309. kanálu systému TETRAPOL, který je alokován na kmitočtu f_c = 393,85625 *MHz*.

2.2 Digitální televizní vysílaní

Plán přidělení kmitočtových pásem vydaný Českým telekomunikačním úřadem [10] pro provoz digitálního televizního vysílání DVB-T (*Digital Video Broadcasting Terrestrial*) dedikuje kmitočtové pásmo 470-862 *MHz*. V tomto pásmu je alokováno celkem 49 kanálů o šířce 8 *MHz*.

2.2.1 Rušení systému GPS

Následující tabulka znázorňuje, na jakých kmitočtech dochází k potencionálnímu konfliktu harmonických složek širokopásmových televizních kanálů standardu DVB-T a nosných kmitočtů systému GPS.

	GPS L1 1575,42 *MHz*	**GPS L2** 1227,60 *MHz*	**GPS L5** 1176,45 *MHz*
DVB-T 470-862 *MHz*	②. ③.	②.	②.

Tabulka 2.3: Rušení GPS signálů vysíláním DVB-T

Kmitočet L1 je potencionálně rušen ②. harmonickou 40. kanálu standardu DVB-T, který je alokován na kmitočtu f_c = 786 *MHz*. Dále je kmitočet L1 potencionálně rušen ③. harmonickou 7. kanálu standardu DVB-T, který je alokován na kmitočtu f_c = 522 *MHz*. Kmitočet L2 je potencionálně rušen ②. harmonickou 18. kanálu standardu DVB-T, který je alokován na kmitočtu f_c = 610 *MHz*. Kmitočet L5 je potencionálně rušen ②. harmonickou 15. kanálu standardu DVB-T, který je alokován na kmitočtu f_c = 586 *MHz*.

2.2.2 Rušení systému Galileo

Následující tabulka znázorňuje, na jakých kmitočtech dochází k potencionálnímu konfliktu harmonických složek širokopásmových televizních kanálů standardu DVB-T a nosných kmitočtů systému Galileo.

	Galileo E1 1575,42 *MHz*	**Galileo E6** 1278,75 *MHz*	**Galileo E5** 1191,79 *MHz*
DVB-T 470-862 *MHz*	②. ③.	②.	②.

Tabulka 2.4: Rušení Galileo signálů vysíláním DVB-T

Kmitočet E1 je potencionálně rušen ②. harmonickou 40. kanálu standardu DVB-T, který je alokován na kmitočtu f_c = 786 *MHz*. Dále je kmitočet E1 potencionálně rušen ③. harmonickou 7. kanálu standardu DVB-T, který je alokován na kmitočtu f_c = 522 *MHz*. Kmitočet E6 je potencionálně rušen ②. harmonickou 22. kanálu standardu DVB-T, který je alokován na kmitočtu f_c = 642 *MHz*. Kmitočet E5 je potencionálně rušen ②. harmonickou 16. kanálu standardu DVB-T, který je alokován na kmitočtu f_c = 594 *MHz*.

2.3 Řízení letového provozu

Evropská tabulka frekvenčních alokací ECA (*European Common Allocation*) [6] vydaná Evropskou komisí elektronických komunikací ECC (*Electronic Communications Committee*) dedikuje kmitočtové pásmo 108-117,95 MHz pro účely radionavigačních systémů VOR / ILS. V tomto pásmu je alokováno celkem 200 kanálů a šířce 50 *kHz*. Dále ECA dedikuje kmitočtové pásmo 117,975-137 *MHz* pro účely služeb řízení letového provozu ATC (*Air Traffic Control*). V tomto pásmu je alokováno celkem 760 kanálů o šířce 25 *kHz*.

2.3.1 Rušení systému GPS

Následující tabulka znázorňuje, na jakých kmitočtech dochází k potencionálnímu konfliktu harmonických složek komunikačních kanálů řízení letového provozu ATC a nosných kmitočtů systému GPS.

	GPS L1 1575,42 *MHz*	**GPS L2** 1227,60 *MHz*	**GPS L5** 1176,45 *MHz*
ATC 117,975-137 *MHz*	⑫. ⑬.	⑨. ⑩.	⑨.

Tabulka 2.5: Rušení GPS signálů službami ATC

Kmitočet L1 je potencionálně rušen ⑫. harmonickou 532. kanálu služeb ATC, který je alokován na kmitočtu f_c = 131,275 *MHz*. Dále je kmitočet L1 potencionálně rušen ⑬. harmonickou 128. kanálu služeb ATC, který je alokován na kmitočtu f_c = 121,175 *MHz*. Kmitočet L2 je potencionálně rušen ⑨. harmonickou 737. kanálu služeb ATC, který je alokován na kmitočtu f_c = 136,400 *MHz*. Dále je kmitočet L2 potencionálně rušen ⑩. harmonickou 191. kanálu služeb ATC, který je alokován na kmitočtu f_c = 122,750 *MHz*. Kmitočet L5 je potencionálně rušen ⑨. harmonickou 510. kanálu služeb ATC, který je alokován na kmitočtu f_c = 130,725 *MHz*.

2.3.2 Rušení systému Galileo

Následující tabulka znázorňuje, na jakých kmitočtech dochází k potencionálnímu konfliktu harmonických složek komunikačních kanálů řízení letového provozu ATC a nosných kmitočtů systému Galileo.

	Galileo E1 1575,42 *MHz*	**Galileo E6** 1278,75 *MHz*	**Galileo E5** 1191,79 *MHz*
ATC 117,975-137 *MHz*	⑫. ⑬.	⑩.	⑨. ⑩.

Tabulka 2.6: Rušení Galileo signálů službami ATC

Kmitočet E1 je potencionálně rušen ⑫. harmonickou 532. kanálu služeb ATC, který je alokován na kmitočtu f_c = 131,275 *MHz*. Dále je kmitočet E1 potencionálně rušen ⑬. harmonickou 128. kanálu služeb ATC, který je alokován na kmitočtu f_c = 121,175 *MHz*. Kmitočet E6 je potencionálně rušen ⑩. harmonickou 396. kanálu služeb ATC, který je alokován na kmitočtu f_c = 127,875 *MHz*. Kmitočet L5 je potencionálně rušen ⑨. harmonickou 578. kanálu služeb ATC, který je alokován na kmitočtu f_c = 132,425 *MHz*. Dále je kmitočet L5 potencionálně rušen ⑩. harmonickou 48. kanálu služeb ATC, který je alokován na kmitočtu f_c = 119,175 *MHz*.

2.4 Letecké radionavigační služby

Evropská tabulka frekvenčních alokací ECA (*European Common Allocation*) [6] vydaná Evropskou komisí elektronických komunikací ECC (*Electronic Communications Committee*) dedikuje kmitočtové pásmo 108-117,95 MHz pro účely radionavigačních systémů VOR (*VHF Omni Directional Radio Range*) a ILS (*Instrumental Landing System*). V tomto pásmu je alokováno celkem 200 kanálů a šířce 50 *kHz*. Letecký radionavigační systém DME (*Distance Measuring Equipment*), který je obvykle instalován soustředně s anténami systému VOR, má dedikované pásmo 960-1164 *MHz* [6] a jeho harmonické kmitočty tak nemůžou do pásma vyhrazeného pro GNSS systémy zasáhnout.

2.4.1 Rušení systému GPS

Následující tabulka znázorňuje, na jakých kmitočtech dochází k potencionálnímu konfliktu harmonických složek signálů radionavigačních systémů VOR / ILS a nosných kmitočtů systému GPS.

	GPS L1 1575,42 *MHz*	**GPS L2** 1227,60 *MHz*	**GPS L5** 1176,45 *MHz*
VOR / ILS 108-117,95 *MHz*	⑭.	⑪. ⑪.	⑩.

Tabulka 2.7: Rušení GPS signálů systémy VOR a ILS

Kmitočet L1 je potencionálně rušen ⑭. harmonickou 91. kanálu radionavigačních systémů VOR / ILS, který je alokován na kmitočtu f_c = 112,525 *MHz*. Kmitočet L2 je potencionálně rušen ⑪. harmonickou 72. kanálu radionavigačních systémů VOR / ILS, který je alokován na kmitočtu f_c = 111,575 *MHz*. Dále je kmitočet L2 potencionálně rušen ⑪. harmonickou vedlejšího 73. kanálu radionavigačních systémů VOR / ILS, který je alokován na kmitočtu f_c = 111,625 *MHz*. Kmitočet L5 je potencionálně rušen ⑩. harmonickou 193. kanálu radionavigačních systémů VOR / ILS, který je alokován na kmitočtu f_c = 117,625 *MHz*.

2.4.2 Rušení systému Galileo

Následující tabulka znázorňuje, na jakých kmitočtech dochází k potencionálnímu konfliktu harmonických složek signálů radionavigačních systémů VOR / ILS a nosných kmitočtů systému Galileo.

	Galileo E1 1575,42 *MHz*	**Galileo E6** 1278,75 *MHz*	**Galileo E5** 1191,79 *MHz*
VOR / ILS 108-117,95 *MHz*	⑭.	⑪. ⑪.	⑪.

Tabulka 2.8: Rušení Galileo signálů systémy VOR a ILS

Kmitočet E1 je potencionálně rušen ⑭. harmonickou 91. kanálu radionavigačních systémů VOR / ILS, který je alokován na kmitočtu f_c = 112,525 *MHz*. Kmitočet E6 je potencionálně rušen ⑪. harmonickou 165. kanálu radionavigačních systémů VOR / ILS, který je alokován na kmitočtu f_c = 116,225 *MHz*. Dále je kmitočet E6 potencionálně rušen ⑪. Harmonickou vedlejšího 166. kanálu radionavigačních systémů VOR / ILS, který je alokován na kmitočtu f_c = 116,275 *MHz*. Kmitočet L5 je potencionálně rušen ⑪. harmonickou 7. kanálu radionavigačních systémů VOR / ILS, který je alokován na kmitočtu f_c = 108,325 *MHz*.

3 ÚMYSLNÉ RUŠENÍ

Úmyslné rušení je druhou elementární skupinou, s kterou se jako provozovatelé kritických rádiových systémů můžeme setkat. Takové rušení má zpravidla za cíl zcela vyřadit nebo alespoň částečně omezit určitý rádiový systém. Tento typ rušení je realizován soustředěním elektromagnetické energie v rámci kmitočtů, na kterých cílený systém pracuje, případně do směrů, ve kterých se prvky daného systému nachází. Oproti předchozímu případu neúmyslného rušení je tento typ generován pomocí zařízení, která jsou k tomu speciálně uzpůsobená. Nejčastěji v tomto směru setkáváme s výrazem „rušička“ (v angl. lit. *Jammer*). V této práci se však čtenář může setkat spíše s obecnějším pojmenováním „zdroj rušivých signálů“.

3.1 Základní rozdělení

Úmyslné rušivé signály, kterými se v této kapitole budeme zabývat, lze dále klasifikovat do třech skupin podle toho, jakým způsobem je cílený rádiový systém napaden. Toto rozdělení zároveň vypovídá o technické úrovni, na jaké je dané zařízení zkonstruováno, a může tak pomoci klasifikovat povahu samotného útočníka.

JAMMING

První skupinou je rušení typu *Jamming*, které lze charakterizovat jako tzv. „rušení hrubou silou“. Samotný princip rušení je v tomto případě založen primárně na vysílání signálu o relativně velkém výkonu. Mohou být použity nejrůznější typy kontinuálních a impulsních signálů. Odhalení takového útoku je relativně jednoduché, a to zejména díky vysokému výkonu rušivého signálu.

SPOOFING

Druhou skupinou je rušení typu *Spoofing*, které lze oproti tomu považovat za sofistikovanou formu rušení. V tomto případě se vysíláním silně korelovaných rušivých signálů snažíme docílit synchronizaci přijímače právě na tyto signály. S časovou základnou těchto rušivých signálů pak můžeme libovolně manipulovat a zkreslovat tak údaje o poloze, jež jsou přijímačem interpretovány. V dalším scénáři mohou být prostřednictvím těchto signálů do navigační zprávy zaneseny chybné údaje o polohách družic, které přijímač bez povšimnutí vyhodnotí a stejně jako v předchozím případě pak uživateli interpretuje chybné údaje o poloze.

Signály typu *Spoofing* je možné vysílat s až několikanásobně nižšími výkony než v předchozím případě, čímž se tento typ rušení zároveň stává výrazně hůře detekovatelným.

SEMI-SPOOFING

Poslední skupinou je tzv. *Semi-spoofing*, který lze do jisté míry považovat za inteligentní formu rušení. V tomto případě se vysíláním slabě korelovaných signálů snažíme v rámci přijímače docílit krátkodobých výpadků družicového signálu, které jsou podněcovány jeho snahou o synchronizaci právě na tyto signály.

3.2 Rušení typu Jamming

Rušení typu *Jamming* někdy označované pouze jako RFI (*Radio Frequency Interference*) je nejjednodušším a nejčastěji využívaným způsobem, jak přijímači omezit případně zcela znemožnit přístup k navigačním signálům GNSS družic. Stavu, kdy je uživatelskému zařízení znemožněn přístup k polohovým službám GNSS systémů, je dosaženo zpravidla vysíláním rušivého signálu s relativně velkým výkonem. V praxi je pak rušivý signál vysílán přímo na daném kmitočtu nebo je rozmítán v jeho těsné blízkosti. Použití impulsních signálu a signálů s rozprostřeným spektrem také není vyloučeno.

3.2.1 Obecné ohrožení

Na internetu je k dostání velké množství GPS rušiček. Efektivní dosah těchto rušiček je výrobci udáván v řádu jednotek metrů. Realita je však odlišná a tato vzdálenost je zpravidla mnohonásobně vyšší. Pro některé prvky kritické infrastruktury, jako je právě institut ŘLP, tak může mít ilegální užívání těchto rušiček zcela fatální následky. V této souvislosti lze uvést příklad nepoctivého řidiče dodávkové služby [2]. Ten může jednoduše žít v domnění, že zakoupil rušičku GPS signálu, která funguje do vzdálenosti 20 *m* a pouze znemožní zaměstnavateli, aby v určitých situacích (např. při cestě na nákup) mohl sledovat jeho polohu. Ve skutečnosti však bude zcela nevědomky rušit GNSS signál v širokém okolí letiště, kolem kterého každý den pravidelně projíždí. V rámci tohoto hypotetického scénáře se tak bavíme o v podstatě „neškodném“ záměru, který však s sebou přináší vážné vedlejší účinky. Relativně levným čínským zařízením (viz následující kapitola **3.2.2** „Třídy dostupných rušiček“) tak dnes v podstatě kdokoliv může zapříčinit zásadní bezpečnostní rizika.

Konkrétním příkladem obecného ohrožení mohou být útoky prováděné Severní Koreou v příhraničních oblastech jihokorejského Soulu [11]. Jihokorejským autoritám se tyto útoky daří lokalizovat, účinná obrana vůči nim však neexistuje. Severokorejci používají vysoce výkonné GPS

rušičky (pravděpodobně ruské výroby) a jsou tak schopni výrazně omezit dostupnost GPS signálů v centru samotného Soulu, jehož centrum se nachází pouhých 50 *km* od hranic. Tyto útoky tak mohou pocítit zejména řidiči osobních automobilů, kteří v rámci palubních navigací pozorují takřka neustálé výpadky polohové služby. Zaznamenané útoky mají zpravidla trvání několika dnů až týdnů a opakují se každým rokem zejména při americko-jihokorejských vojenských cvičeních [11]. Letecká doprava těmito útoky v zásadě není nijak ohrožena, neboť využívá alternativních navigačních systémů.

3.2.2 Třídy dostupných rušiček

Na internetu je k dostání celá řada nejrůznějších rušiček určených výhradně pro rušení GPS signálu. Jakékoliv rušení GPS signálu je ve většině vyspělých zemí samozřejmě ilegální. To však nijak nebrání čínským výrobcům elektroniky taková zařízení vyrábět a dále distribuovat. Tato zařízení jsou pak volně dostupná na některých specializovaných internetových obchodech [12] nebo čínských obchodních platformách [13]. Nabízené rušičky se pak liší zejména v konstrukčním uspořádání funkčních prvků a parametrech rušivého signálu. Z pohledu konstrukčního uspořádání je to především způsob, kterým je danému zařízení dodávána energie a také volba rádiových kmitočtů, jenž je zařízení schopno generovat, resp. rušit. Z hlediska typu signálu je hlavním kritériem snaha o co nejefektivnější rušení daného rádiového systému, která je podmíněna udržením co možná nejnižších výrobních nákladů. Z pohledu konstrukčního uspořádání šasi, napájení a operačních kmitočtů lze dostupné GPS rušičky rozdělit do následujících čtyřech tříd [26].

TŘÍDA I

Do první třídy patří rušičky určené do zdířek autozapalovačů. Napájení je tedy přizpůsobeno 12 *V* rozvodné síti automobilu. Jedná se o zpravidla tzv. monofrekvenční rušičky, které disponují schopností rušit dálkoměrný signál pouze na kmitočtu L1/E1. Tyto rušičky patří mezi nejdostupnější a jejich cena se na internetu pohybuje v rozmezí 30 až 50 *USD* [13].

TŘÍDA II

Do druhé třídy řadíme rušičky s vlastní baterií a integrovanou anténou. Oproti předchozímu případu se jedná o vysoce mobilní provedení, které může potenciální útočník bez problému schovat do kapsy. Tyto rušičky jsou speciálně konstruovány tak, aby připomínaly např. mobilní telefon nebo krabičku cigaret a byly tak špatně identifikovatelné. Tato taktická výhoda je však vykoupena horším dosahem, který je způsoben zabudováním vysílací antény do šasi

rušičky. Opět se jedná zpravidla o rušičky monofrekvenční, které jsou schopné vysílat pouze na kmitočtu L1/E1. Cena těchto rušiček se pohybuje v rozmezí 50 až 100 *USD* [13].

TŘÍDA III

Do třetí třídy patří rušičky s vlastní baterií a externími anténami, které jsou k rušičce připojeny pomocí SMA konektorů. Tyto rušičky jsou rovněž plně mobilní. Cena těchto rušiček se na internetu pohybuje v rozmezí 100 až 200 *USD* [12] v závislosti na operačních schopnostech inzerovaného zařízení. Oproti monofrekvenčním rušičkám I. a II třídy jsou totiž schopny rušit signál několika nezávislých rádiových systémů zároveň, podle čehož jsou pak vybaveny příslušným počtem antén. Tyto rušičky tak včetně signálu L1/E1 mají obvykle schopnost rušit i další GPS signály na kmitočtech L2 a L5 a zároveň jsou schopny rušit komunikaci rádiových systémů jako GSM, 3G, 4G nebo Wi-Fi.

TŘÍDA IV

Do čtvrté třídy patří robustní „stolní“ rušičky, které jsou oproti ostatním třídám konstruovány pro dlouhodobé statické využití. Hardware těchto rušiček je chráněn kovovým krytím, které je navíc opatřeno jak pasivním, tak aktivním chlazením umožňujícím nepřetržitý provoz. Z toho důvodu jsou zpravidla síťově napájeny, což také umožňuje větší efektivní dosahy. Tyto rušičky jsou schopny rušit družicové signály L1/E1, L2 a L5. Zároveň jsou standardně vybaveny schopností rušit komunikaci rádiových systémů jako GSM, 3G, 4G nebo Wi-Fi. Cena těchto rušiček na internetu šplhá až ke stovkám *USD* [12].

Obrázek 2: Rušička třídy I [12]

Obrázek 3: Rušička třídy II [12]

Obrázek 4: Rušička třídy III [12]

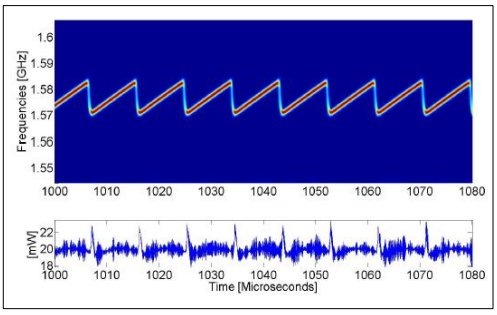
Obrázek 5: Rušička třídy IV [12]

3.2.3 Signály dostupných rušiček

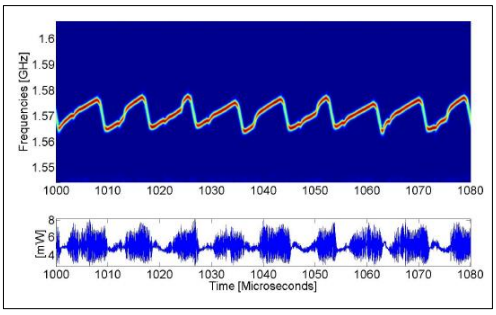
Naprostá většina komerčně dostupných GNSS rušiček je schopná generovat pouze signály neinteligentní formy rušení typu *Jamming*. Tyto rušičky zpravidla generují lineárně rozmítaný frekvenčně modulovaný signál, který je často označován pouze jako *Chirp*. Průběh změny kmitočtu v čase je u signálu tohoto typu téměř periodický a má zpravidla pilovitý průběh. Důvodem, proč jednotliví výrobci nejčastěji volí tento typ signálu, je relativní jednoduchost realizace a s tím spojené nízké výrobní náklady. Konstrukce těchto rušiček může být velice snadno realizována pomocí napětím řízeného oscilátoru VCO (*Voltage Controlled Oscillator*) [26].

Frekvenční charakteristiku *Chirp* signálu lze popsat dvěma parametry. Prvním parametrem je frekvenční rozsah rozmítání (*Sweep Range*), který je reprezentovaný maximální zápornou a maximální kladnou odchylkou od nosného kmitočtu. Druhým parametrem je perioda rozmítaní kmitočtu (*Sweep Period*), která vyjadřuje dobu, za kterou rušička přeladí od maximální záporné k maximální kladné odchylce (tedy v intervalu *Sweep Range*). Pokud je průběh přeladění z maximální záporné k maximální kladné odchylce lineární, má frekvenční charakteristika pilovitý průběh (*Chirp*).

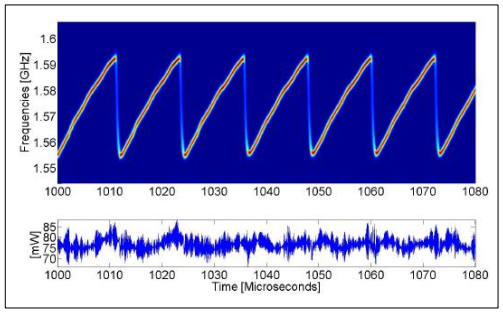
V rámci studie [4] bylo u širokého spektra komerčně dostupných rušiček prokázáno právě využití signálu typu *Chirp*, a to u všech osmnácti testovaných vzorků. Většina těchto vzorků podléhá parametrům I., II. a III. třídy. Větší část vzorků je orientována výhradně na kmitočet L1/E1. Schopností zároveň rušit kmitočet L2 je zde vybavena třetina testovaných. Schopností rušit kmitočet GPS L5 pak nebylo vybaveno žádné z testovaných zařízení. Termín „schopnost rušit“ je zde mírně zavádějící, protože se v některých případech prokázalo, že je frekvenční rozsah rušičky zcela mimo cílený kmitočet a její účinnost tak lze považovat za mizivou. Na obrázku **3.8** je tento případ zcela zřetelný. Vzorek č. 13 rozmítá signál zcela mimo cílený harmonický kmitočet L1, který je na obrázku znázorněn červenou horizontální čarou. Robustní multifunkční rušičky IV. třídy v rámci citované studie nebyly testovány.



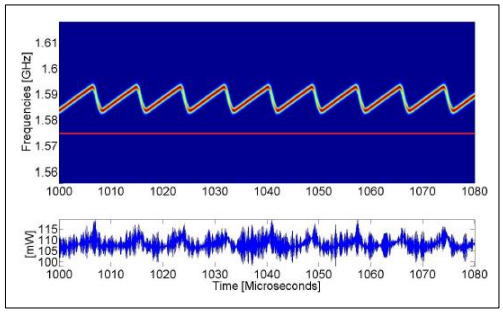
Obrázek 6: Vzorek č. 4 třídy I [4]



Obrázek 7: Vzorek č. 15 třídy II [4]



Obrázek 8: Vzorek č. 6 třídy III [4]



Obrázek 9: Vzorek č. 13 třídy III [4]

V následující tabulce jsou shrnuty výsledky měření pro osm vybraných vzorků, které byly v rámci této studie testovány. V tabulce je vždy ke konkrétní rušičce uvedena její konstrukční

třída, frekvenční rozsah rozmítání, perioda rozmítání a také hodnota vysílacího výkonu. Šířka filtru přijímače byla v rámci měření vysílacího výkonu nastavena na 50 *MHz*. Výsledky byly pro lepší souvislost s touto prací upraveny a zaokrouhleny.

Třída rušičky dle konstrukce	**Číslo vzorku dle citované studie**	**Rozsah rozmítání**	**Perioda rozmítání**	**Výkon v pásmu filtru přijímače**
Třída I	1	-25 až +31 *MHz*	26 *μs*	22 *mW*
Třída I	4	-4 až +10 *MHz*	9 *μs*	23 *mW*
Třída II	15	-13 až +4 *MHz*	9 *μs*	5 *mW*
Třída II	18	-8 až + 11 *MHz*	9 *μs*	5 *mW*
Třída III	5	-7 až +12 *MHz*	9 *μs*	58 *mW*
Třída III	6	-21 až +20 *MHz*	12 *μs*	77 *mW*
Třída III	8	-9 až +7 *MHz*	9 *μs*	334 *mW*
Třída III	13	+5 až +19 *MHz*	9 *μs*	107 *mW*

Tabulka 3.1: Vybrané vzorky rušiček a jejich parametry [4]

> *Nosný kmitočet GPS signálu L1 je modulován pseudonáhodnou posloupností PRN kódu, který ve frekvenčním spektru rozprostře signál v rádu několika MHz. Každý GPS přijímač pak na tuto část spektra nahlíží přes filtry o různých šířkách propustného pásma. Společně s úrovní vysílacího výkonu naměřeném na výstupním SMA konektoru je proto třeba vždy uvést i šířku pásma, na kterou je filtr přijímače nastaven.*

Data nashromážděná v rámci studie [4] byla nezávisle potvrzena výsledky experimentálních měření provedených kolektivem GNSS laboratoře německé univerzity FAF (*University of Federal Armed Forces*) v Mnichově [26]. Stejně jako v případě studie [4] je zkoumáno několik vzorků běžně dostupných rušiček. Na rozdíl od studie [4], kde jsou veškerá měření provedena v laboratorních podmínkách, měl tým univerzity FAF možnost provést svá měření pod širým nebem zkušebního polygonu GATE (*Galileo Test and Development Environment*). Experimentální měření provedená v rámci studie [26] potvrzují využití signálu typu *Chirp* u všech testovaných zařízení.

3.2.4 Dosah dostupných rušiček

Uvážíme-li základní model šíření volným prostorem, tak z naměřených hodnot uvedených předchozí tabulce vyplývá, že i ty nejslabší rušičky mohou značně převyšovat původní záměr o pouze lokální eliminaci GNSS signálů. Z naměřených hodnot je totiž v rámci studie [4] usuzováno, že i ty nejslabší rušičky mohou být teoreticky schopny znemožnit sledování cíle (*Tracking*) do vzdálenosti až 300 *m*. Prvotní určení polohy (*Acquisition*) pak mohou tyto rušičky znemožnit až do vzdálenosti 1 *km*. Ty výkonnější rušičky teoreticky zvládnou znemožnit sledování cíle až do vzdálenosti 6 *km* a prvotní určení polohy znemožnit až do vzdálenosti 9 *km*. Rozdíl mezi efektivní vzdáleností rušičky pro sledování cíle a efektivní vzdáleností pro prvotní určení polohy je dán tím, že proces sledování polohy v čase je mnohem robustnější, jelikož přesně známe okamžitou polohu cíle a poloha budoucí se tak dá předpokládat v blízkém okolí. Naproti tomu je prvotní fáze provedena bez jakékoliv znalosti předešlé polohy a je tedy pochopitelně citlivější na jakékoliv rušení.

3.2.5 Zvýšení účinku rušení

Pro zvýšení rušivého účinku pak mohou být antény rušiček vůči GNSS signálům polarizačně nepřizpůsobeny [4]. Anténu rušičky tak lze realizovat např. formou zatíženého monopólu nebo elektricky krátké šroubovicové antény. Tyto typy antén vyzařují lineárně polarizované vlny. Družice systému GPS oproti tomu vysílají vlny s kruhovou polarizací. Takové polarizační nepřizpůsobení mezi rušivým a družicovým signálem se pak projeví poklesem úrovně přijímaného výkonu na GPS přijímači.

Pro zvýšení účinku rušení lze také kombinovat výstup několika generátorů rozmítaného signálu. V rámci studie [26] byly analyzovány rušičky, které disponují až čtyřmi nezávislými generátory s různými periodami rozmítání kmitočtu. Studie dále obsahuje podrobnější rozbor takových zařízení včetně matematického modelu generovaného signálu.

Dalším faktorem, kterým lze potenciálně zvýšit účinnost rušičky, je maximální možné zkrácení periody rozmítaní při současném zachování rozsahu rozmítání kmitočtu. Čím kratší je pak perioda rozmítání, tím obtížnější je pro přijímač potlačení vlivu tohoto rušivého signálu. Přijímač se však je schopen bránit. Většina dostupných GNSS přijímačů totiž disponuje adaptivní pásmovou zádrží typu *Notch Filter*, která souží k potlačení zejména kontinuálních rušivých signálů. Studie [27] ale prokazuje, že při použití vhodného adaptačního algoritmu LMS (*Least Mean Squares*) je ochrana přijímače tímto filtrem zajištěna i vůči signálům s rychlými změnami

kmitočtu typu *Chirp*. Schopnost tohoto filtru určit okamžitou frekvenci rušivého signálu však bude mít svůj limit [2]. Pokud bychom zajistili dostatečně rychlou změnu kmitočtu, mohl by se tento filtr přestat stíhat dostatečně rychle adaptovat a rušivý signál by tak prošel k dalšímu zpracování.

3.3 Rušení typu Spoofing

Hned na úvod je dobré zmínit, že zařízení, která jsou schopna generovat signály typu *Spoofing*, už na internetu tak lehko jako v předchozím případě neseženeme a pokud ano, můžou se jejich ceny pohybovat v řádech několika tisíc *USD*. Rušení typu *Spoofing* lze klasifikovat jako „řízenou“ formu rušení, kdy se útočník snaží převzít kontrolu nad tím, jaké polohové údaje jsou uživateli interpretovány.

3.3.1 Silně korelované signály

Aby nám přijímač rušivý signál „uvěřil“, musíme pochopitelně co nejvěrněji napodobit ten skutečný. Čím více se bude rušivý signál podobat tomu skutečnému, tím více bude korelovaný. V případě silně korelovaných signálů tak mluvíme v podstatě o reálně vzhlížející kopii, která je však generována specializovaným zařízením nikoliv družicí. Moderní signálové generátory jsou takové signály schopny generovat. V rámci těchto signálů jsou pak zcela věrně promítnuty reálné konstelace družic. Jako vstupní parametr je však třeba zadat přesnou polohu přijímače. Bez znalosti jeho přesné polohy se tyto signály nebudou přijímači jevit jako věrohodné. Budou totiž odpovídat jinému místu příjmu, a tedy jiné aktuální konstelaci družic, než by přijímač v dané chvíli očekával. V případě, že neznáme polohu přijímače, který chceme „zmást“, je použití rušení typu *Spoofing* takřka vyloučeno. Tento typ rušení tak není možné úspěšně realizovat na větší vzdálenosti [3]. Pro úspěšný útok založený na tomto principu by nám v tu chvíli zbýval pouze scénář, ve kterém bychom museli rušičku adaptivně přemísťovat v závislosti na pohybu cíleného přijímače, a navíc přitom minimalizovat jejich vzájemnou vzdálenost.

3.3.2 Synchronizace na rušivý signál

Základní princip rádiového určování polohy pomocí systému GNSS spočívá v určení vzdálenosti mezi družicí a přijímačem [1]. Družice vyšle dálkoměrný signál v čase t_0. Přijímač začne ve stejném okamžiku lokálně generovat jeho kopii. Přijímačem je následně provedena korelace mezi přijatým signálem a jeho lokálně generovanou kopií. Korelační špička této funkce je pak vůči autokorelační funkci lokálně generované kopie posunuta o zpoždění mezi počátkem

generovaní lokální kopie v čase t_0 a příchodem družicového signálu. Toto zpoždění udává dobu šíření signálu od družice k přijímači.

Pokud by se tedy někdy v blízkosti vyskytla „falešná“ korelační špička, tak by se přijímač teoreticky mohl synchronizovat právě na ni. Aby se však někde v blízkosti taková špička vyskytla, museli bychom družicový signál přijmout, zesílit a znovu vyslat k přijímači (viz kapitola **3.3.3** „Spoofing I. třídy“). Druhou možností pak je generování vlastního „falešného“ GPS signálu (viz kapitola **3.3.4** „Spoofing II. třídy“ a kapitola **3.3.5** „Spoofing III. třídy“).

V obou případech by přijímač registroval dva téměř totožné signály (družicový a rušivý). Ty by však byly vzájemně časově posunuté. Přijímač by pak po provedení korelace přijímaných signálů s lokálně generovanou kopií viděl dvě korelační špičky. Vhodným přizpůsobením výkonu bychom zajistili, že „rušivá“ korelační špička bude tou silnější. Tím bychom teoreticky vytvořili podmínky k tomu, aby se na ni přijímač synchronizoval.

Otázkou je, jak přijímač donutit, aby se na rušivý signál opravdu synchronizoval. To znamená, aby nám v podstatě „uvěřil“, že se jedná o skutečný družicový signál a přeladil se na něj. V tomto případě se však nejedná o „přeladění“ ve smyslu změny kmitočtu (rušivý signál se samozřejmě nachází na stejném kmitočtu), ale o přeladění na korelační špičku rušivého signálu, která má vůči lokálně generované kopii odlišné zpoždění než signál skutečný. Častěji se proto setkáme s termínem „synchronizace na rušivý signál“. Aby k oné synchronizaci došlo, musí se nám podařit vygenerovat rušivý signál dostatečně korelovaný se signálem skutečným. Pokud se nám takový signál podaří vygenerovat, může pak pro vynucení synchronizace teoreticky stačit pouze zvýšit jeho výkon nad úroveň skutečného družicového signálu.

Vedlejším cílem takového útoku je pak to, aby přijímač neměl šanci nijak rozpoznat, zda je synchronizován na skutečný družicový signál nebo na signál rušivý, který mu byl vnucen útočníkem. V případě úspěšné synchronizace může být zcela nepozorovaně ovlivňována interpretace polohy, rychlosti a systémového času přijímače. Toho může být dosaženo např. zavedením fiktivních údajů o polohách družic přímo do navigační zprávy nebo mírnou deformací hodinového signálu. Za *Spoofing* lze považovat i kybernetické útoky, jejichž cílem může být např. falsifikace mapového podkladu přijímače [3]. Útoky tohoto charakteru je tak pochopitelně velice komplikované detekovat natož pak spolehlivě eliminovat.

3.3.3 Spoofing I. třídy

Za nejjednodušší zařízení schopné generovat rušivý signál typu *Spoofing* lze považovat opakovač GNSS signálu (angl. *Repeater*) [5]. Taková zařízení slouží primárně k redistribuci GNSS signálů např. uvnitř budov. GNSS signály jsou na střeše dané budovy přijaty kvalitní hemisférickou anténou, dále zesíleny a v místě potřeby pak redistribuovány. Takové zařízení je pak v daném prostředí schopné plně suplovat funkci družic a lze jej tak snadno zneužít jako jednoduchý *Spoofer*. Pokud budeme GNSS signál tímto zařízením redistribuovat ve venkovním prostředí, tak jej přijímače nacházející se v jeho blízkosti mohou mylně považovat za „družicový" zdroj navigačního signálu a za určitých podmínek se na něj synchronizovat. Pro vynucení synchronizace na signál opakovače by pak teoreticky mohlo postačovat pouze nastavení vyšší výkonové úrovně tohoto signálu oproti signálům družicovým. V případě, že dojde k synchronizaci na signál opakovače, přijímač bude namísto své polohy chybně interpretovat právě polohu opakovače. Neočekávaný fázový skok mezi skutečným a rušivým signálem však bude pravděpodobně vyhodnocen jako krajně podezřelý. Relativně vysoký výkon opakovače se navíc projeví nestandardní odezvou zpětnovazební smyčky AGC (viz kapitola **4.2.1** „Vyhodnocení odezvy AGC"). Útok tohoto typu by tak měl být poměrně snadno odhalen.

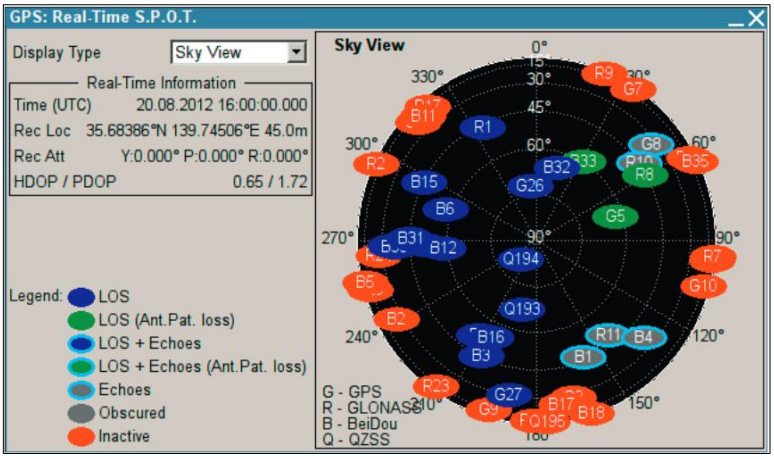
Pro další informace o dostupných zařízeních tohoto typu doporučujeme navštívit stránky finského výrobce Roger [19], který se dlouhodobě zabývá výrobou a distribucí těchto zařízení nebo americké společnosti GPS Source [20], která svými produkty splňuje přísné vojenské standardy MIL-STD a je přímým dodavatelem Americké armády. Na internetu jsou rovněž k dostání čínské výrobky, jejichž cena se pohybuje okolo 150 *USD*. O kvalitě redistribuce družicových signálů by se v jejich případě dalo pochybovat, ale pro experimentální účely simulace útoku typu *Spoofing* by se mohlo jednat o ideální cenově dostupnou alternativu.

3.3.4 Spoofing II. třídy

Druhou třídou zařízení schopných generovat rušivý signál typu *Spoofing* jsou speciální signálové generátory, které jsou softwarově uzpůsobeny k simulaci GNSS signálů [5]. Vstupním parametrem těchto simulátorů je poloha přijímače a aktuální čas. Simulátor je tak schopen vygenerovat signál, který v čase odpovídá reálné konstelaci družic. Navíc jsme v případě takového zařízení schopni adaptivně regulovat úroveň vysílaného signálu tak, aby co nejvíce odpovídala reálným podmínkám. To však nezabrání skokovým změnám odezvy obvodu AGC během synchronizace přijímače na generovaný signál (viz kapitola **4.2.1** „Vyhodnocení odezvy

AGC“). Stejně jako v předchozím případě dochází k podezřelým změnám vyhodnocené polohy a systémového času. Analýzou příslušných proměnných jsme tak schopni takový útok odhalit.

Příkladem takového zařízení může být vektorový signálový generátor Rohde&Schwarz SMBV100A se zabudovaným modulem pro simulaci GNSS signálů [15]. Na následujícím obrázku vidíme konkrétní konstelaci družic vztaženou k určité poloze přijímače v přesně definovaný čas. Zařízení tohoto typu jsou však velice drahá. Mnohem levnější variantou může být konfigurace navržená ve studii [18]. Navržená konfigurace kombinuje speciální GNSS toolbox simulačního prostředí Matlab, vlastnosti softwarově definovaného rádia a externí zdroj hodinového signálu [18].



Obrázek 10: Signálový generátor s GNSS modulem [15]

3.3.5 Spoofing III. třídy

Nejpokročilejší forma rušení typu *Spoofing* je zprostředkována zařízením, které se v reálném čase dokáže automaticky přizpůsobovat vnějším podmínkám a zároveň předcházet podezřelému chování přijímače [5]. Takové zařízení je angl. literatuře označováno jako tzv. „*Spoofer*“. V první fázi toto zařízení analyzuje přijímaný družicový signál. Poté obdobně jako v předchozím případě začne generovat „falešný“ GNSS signál vztažený k aktuálnímu času a poloze s tím rozdílem, že jej v reálném čase upravuje tak, aby se zcela shodoval s tím družicovým. Ve chvíli, kdy je tohoto stavu dosaženo, začne *Spoofer* citlivě zvyšovat výkon rušivého signálu až do chvíle, kdy dojde k synchronizaci přijímače na onen rušivý signál. Tímto „citlivým“ přechodem na paralelně generovaný rušivý signál jsou teoreticky eliminovány snadno odhalitelné změny vybraných parametrů, na kterých mohou selhávat principy I. a II. třídy. Jakmile je přijímač na rušivý signál synchronizován, může *Spoofer* v určitých mezích měnit parametry generovaného signálu a zkreslovat tak údaj o poloze a systémovém čase, který je přijímačem interpretován.

Budou-li tyto změny prováděny s dostatečnou jemností, šance na úspěšnou detekci rušivého signálu se oproti předchozím případům I. a II. třídy výrazně snižují.

3.3.6 Scénář útoku

Konkrétní scénář útoku typu *Spoofing* by mohl být proveden následujícím způsobem. Jako potenciální cíl můžeme uvažovat letištní multilaterační systém MLAT od pardubické společnosti ERA a.s., jehož zranitelnost dala za vznik této práci. Přijímací uzly tohoto systému vyžadují velice přesnou synchronizaci a jsou tak přímo závislé na dostupnosti hodinového signálu GNSS systémů. Systém pravděpodobně disponuje záložním zdrojem hodinového signálu v podobě CSAC (*Chip Scale Atomic Clock*), ale v případě úspěšné realizace útoku typu Spoofing nemusí dojít k jeho aktivaci. Pokud by se nám podařilo vnutit systému námi generovaný rušivý signál, mohli bychom velice jemným laděním nosného kmitočtu dosáhnout znehodnocení časové reference jednoho přijímacího uzlu systému. Takové ladění by tak mohlo trvat i několik desítek minut. Zároveň by muselo být navázáno na velice přesný kmitočtový normál. Rušivý signál bychom v rámci takového útoku distribuovali přímo vůči stanici systému MLAT např. pomocí směrové antény typu YAGI.

Obrázek 11: ERA a.s. MLAT na letišti v Baku [17]

3.3.7 Potenciální zneužití

Spoofing zatím nebyl v četnější míře nikde zaznamenán ani řádně zdokumentován. V posledních letech se objevují pouze ojedinělé případy, u kterých navíc není zcela prokázáno, kdo za nimi stojí a jakými konkrétními prostředky se mu je podařilo realizovat. Asi nejznámějším případem je incident z roku 2011, kdy došlo k pádu amerického dronu RQ-170 Sentinel poblíž

města Kashmar v severovýchodním Iránu. Letoun byl Iránskou stranou zajat, a to v údajně téměř neporušeném stavu. Původní domněnka o sestřelení letounu byla americkými armádními představiteli vyvrácena a rychle se tak začaly objevovat spekulace o možném kybernetickém útoku ze strany Iránu. Íránské ministerstvo obrany v souvislosti s touto událostí vzápětí vydalo oficiální prohlášení, ve kterém se mluví o blíže nespecifikované formě kybernetického útoku, jejímž prostřednictvím byl letoun donucen přistát [15]. Tento scénář americká strana pochopitelně popřela a pád stroje přičetla problémům mechanického charakteru. Co kdyby se však Iránu opravdu podařilo zapříčinit ať už pád nebo dokonce přistání tohoto letounu bez jediného výstřelu? Primárním navigačním systémem těchto letounů jsou prvky inerciální navigace IMU (*Inertial Measurement Unit*), ty ale mohly být právě z důvodu mechanické závady vyřazeny z provozu. V takové situaci se stává primárním zdrojem navigačních dat signál družic systému GPS. V tu chvíli se tak letoun stává extrémně zranitelným. V případě úspěšné realizace útoku nemají řídící systémy letounu důvod k jakémukoliv podezření, a i kdyby měly, další záložní řešení již nemusí být k dispozici. Jen připomeňme, že úspěšná realizace takového útoku je podmíněna znalostí přesné polohy letounu. Ta mohla být v tomto případě snadno dodána radarovými systémy protivníka. Každopádně to, zda se skutečně jednalo o Iránem vedený kybernetický útok, nebo šlo pouze o mechanickou závadu letounu, se už pravděpodobně nikdy nedozvíme.

Obrázek 12: RQ-170 na palubě USS George H.W. Bush [14]

Další potencionální zneužití tentokrát ze zcela odlišného prostředí lze očekávat v oblasti rybolovu, a to zejména za účelem dosažení vyšších zisků [5]. V některých oblastech je totiž z nejrůznějších důvodů rybolov dočasně nebo zcela zakázán a rybářské lodě jsou příslušnými orgány monitorovány, zda tento zákaz dodržují. Motivace pro zneužití signálů typu *Spoofing* je tak za účelem zvýšení profitu poměrně vysoká.

3.4 Rušení typu Semi-spoofing

Stejně jako v předchozím případě je primárním cílem takového útoku, aby se přijímač synchronizoval na rušivý signál. V případě rušení typu *Spoofing* jsme se snažili, aby byl stav synchronizace zachován po co možná nejdelší dobu a my tak mohli prostřednictvím rušivého signálu zcela nepozorovaně ovlivňovat funkci přijímače. Princip rušení typu *Semi-spoofing* je však odlišný. K ovlivnění funkce přijímače přistupuje jiným a mnohem jednodušším způsobem. Tentokrát se nesnažíme generovat přesnou kopii družicového signálu, které by přijímač bez jakéhokoliv podezření důvěřoval. Snažíme se přijímač pouze na krátkou dobu „zmást“ rušivým signálem a způsobit tak výpadek skutečného družicového signálu.

Rušení typu *Semi-spoofing* je charakterizováno obdobnou signálovou strukturou jako skutečné družicové signály. Tato podobnost je však omezena a poměrně snadno tak může dojít k odhalení (viz kapitola **4.2** „Metody detekce rušivých signálů“). Celkově tedy úspěšná synchronizace na rušivý signál (resp. jakési dočasné „zmatení“ přijímače) vede pouze ke krátkodobému výpadku družicového signálu. V případě nastolení určitého řádu v načasování a intenzitě takových útoků, jsme teoreticky schopni docílit dlouhodobého výpadku družicového signálu (viz kapitola **3.4.2** „Synchronizace přijímače na rušivý signál“).

3.4.1 Slabě korelované signály

Čím více se rušivý signál podobá tomu skutečnému, tím více je s ním korelovaný. V případě rušení typu *Spoofing* jsme mluvili o silně korelovaných signálech, které jsou s družicovým signálem v podstatě shodné, a korelační špička vzniklá jejich vzájemnou korelací je tak téměř maximální. Úplným opakem takového signálu je termický šum Země. Ten má v čase zcela náhodný charakter, díky čemuž je s družicovým signálem korelován pouze velice slabě. To si lze vysvětlit tím, že družicový signál je ve spektru rozprostřen pomocí pseudonáhodné posloupnosti a v časové doméně tak má zdánlivě náhodný charakter. Vzhledem k náhodné povaze obou signálů (termického šumu a družicového signálu) lze v jejich průběhu pozorovat určité shody a v případě jejich vzájemné korelace tak vzniká nezanedbatelná korelační špička.

Signály, které jsou téměř identické (družicový signál a signál typu *Spoofing*) tedy považujeme za silně korelované. Signály, které jsou si jen vzdáleně podobné (družicový signál a termický šum Země), považujeme za slabě korelované. Rušení typu *Semi-spoofing* můžeme zařadit spíše k signálům slabě korelovaným. Tento rušivý signál totiž není generován s odkazem na aktuální polohu přijímače tak, jak tomu je u signálů silně korelovaných. Ani neobsahuje

kompletní navigační zprávu. Korelace s družicovým signálem je zde zajištěna pouze napodobením struktury dálkoměrného signálu reprezentované především C/A kódem (viz kapitola **6.5.1** „Generování C/A kódu“). Jeho součástí také mohou být smyšlené informace o polohách družic či jiné prvky navigační zprávy.

3.4.2 Synchronizace na rušivý signál

Zvýšením výkonu rušivého signálu nad úroveň skutečného družicového signálu vytvoříme podmínky pro synchronizaci přijímače na rušivý signál. Pravděpodobnost, že k tomu skutečně dojde, v tu chvíli není příliš vysoká. Pokud je totiž přijímač již synchronizován (na družicový signál), tak nemá potřebu „přelaďovat“ na jinou, ač silnější korelační špičku. Nabízí se tři řešení, která by pravděpodobnost úspěšné synchronizace mohla teoreticky zvýšit.

3.4.3 Semi-spoofing I. třídy

Prvním řešením by tak mohlo být generování rušivého signálu, jež by svou strukturou zapříčinil výskyt většího počtu korelačních špiček. Takový signál by např. mohla představovat sumace slabě korelovaných a vzájemně fázově posunutých signálů. Takto modulovaný rušivý signál by pak na výstupu korelační fáze mohl způsobit vznik slabých korelačních špiček, které bychom vhodným přizpůsobením výkonu zesílili nad úroveň družicového signálu. Takovéto zvýšení koncentrace korelačních špiček by teoreticky mohlo zvýšit pravděpodobnost, že se přijímač synchronizuje na námi vnucený signál.

3.4.4 Semi-spoofing II. třídy

Dalším způsobem, kterým bychom teoreticky mohli zvýšit pravděpodobnost úspěšné synchronizace, je rozdělení vysílacího intervalu na několik stejně dlouhých částí. Řekněme, že jich bude celkem deset. V první desetině celkového intervalu budeme vysílat slabě korelovaný rušivý signál, který jsme vlastním úsilím vygenerovali. V druhé desetině budeme vysílat totožný signál, ale posunutý o polovinu kódového čipu. Ve třetí desetině budeme opět vysílat stejný signál, ale posunutý o celý jeden čip. Takto budeme pokračovat, až vyplníme celý interval. Tato signálová struktura by teoreticky mohla vytvořit podmínky ke vzniku deseti korelačních špiček, na které by se mohl přijímač potenciálně synchronizovat.

3.4.5 Semi-spoofing III. třídy

Další formu útoku typu *Semi-spoofing* by mohl představovat signál, prostřednictvím kterého bychom postupně vyřadili signály jednotlivých družic. V tomto případě se pro názornější popis principu zaměříme konkrétně na systém GPS. Tento systém je tvořen konfigurací 32 družic. Každá družice má svůj unikátní pseudonáhodný kód (C/A kód), kterým se v rámci systému jednoznačně identifikuje.

Řekněme, že obdobně jako v předchozím případě rozdělíme časový interval vysílání rušivého signálu, tentokrát však na 32 částí. V první části bychom vysílali signál korelovaný s první družicí, ve druhé části signál korelovaný s druhou družicí, ve třetí části se třetí družící a tak dále. Tak bychom celý interval rušivého signálu koncentrovali korelačními špičkami, vztaženými k signálům jednotlivých družic. Jelikož by se jednalo pouze o slabě korelované signály (v tomto případě právě prostřednictvím C/A kódu), výpadek signálu dané družice by byl pouze krátkodobý. Přijímači každopádně nějakou dobu trvá, než se opět synchronizuje na skutečný družicový signál a celkový efekt rušení by tak mohl vykazovat dlouhodobější charakter. Rušivý signál tohoto typu je vygenerován v rámci kapitoly **6.5.3** „Inteligentní signál II“ (viz **PŘÍLOHA 12**).

4 DETEKCE RUŠENÍ

DETEKCE RUŠENÍ TYPU JAMMING

V ideálních podmínkách má termický šum Země přibližně o 10 *dB* vyšší výkonovou úroveň než družicový signál GNSS systémů. Družicové signály jsou tak ve spektru rozprostřeny pod úrovní termického šumu. Zisk zpracování signálů s rozprostřeným spektrem nám však s takovými signály umožní pracovat. Vzhledem k této skutečnosti můžeme jako rušení klasifikovat jakýkoliv signál, který se právě nad touto úrovní objeví. V případě rušivých signálů typu *Jamming* je tedy jejich detekce poměrně jednoduchá. Povaha takového rušení je charakterizována především vysokým výkonem. V GNSS pásmu se tak objeví nad šumovým prahem rušivý signál. Určíme-li práh vymezující důvěryhodnou úroveň odstupu signálu od šumu, budou hodnoty vystupující nad tímto prahem vyhodnoceny jako indikátor rušení typu *Jamming*.

DETEKCE RUŠENÍ TYPU SPOOFING

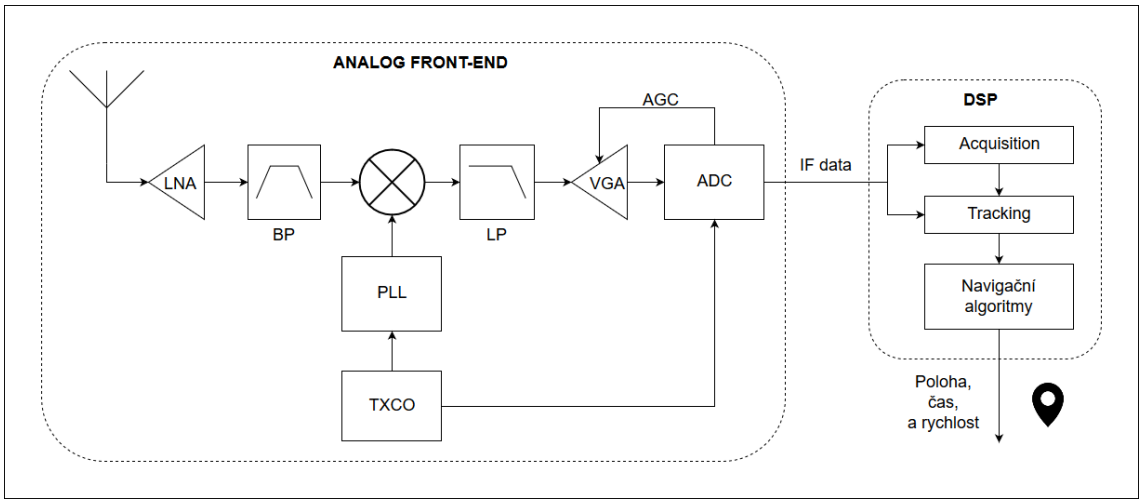
Přijímače jsou vůči téměř jakékoliv formě útoku typu *Spoofing* extrémně zranitelné. Obecně je hlavním problémem přijímačů jejich přílišná důvěra v cokoliv, co se GNSS signálům alespoň do jisté míry podobá [3]. Přijímač pak může v těchto rušivých signálech hledat navigační řešení, aniž by řádně vyšetřil jejich konzistenci a důvěryhodnost.

Většina přijímačů není schopna takovou formu útoku samostatně rozpoznat, ač k tomu má určité předpoklady, a to jak v pre-korelační tak post-korelační fázi procesu určování polohy [3]. V pre-korelační fázi je úroveň přijímaného signálu upravována automatickým řízením zisku AGC, protože v čase kolísá. Objeví-li se na vstupu přijímače rušivý signál s několikanásobně vyšší výkonovou úrovní, než byla ta dosavadní, dojde k výraznému poklesu zisku AGC a pokus o narušení systému zcela evidentní. Během post-korelační fáze je prostor pro odhalení narušitele především při vyhodnocování okamžitých změn pseudo-vzdáleností a Dopplerovských kmitočtů. Skoková změna těchto parametrů je přinejmenším podezřelá a může rovněž indikovat pokus o narušení systému.

4.1 Zpracování přijatých signálů

Pro pochopení základních principů detekce rušivých signálů je nejprve třeba uvést proces, kterým přijatý signál (družicový i rušivý) v rámci přijímače prochází. GNSS signál je nejprve zachycen přijímací anténou, od které dále putuje analogovou částí přijímače (v angl.

Front-end). Tam je nejprve zesílen, dále filtrován, konvertován do základního pásma, a v poslední řadě digitalizován. Úlohou této části je příprava přijatého signálu k digitálnímu zpracování, které probíhá v rámci DSP (*Digital Signal Processor*).



Obrázek 13: Typická struktura GNSS přijímače [5]

FILTRACE A ZESÍLENÍ

Vzhledem k velice slabé úrovni GNSS signálů dostupných na povrchu Země jsou bezprostředně za přijímací anténu zařazeny zesilovací a filtrační prvky. Zpravidla se jedná o nízko-šumový zesilovač LNA (*Low Noise Amplifier*) a filtr typu pásmová propust BP (*Band Pass*). Konfigurace těchto prvků se v rámci různých přijímačů může lišit, ale princip je zachován vždy stejný. Úkolem těchto prvků je zesílení signálu, udržení nízkého šumového čísla a filtrace signálů nacházejících se mimo žádoucí GNSS pásmo [7].

KONVERZE DO ZÁKLADNÍHO PÁSMA

Po zesílení a filtraci přijímaného RF signálu přichází na řadu jeho konverze do základního pásma BB (*Base Band*). Ta může být provedena buď přímo nebo s mezi-převodem na mezifrekvenční kmitočet IF (*Intermediate Frequency*). Opět závisí na konfiguraci daného přijímače. Vlastní konverze je provedena směšováním přijímaného signálu a signálu místního oscilíátoru TCXO (*Temperature Compensated Crystal Oscillator*). Produktem směšování pak je součtová a rozdílová složka, z nichž je pro další zpracování zpravidla využívána složka rozdílová. Součtová složka je odfiltrována dolní propustí LP (*Low Pass*) řazenou na výstupu směšovače. Kritickou komponentou směšování je lokální oscilátor, který musí být zvolen tak, aby neprodukoval nežádoucí harmonické kmitočty v blízkosti IF.

KVANTOVÁNÍ A VZORKOVÁNÍ

V rámci ADC (*Analog-Digital Converter*) je proveden kvantizační proces, jehož výstupem jsou diskrétní vzorky digitálního signálu. Většina GNSS přijímačů využívá uniformní kvantizační metody, které se vyznačují jednotnými kvantizačními kroky a jsou tak často označovány pojmem „lineární kvantování“. Existují také adaptivní kvantizační metody, které kvantizační úrovně upravují v závislosti na histogramu výstupního signálu [7]. Při kvantizačním procesu dochází v ADC k určitým kvantizačním ztrátám. Tyto ztráty závisí na poměru k_{opt} mezi maximálním kvantizačním prahem L a směrodatnou odchylkou přijatého signálu σ [7].

$$k_{opt} = \frac{L}{\sigma} \tag{4.1}$$

Zpětnovazební smyčka AGC (*Automatic Gain Control*) je fyzicky realizována zesilovačem s variabilním ziskem VGA (*Variable Gain Amplifier*). Zesilovač s variabilním ziskem VGA prostřednictvím zpětnovazební smyčky AGC adaptivně přizpůsobuje úroveň signálu tak, aby tento poměr optimalizoval a minimalizoval tak kvantizační ztráty [5].

4.2 Metody detekce rušivých signálů

Důvěryhodnost přijímaných signálů lze prověřovat několika nezávislými způsoby [3]. Většina těchto metod je založena na softwarovém přístupu testování specifických vlastností přijímaného signálu. V následujících kapitolách jsou tyto metody podrobně popsány.

4.2.1 Vyhodnocení odezvy AGC

Obvod zpětnovazební smyčky AGC má klíčový potenciál k plnění funkce primárního detektoru rušivých signálů. Obvodem AGC totiž disponuje většina dostupných GNSS přijímačů a tato metoda detekce je tak snadno implementovatelná napříč širokým spektrem uživatelů.

Primárním podezřelým faktorem indikujícím možné rušení může být náhlý pokles zisku přijímače. GNSS signály jsou legislativně chráněny dedikovanými pásmy 1164-1215 *MHz* a 1559-1610 *MHz* určenými striktně pro účely radionavigace [6]. Pásmo přijímače by tak v ideálním případě mělo být zcela bez přítomnosti jakéhokoliv rušivého signálu. Vzhledem k tomuto předpokladu a také skutečnosti, že se přijímané GNSS signály nachází pod šumovým prahem, by v ideálním případě měl zisk AGC záviset pouze na úrovni termického šumu Země. Termický šum Země je stálý a s minimálními fluktuacemi, tj. můžeme tvrdit, že právě on se ziskem AGC v podstatě „nehýbe“. To, co odezvu AGC skutečně ovlivňuje, je především adaptace na různé

hodnoty zisku aktivní přijímací antény. V přítomnosti rušení tak zisk AGC skokově klesne v reakci na zvýšenou výkonovou úroveň v GNSS pásmu [5]. Náhlým poklesem zisku AGC tak lze poměrně snadno indikovat potencionální rušení [34]. Tento pokles zisku AGC totiž přichází dávno před tím, než se přijímač stačí na rušivý signál synchronizovat. To nám dává prostor k nastavení vhodných příznaků, které by v dostatečném předstihu mohly poskytnout varování o potencionálním narušení integrity přijímaných GNSS signálů.

4.2.2 Kontrola integrity RAIM

Dalším možným stupněm ochrany je systém RAIM (*Receiver Autonomous Integrity Monitoring*), jehož úkolem je verifikace integrity přijímaných GNSS signálů. Systém dokáže uživatele včas varovat, kdy by na základě podezřelých okolností neměl svůj přijímač vůbec používat. Existuje několik detekčních schémat, které mohou být tímto systémem používány [23]. RAIM např. může srovnávat dostupné signály jednotlivých GNSS systémů a indikovat případné neshody, které se mohou projevit neočekávanými stavy hodinových signálů [3]. V rámci jiného detekčního schématu systém RAIM dokáže zohlednit i údaje získané alternativními prostředky určování polohy. Alternativním zdrojem polohových údajů může být např. systém hyperbolické navigace eLoran (*Enhanced Long Range Navigation*) nebo prvky inerciální navigace IMU (*Inertial Measurement Unit*) [3]. Výsledkům těchto srovnání lze přiřknout nejvyšší váha, protože existuje pouze malá pravděpodobnost, že by se potenciálnímu útočníkovy podařilo falsifikovat nebo úplně znehodnotit údaje všech uvedených systémů současně. Podrobný popis detekčních schémat a postupů, které mohou být systémem RAIM aplikovány, lze dohledat v publikaci [23] na straně 143-165. Na závěr je potřeba sdělit, že dle [24] jsou metody RAIM dostatečně účinné zejména proti méně sofistikovaným útokům typu *Semi-Spoofing*. S pokročilejšími formami rušení typu *Spoofing* si již metody RAIM nemusí umět poradit.

4.2.3 Vzájemná korelace dvou přijímačů DRCC

Metoda vzájemné korelace dvou přijímačů DRCC (*Dual-Receiver Cross-correlation*) spočívá ve vzájemné korelaci šifrovaných GPS signálů, která je provedena v rámci dvou nezávislých přijímačů. Tato metoda slouží k detekci sofistikovaných útoků typu *Spoofing*, jež jsou vedeny především na veřejně dostupné GPS signály [21]. Šifrovaný vojenský P(Y) kód tak může sloužit jako ochrana civilního C/A kódu. Podstatou této metody je využití referenčního přijímače, který se nachází na zabezpečené lokaci, která je od zdroje rušení buď dostatečně vzdálena nebo adekvátně stíněna. Nevýhodou tohoto systému je, že vyžaduje dedikovaný komunikační kanál mezi referenčním a chráněným/napadeným přijímačem. Pro samotné odhalení útoku typu

Spoofing využívá tato metoda známých „*Carrier-phase*“ a „*Code-phase*“ vztahů mezi civilním a vojenským kódem [21]. Část signálu, která je přijata zabezpečeným přijímačem, a o které je zřejmé, že obsahuje vojenský kód v tom správném „vztahu“ s kódem civilním, je korelována se stejnou částí signálu, která však byla přijata napadeným přijímačem. Pokud je vzájemná korelace těchto dvou částí signálu získaných rozdílnými přijímači dostatečně velká, je přítomnost rušení vyhodnocena jako negativní. V opačném případě jsou v rámci napadeného přijímače aktivovány příslušné alarmy. Matematický popis této metody je uveden v americkém patentu [22], který je zároveň prvním odborným textem, jež se aplikaci této metody blíže věnuje.

4.2.4 Ověření navigační zprávy NMA

Tento přístup využívá kryptografické metody ověření navigační zprávy NMA (*Navigation Message Authentication*). Tato metoda spočívá ve využití speciálních bezpečnostních kódů SSSC (*Spread Spectrum Security Codes*), které jsou na na družicový signál modulovány po dobu 10 *ms* v rámci každé sekundy vysílání [24]. Použitý kód je přijímači dobře známý. Provedením korelace s přijímaným signálem se tak vyskytne korelační špička, která potvrdí autenticitu přijatého signálu. Tato metoda by tak vyžadovala změnu struktury navigační zprávy, což by vyžadovalo poměrně významný zásah do infrastruktury systému GPS. Konkrétní autentizační NMA schémata jsou uvedena ve studii [21] včetně jejich matematického popisu a zhodnocení celkového přínosu.

4.2.5 Více prvková anténní konfigurace

Poměrně robustním řešením pro detekci rušivého signálu je přijímač disponující více prvkovou anténní řadou, díky které lze získat informaci o směru příchodu navigačního signálu. Princip této metody je založen na faktu, že v případě aktivního rušení přichází „falešný“ dálkoměrný signál pouze z jednoho směru a napadení systému je tak zcela evidentní [25]. V případě, že se nám podaří určit směr příchodu tohoto rušivého signálu, můžeme prostřednictvím směrově citlivé regulace zisku tento signál eliminovat (laicky řečeno „vyřadit z hledáčku“ přijímače) [25]. Tato metoda nevyžaduje žádnou anténní kalibraci a je tak poměrně snadno implementovatelná. V tomto případě se tak ocitáme spíše v problematice rádiového určování polohy, které je v rámci této práce věnována separátní kapitola. Konkrétní metoda využívající obdobného principu je analyzována v rámci kapitoly **5.1.2** „Směrový zaměřovač AoA“.

4.2.6 Další metody detekce

SKOKOVÉ ZMĚNY PSEUDOVZÁLENOSTÍ A DOPPLEROVSKÝCH KMITOČTŮ

V případě, že došlo k přeladění přijímače na rušivý signál a útočník nemá informaci o poloze přijímače, projeví se útok skokovou změnou pseudo-vzdáleností a Dopplerovských kmitočtů [3]. Aplikace této metody vyžaduje softwarové vyhodnocování těchto parametrů v reálném čase, které spočívá v nastavení prahové hodnoty pro jejich maximální věrohodnou odchylku za jednotku času. Rušení by pak bylo detekováno při překročení této prahové odchylky.

NESOULAD DÁLKOMĚRNÝCH MĚŘENÍ V RÁMCI ROZDÍLNÝCH KMITOČTŮ

Dalším znakem možné synchronizace přijímače na rušivý signál může být nesoulad výsledků dálkoměrných měření v rámci rozdílných GNSS kmitočtů [3]. V případě systému GPS mohou být porovnány např. výsledky získané měřením na kmitočtu L1 a L2. Vzhledem k rozdílným kmitočtům těchto signálů a jejich průchodu ionosférou budou určité rozdíly zaznamenány i bez přítomnosti rušení. V případě přítomnosti rušení na jednom z porovnávaných kmitočtů bude tento rozdíl signifikantní. Aplikace této metody by tak vyžadovala nastavení prahové hodnoty poměru mezi pseudovzdáleností změřenou v rámci kmitočtu L1 a pseudovzdáleností změřenou pomocí kmitočtu L2. Rušení by pak bylo detekováno při překročení definované prahové úrovně.

5 LOKALIZACE RUŠENÍ

V předešlých kapitolách této práce byly podrobně klasifikovány potenciální rušivé signály a možnosti jejich detekce. Nyní je tedy třeba vyšetřit, jakými způsoby jsme schopni zdroje těchto rušivých signálů lokalizovat.

CENTRALIZOVANÝ SYSTÉM

Systémy určování polohy lze rozdělit na centralizované a distribuované. Typickým příkladem distribuovaného systému je systém GPS, kdy je výpočet polohy prováděn v rámci mobilních uživatelských zařízení. V případě určování polohy zdroje rušivého signálu oproti tomu budeme vždy mluvit o centralizovaném systému, kdy je výpočet polohy prováděn v rámci jediné výpočetní entity v podobě centrálního serveru. Tento server vyhodnocuje rušivé signály přijímané jednotlivými uzly systému. Tato kapitola se věnuje především tomu, jakým způsobem tyto uzly přistupují k někdy doslova směrodatné informaci, která je v rámci rušivých signálů přenášena.

PŘESNOST URČENÍ POLOHY

V reálném prostředí se totiž může vyskytovat několik nezávislých zdrojů rušení. Na místě je tak vyslovení požadavku na přesnost určení polohy, který by definoval kruhovou odchylku od skutečné polohy zdroje rušení. Pokud by se totiž v oblasti dané kruhovou odchylkou nacházel další nespecifikovaný zdroj rušivého signálu, nemuseli bychom být schopni tyto zdroje vzájemně rozlišit a jejich poloha by mohla být snadno zaměněna. V horším případě by oba zdroje rušení mohly být vyhodnoceny za jeden samostatný. V takovém případě bychom sice měli k dispozici informaci o přítomnosti rušivého signálu, z taktického hlediska by však tato dezinformace mohla znevýhodnit autoritu, jež dále nakládá s údaji o poloze zdrojů rušivého signálu (ve smyslu dalšího postupu při eliminaci zdrojů rušení).

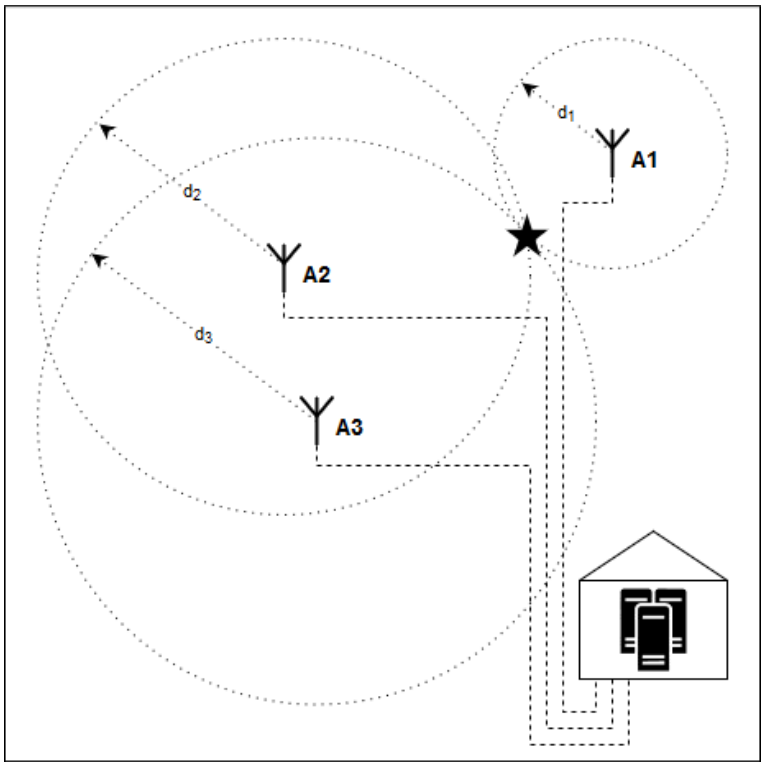
Jako dosažitelný požadavek splňující výše uvedená kritéria na přesnost určení polohy tak lze považovat kruhovou odchylku <30 *m* pro systémy založené na vyhodnocení úrovně rušivého signálu RSS (*Received Signal Strength*) a <10 *m* pro systémy založené na vyhodnocení doby šíření signálu AoA (*Angle of Arrival*) a TDoA (*Time Difference of Arrival*). Odchylka 10 resp. 30 *m* dokáže zajistit dostatečné „rozlišení“ jak pro letištní, tak jiné průmyslové aplikace.

5.1 Základní metody lokalizace

V této kapitole jsou navrženy konkrétní konfigurace lokalizačních systémů, s nimiž se můžeme setkat v rámci problematiky lokalizace zdroje rušivých signálů. První metodou popsanou v kapitole **5.1.1** je tzv. „Trilaterační zaměřovač RSS“. Tato metoda využívá zisku zpětnovazební smyčky AGC k odhadu vzdálenosti zdroje rušení. Výsledná poloha zdroje rušení je následně určena pomocí principu trilaterace. Druhou metodou popsanou v kapitole **5.1.2** je tzv. „Směrový zaměřovač RSS“. Tato metoda spočívá v určení směru příchodu rušivého signálu. Ten je určen na základě nejvyšší zaznamenané úrovně rušivého signálu v daném azimutu. Třetí metodou popsanou v kapitole **5.1.3** je tzv. „Směrový zaměřovač AoA“. Princip této metody spočívá v určení směru příchodu signálu na základě rozdílu fáze přijatého signálu. Čtvrtou metodou popsanou v kapitole **5.1.4** je tzv. „Multilaterační zaměřovač TDoA“. Ten je realizován formou tří přijímacích uzlů, které měří vzájemné rozdíly v časech příchodu rušivého signálu. Na základě zpoždění v příchodu signálu mezi jednotlivými uzly je pak určena výsledná poloha zdroje rušení.

5.1.1 Trilaterační zaměřovač RSS

Pod pojmem „trilaterace“ se skrývá složenina dvou latinských slov *tri* (tři) a *later* (délka nebo také vzdálenost). Určení polohy pomocí principu trilaterace je tedy, jak již název napovídá, realizováno na základě znalosti alespoň vzdáleností mezi zdrojem signálu a alespoň třemi různě rozmístěnými přijímači. Otázkou je, jak tyto vzdálenosti získáme. V rámci studie [34] jsou tyto vzdálenosti odhadovány na základě rozdílu mezi ziskem AGC v „klidovém“ stavu (tedy bez přítomnosti rušení) a ziskem AGC v přítomnosti rušení. Každá z takto odhadnutých vzdáleností pak určuje poloměr kružnice vyjadřující množinu bodů možného výskytu zdroje rušení. Průsečík třech takto získaných kružnic určuje výslednou polohu zdroje rušení.



Obrázek 14: Trilaterační zaměřovač RSS

5.1.2 Směrový zaměřovač RSS

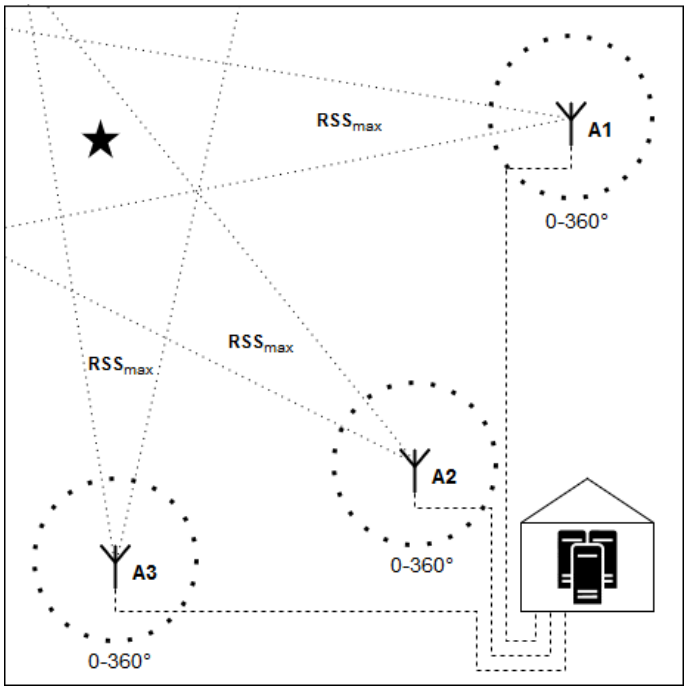
Odhad směru příchodu rádiového signálu na základě jeho nejvyšší zaznamenané RSS úrovně patří rovněž mezi ty nejjednodušší principy rádiového určování polohy. Jeho aplikace nevznáší příliš vysoké nároky na realizaci. Tato konkrétní metoda rádiového určování polohy spočívá ve vyhodnocení RSS úrovně přijímaného rušivého signálu několika směrově citlivými přijímacími uzly. Ty je možné realizovat dvěma způsoby.

Prvním způsobem je instalace sektorové antény v rámci každého uzlu. Tato sektorová anténa pokrývá azimut v rozsahu 0 až 360° dle lokálního rozložení terénu. Sektorová anténa je složena z několika anténních segmentů, přičemž každý segment pokrývá pouze vymezený rozsah azimutu. Výstup jednotlivých anténních segmentů může být sekvenčně přepínán pomocí časovacího obvodu tak, aby nedocházelo k překryvu postranních laloků jednotlivých segmentů. Datovým výstupem každého přijímacího uzlu je pak sekvence naměřených RSS hodnot, která je rozdělena na časové intervaly, přičemž každý z těchto intervalů náleží jednomu segmentu sektorové antény.

Druhým způsobem realizace je instalace rotační antény v rámci každého uzlu. Rotace antény může být zprostředkována např. krokovým motorkem. Datovým výstupem jednoho

příjímacího uzlu je pak sekvence změřených RSS hodnot, které jsou svázány s údajem o okamžité výchylce antény.

Výpočet výsledné polohy zdroje rušivého signálu je proveden v rámci centrálního serveru, který shromažďuje data ze všech uzlů konfigurace. Server z datového výstupu každého uzlu vyhodnotí směr, z kterého byly zaznamenány nejvyšší RSS hodnoty. Tím je pro každý uzel určena jakási výseč nejpravděpodobnějšího výskytu zdroje rušivých signálů. Jeho výsledná poloha je pak určena v oblasti průniku jednotlivých výsečí.



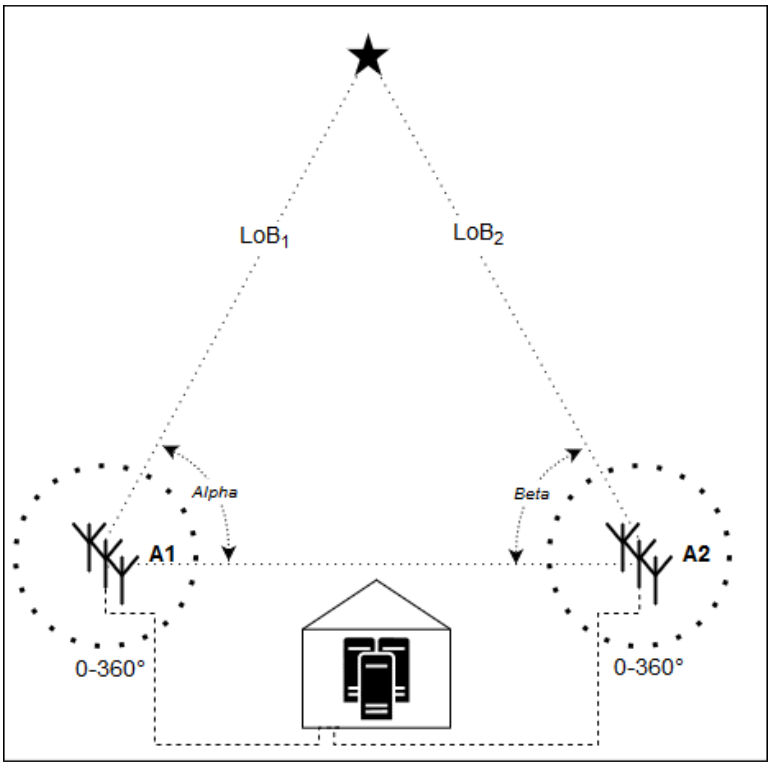
Obrázek 15: Směrový zaměřovač RSS

5.1.3 Směrový zaměřovač AoA

Metoda lokalizace založená na principu AoA (*Angle of Arrival*) je v praxi často využívanou alternativou rádiového určování polohy [28]. Jak již název napovídá, metoda spočívá v určení úhlu dopadu rušivého signálu, tentokrát však na základě rozdílů ve fázi dopadajícího signálu.

Úhel dopadajícího signálu je touto metodou určen pomocí směrově citlivých anténních řad, které jsou instalovány v rámci každého přijímacího uzlu. Na každý z prvků dané anténní řady dopadne signál v jiné fázi. Z rozdílu fáze je pak určen úhel dopadajícího signálu, který je svírán spojnicí LoB (*Line of Bearing*) a spojnici obou přijímacíh uzlů [29]. Na základě znalosti úhlů dopadu *Alpha* a *Beta*, přesné polohy obou přijímacích uzlů a jejich vzájemné vzdálenosti, jsme následně schopni určit polohu zdroje rušivého signálu [29]. Tato metoda klade poměrně vysoké nároky na výpočetní výkon, který je nutný pro kalibraci jednotlivých anténních řad [28]. Pro

splnění nároků na velký výpočetní výkon je zároveň třeba instalace relativně velkého a komplexního hardwaru [30].



Obrázek 16: Směrový zaměřovač AoA

Zásadní nevýhodou tohoto systému je, že spolehlivě funguje pouze v případě jednoho zdroje signálu. Pokud by byl aktivován vyšší počet rušiček (působících z různých míst v okolí letiště), nebylo by možné směr příchodu signálů spolehlivě určit. Dalším faktorem, jež zásadně omezuje možnost nasazení AoA systému je jeho velká citlivost na vícecestné šíření. Správná funkce systému je tak zaručena pouze v podmínkách s přímou viditelností, kterými komplexní prostředí průmyslových areálů a letišť rozhodně není.

5.1.4 Multilaterační zaměřovač TDoA

Princip TDoA (*Time Difference of Arrival*) patří mezi nejvyužívanější metody rádiového určování polohy. TDoA je využíván širokým spektrem vojenských i civilních aplikací rádiového určování polohy. Příkladem mohou být pasivní radarové aplikace nebo systémy lokalizace mobilních telefonů [31]. Asi nejznámějším je však navigační systém LORAN. Poloha mobilního zařízení vyhodnocována na základě nízkofrekvenčních signálů, které jsou nepřetržitě vysílány statickými prvky systému [32]. Naše aplikace je založena na pasivním příjmu rušivých signálu s centralizovaným výpočtem polohy mobilního zdroje rušivých signálů. Oproti navigačnímu systému LORAN se tedy architektura naší aplikace dá považovat za inverzní.

ZÁKLADNÍ PRINCIP RÁDIOVÉHO MĚŘENÍ VZDÁLENOSTI SELHÁVÁ

Předpokládáme-li, že se signál šíří rychlostí světla, vzdálenost mezi vysílačem a přijímačem je vypočtena jako součin změřené doby šíření a rychlosti světla ve vakuu. Časem příchodu signálu ToA (*Time of Arrival*) a dobou šíření signálu ToF (*Time of Flight*) označujeme základní pojmy techniky měření doby šíření rádiového signálu. Tato technika však vyžaduje velice přesnou synchronizaci vysílače a přijímače signálu. Přijímač totiž k určení doby šíření musí znát přesný čas počátku vysílání daného signálu. Touto cestou tak k měření vzdálenosti mezi zdrojem rušivých signálů a jejich přijímačem přistupovat nelze. V žádném případě totiž nedokážeme určit referenční okamžik počátku vysílání rušivého signálu a zajistit tak přesnou synchronizaci obou stran.

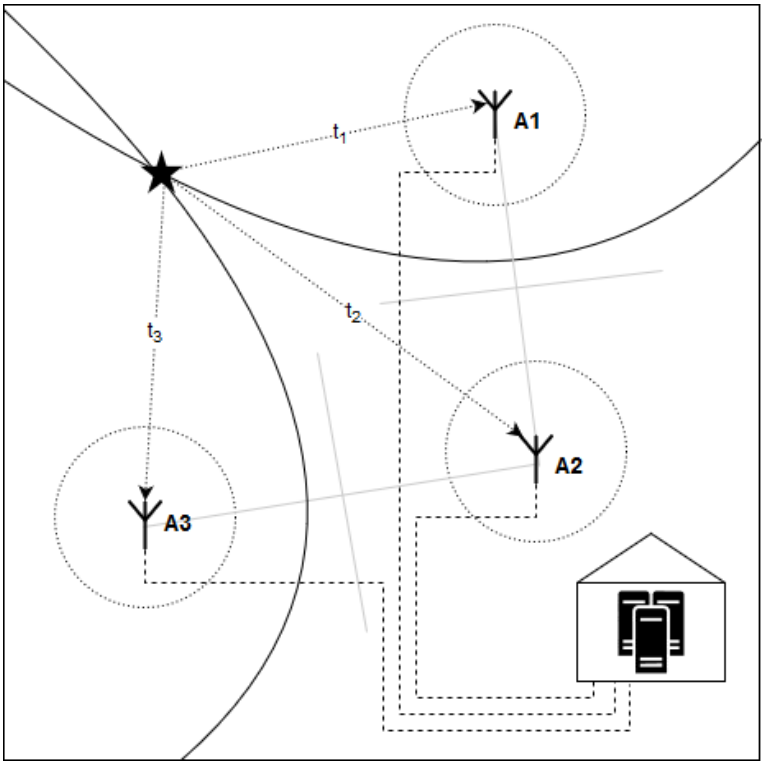
Na rozdíl od ToA nevyžaduje princip TDoA (*Time Difference of Arrival*) přesnou synchronizaci vysílače a přijímače, zato zcela závisí na vzájemné synchronizaci jednotlivých přijímacích uzlů. Realizace systému proto vyžaduje vlastní zdroj hodinového signálu. Využití časové reference družic GPS je totiž vzhledem účelu naší aplikace vyloučeno (GNSS signály jsou již rušeny nebo falsifikovány). Samotný princip TDoA spočívá v konfiguraci alespoň tří pevně umístěných přijímacích uzlů. Důvodem, proč musejí být tyto přijímací uzly přesně synchronizovány, je schopnost vyhodnotit vzájemné rozdíly v časech příchodu rušivého signálu.

Princip TDoA blíže popisuje následující obrázek. Přijímací uzly systému jsou zde označeny jako A_1, A_2 a A_3. Zdroj rušivého signálu je označen hvězdou. Rušivý signál se šíří od zdroje směrem k jednotlivým přijímacím uzlům. Rušivý signál překoná vzdálenost k nejbližšímu přijímacímu uzlu A_1 za dobu t_1, vzdálenost k uzlu A_2 překoná za dobu t_2 a vzdálenost k uzlu A_3 překoná za dobu t_3. Kdybychom časy t_1, t_2 a t_3 dokázali určit, můžeme je rovnou využít k přímé lokalizaci zdroje pomocí principu trilaterace (viz kapitola **5.1.1** „Trilaterační zaměřovač RSS“). Tyto časy však neznáme. Bez problému však můžeme určit rozdíl v čase příchodu (tedy v podstatě zpoždění) signálu vůči jednotlivým uzlům, a to díky jejich vzájemné korelaci.

HYPERBOLICKÁ LOKALIZACE

V první fázi je serverem vyhodnocen rozdíl mezi okamžikem příchodu signálu k uzlu A_1 a okamžikem příchodu signálu k uzlu A_2. Na základě tohoto rozdílu je vykreslena hyperbolická křivka H_1, která udává množinu všech možných pozic zdroje rušivého signálu. Tato hyperbolická křivka je často nazývána jako „křivka konstantního zpoždění“. To proto, že ve všech jejích bodech je rozdíl v časech příchodu signálu konstantní. Jinými slovy, pokud by byl zdroj rušivého signálu umístěn kdekoliv na této křivce, rozdíl v čase příchodu signálu vzhledem k uzlům A_1 a A_2 by byl

vždy stejný. V druhé fázi je pak serverem provedena stejná operace vzhledem k přijímacímu uzlu A_2 a A_3. Na základě rozdílu mezi časem příchodu signálu k uzlu A_2 a časem příchodu k uzlu A_3 je tedy obdobně vynesena hyperbolická křivka H_2, která taktéž udává množinu všech možných pozic zdroje rušivého signálu. Ve dvourozměrném prostoru je pak výsledná poloha zdroje rušivého signálu určena průsečíkem hyperbolických křivek H_1 a H_2.



Obrázek 17: Multilaterační zaměřovač TDoA

Do této chvíle jsme se pro snazší ilustraci zabývali dvourozměrnou situací, kdy je výsledná poloha zdroje rušivého signálu určena průsečíkem hyperbolických křivek. V trojrozměrném prostředí by nám však pouhé dva hyperboloidy k určení polohy zdroje rušení nestačily. Průnikem ploch dvou hyperboloidů totiž vznikne pouze další hyperbolická křivka nesoucí množinu možných poloh, a nikoliv jednoznačný bod v prostoru. My tak potřebujeme ještě třetí hyperboloid, který průnikem touto křivkou určí jednoznačnou polohu zdroje signálu. Výsledná poloha je tak dána průnikem tří hyperboloidů. Pokud tedy chceme získat trojrozměrnou informaci o poloze zdroje rušení, je nutné do konfigurace zařadit ještě čtvrtý přijímací uzel, který nám dodá kýžený třetí hyperboloid [33].

Jak již bylo zmíněno v úvodu, systém založený na principu TDoA vyžaduje přesnou synchronizaci jednotlivých přijímacích uzlů. V případě splnění této podmínky systém přináší požadovanou přesnost v řádu jednotek metrů. Nároky na synchronizaci takového systému však vyžadují alternativní zdroj hodinového signálu, protože využití časové reference družic GPS je

v naší aplikaci naprosto vyloučeno. Požadavek na velice přesnou synchronizaci přijímacích uzlů tak lze požadovat za největší technickou výzvu případné realizace systému.

Oproti systémům uvedeným v předchozích kapitolách vyniká princip TDoA zejména v odolnosti vůči vícecestnému šíření [30]. V korelační fázi principu TDoA totiž dokážeme spolehlivě určit signál, který k danému přijímacímu uzlu přišel tou nejkratší cestou (v ideálním případě cestou přímé viditelnosti). Tento signál pak nejlépe vypovídá o skutečné vzdálenosti mezi jeho zdrojem a daným přijímacím uzlem. Ostatní zpožděné signály, šířící se k přijímači alternativními cestami, tak můžeme zcela zanedbat.

DIFERENČNÍ RSS

Existuje ještě příbuzná metoda založená na principu hyperbolické lokalizace. Hledaný zdroj rušivého signálu se rovněž nachází na průsečíku dvou hyperbolických křivek. Tyto křivky však nejsou určeny vzájemným rozdílem v časech příchodu signálu, ale v rozdílu mezi úrovní přijatého signálu RSS. Touto metodou lokalizace se podrobně zabývá studie [35].

5.2 Vyhodnocení základních metod lokalizace

Tato kapitola shrnuje diskutované metody rádiového určování polohy. V následujícím srovnání jsou porovnány zejména výhody a nevýhody jednotlivých systémů.

TRILATERAČNÍ ZAMĚŘOVAČ RSS

+	relativně jednoduchá realizace	-	nízká přesnost určení polohy
+	nevyžaduje synchronizaci přijímačů	-	citlivost na vícecestné šíření

SMĚROVÝ ZAMĚŘOVAČ RSS

+	relativně jednoduchá realizace	-	nízká přesnost určení polohy
+	nevyžaduje synchronizaci přijímačů	-	citlivost na vícecestné šíření

SMĚROVÝ ZAMĚŘOVAČ AoA

+	nevyžaduje synchronizaci přijímačů	-	nelze sledovat více zdrojů
+	vysoká přesnost v případě více uzlů	-	velká výpočetní náročnost

MULTILATERAČNÍ ZAMĚŘOVAČ TDoA

+	odolnost vůči vícecestnému šíření	-	vyžaduje přesnou synchronizaci
+	vysoká přesnost	-	náročnější realizace

6 GENEROVÁNÍ RUŠIVÝCH SIGNÁLŮ

Víme, že v praxi nejčastěji implementovaným rušivým signálem je signál frekvenčně modulovaný s lineárním rozmítáním kmitočtu neboli *Chirp*. Přistupovat k problematice rušení GNSS signálů pouze z pohledu tohoto typu signálu by však nebylo správné, protože se v praxi mohou objevit i jiné typy neinteligentních rušivých signálů, které by pak pro nás byly hůře detekovatelné. Z toho důvodu bychom se měli připravit na jejich přítomnost tak, že vygenerujeme I/Q vzorky těchto signálů a vyhodnotíme jejich vliv na kvalitu přijímaného GNSS signálu. Díky tomu pak budeme schopni určit, na jaké typy rušivých signálů se v rámci detekce a lokalizace zaměřit.

Základní rozdělení rušivých signálů na *Jamming* a *Spoofing* již známe z teoretické části této práce. Pro účely vyhodnocení vlivu rušení na kvalitu GNSS signálů tak byly vybrány různé typy signálů, které svými vlastnostmi co nejlépe vystihují široké spektrum potenciálně rušivých signálů. Mezi tyto signály byly zvoleni zástupci kontinuálních signálů jako např. harmonický rušivý signál na pevně daném kmitočtu, amplitudově modulovaný rušivý signál s harmonickou změnou amplitudy, fázově modulovaný rušivý signál s harmonickou změnou fáze a frekvenčně modulovaný rušivý signál s harmonickou změnou kmitočtu. Vzhledem k až bezvýhradnému použití v praxi byl dále vybrán frekvenčně modulovaný rušivý signál s lineární změnou kmitočtu neboli *Chirp.* Dále byl zařazen impulsní rušivý signál s vnitropulsní frekvenční modulací a také impulsní rušivý signál bez vnitropulsní modulace. Dále jsme se rozhodli zahrnout signál typu *Frequency Hopping* s rozprostřeným spektrem, a to zejména díky jeho potenciální odolnosti vůči obraným prostředkům (v angl. lit. *Countermeasures*). Závěr je pak věnován té pravděpodobně nejnebezpečnější skupině inteligentních rušivých signálů typu *Spoofing*.

V následujících kapitolách jsou tyto signály matematicky definovány a pro ilustraci i graficky znázorněny. Vzorky těchto signálů jsme vygenerovali pomocí návrhového a simulačního prostředí MATLAB. Vzešlé skripty, zajišťující efektivní generování těchto signálů, jsou uvedeny v příloze této práce. Výstupem těchto skriptů pak jsou soubory obsahující I/Q vzorky ve formátu kompatibilním pro import do SDR. Komplexní obálku vygenerovaných signálů lze vyjádřit následujícím vztahem:

$$R(t) = I(t) + jQ(t) \tag{6.1}$$

6.1 Kontinuální signály

Aby bylo dosaženo požadovaného rušivého účinku, je nutné kontinuální rušivé signály generovat na dedikovaném kmitočtu. V případě frekvenční modulace pak signál rozmítat v jeho těsné blízkosti. Samotného efektu rušení je pak v případě kontinuálních signálů dosaženo relativně velkým výkonem rušivých signálů.

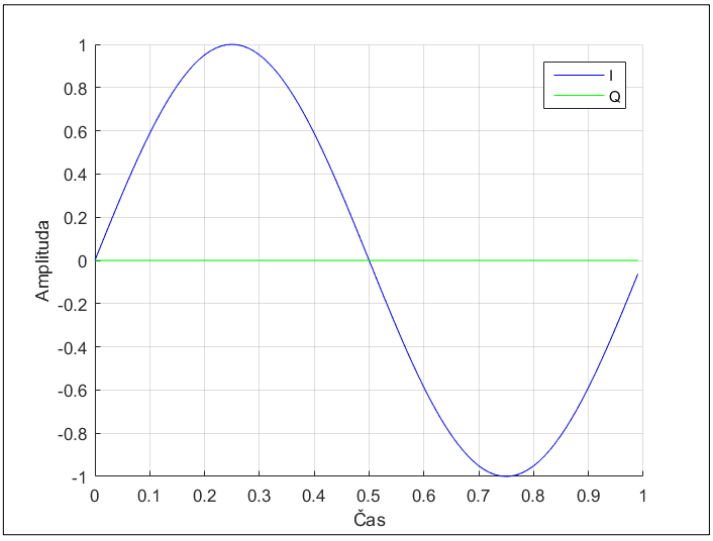
6.1.1 Harmonický signál (Příloha 1)

Teoreticky nejjednodušším způsobem, jak napadnout určitý rádiový komunikační systém, je generovat rušivý harmonický signál na jeho nosném kmitočtu. V případě, že zajistíme dostatečný výkon rušivého signálu, dostaví se požadovaný efekt vlivem silné interference rušivého a cíleného signálu takřka okamžitě. Pak již pouze závisí na schopnosti daného systému takovému útoků odolávat. Takový rušivý signál vyjádřený pomocí jeho soufázové a kvadraturní komponenty lze popsat následujícími vztahy:

$$I = x(t) = A\sin(2\pi f t) \tag{6.2}$$

$$Q = y(t) = 0 \tag{6.3}$$

Kde A vyjadřuje jednotkovou amplitudu signálu a f jeho kmitočet, resp. kmitočet cíleného rádiového komunikačního systému. V sekci „**PŘÍLOHA 1**“ nalezneme skript pro generování I/Q vzorků tohoto signálu. Jedna perioda vygenerovaného rušivého signálu je znázorněna na následujícím obrázku:



Obrázek 18: Harmonický signál

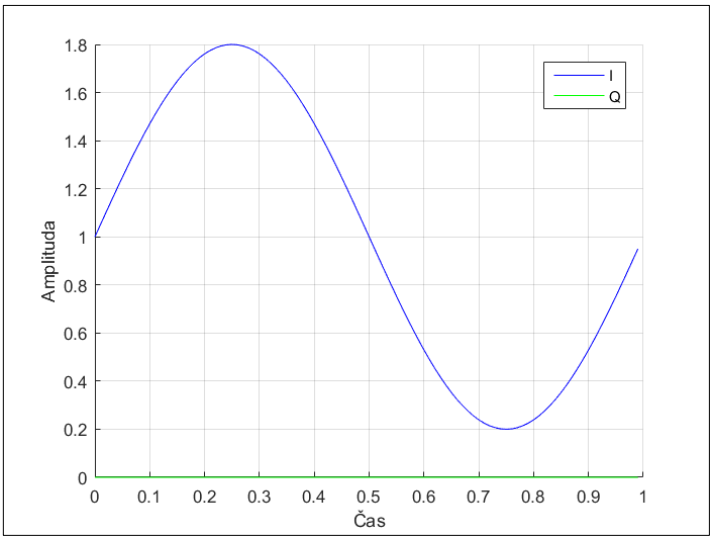
6.1.2 Amplitudově modulovaný signál (Příloha 2)

Amplitudovou modulaci řadíme mezi spojité modulace, kdy se v závislost na průběhu modulačního signál mění amplituda nosného signálu. Frekvence ani fáze nosného signálu se u této modulace nemění. Amplitudově modulovaný rušivý signál vyjádřený soufázovou a kvadraturní komponentou lze popsat následujícími vztahy:

$$I = x(t) = A_C[1 + m(t)] = 1 + \mu\sin(2\pi f_m t) \tag{6.4}$$

$$Q = y(t) = 0 \tag{6.5}$$

Kde A_C vyjadřuje jednotkovou amplitudu nosné vlny, $m(t)$ je modulační signál, f_m je kmitočet modulačního signálu a μ vyjadřuje hloubku modulace. Hloubka modulace je vždy <1 a často je uváděna v procentech. Při překročení 100 % hloubky modulace dochází ke zkreslení přenášené informace, což je pro naší aplikaci sice irelevantní, nicméně to poslouží k popisu zobrazovaného průběhu. V sekci „**PŘÍLOHA 2**“ nalezneme skript pro generování I/Q vzorků tohoto signálu. Jedna perioda vygenerovaného rušivého signálu s hloubkou modulace 80 % je znázorněna na následujícím obrázku:



Obrázek 19: Amplitudově modulovaný signál

6.1.3 Fázově modulovaný signál (Příloha 3)

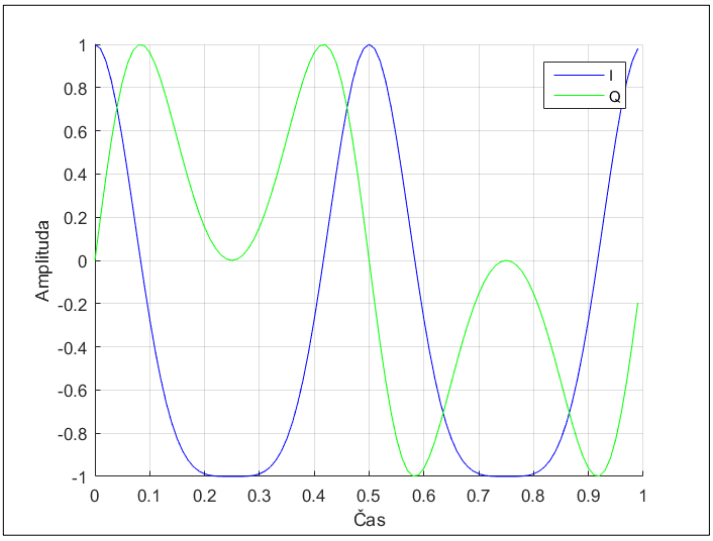
V rámci fázové modulace je modulačním signálem ovlivňována fáze nosné vlny. V našem případě má změna fáze v čase spojitý harmonický průběh. Spojitá fázová modulace není v praxi příliš využívána, protože vyžaduje poměrně složitý demodulátor. Náš signál však nenese žádnou informační hodnotu a pro účely experimentálního měření tak dokáže svůj potenciál rušivého

signálu naplnit. Fázově modulovaný rušivý signál vyjádřený soufázovou a kvadraturní komponentou lze popsat následujícími vztahy:

$$I = x(t) = A_C \cos[\Delta_p m(t)] = \cos[\Delta_p \sin(2\pi f_m t)] \tag{6.6}$$

$$Q = y(t) = A_C \sin[\Delta_p m(t)] = \sin[\Delta_p \sin(2\pi f_m t)] \tag{6.7}$$

Kde A_C vyjadřuje jednotkovou amplitudu nosné vlny, $m(\sigma)$ je modulační signál, f_m je kmitočet modulačního signálu a Δ_p je špičková odchylka fáze, která má v našem případě hodnotu π. V sekci „**PŘÍLOHA 3**“ nalezneme skript pro generování I/Q vzorků tohoto signálu. Jedna perioda vygenerovaného rušivého signálu s harmonickým průběhem změny fáze je znázorněna následujícím obrázku:



Obrázek 20: Fázově modulovaný signál

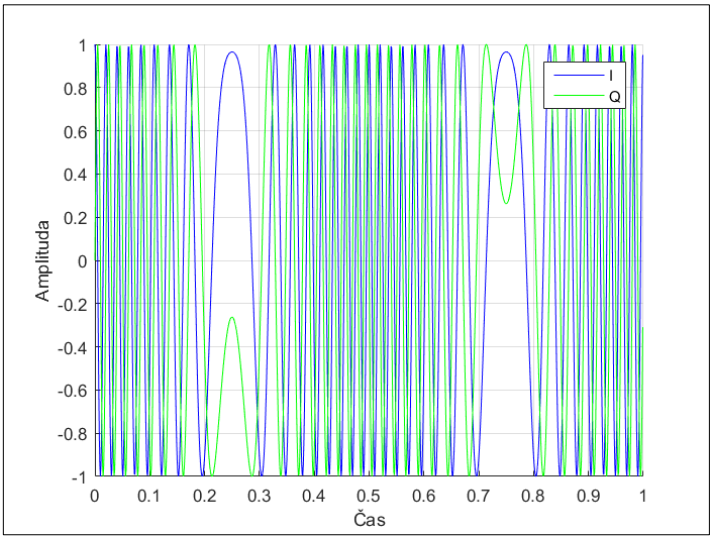
6.1.4 Frekvenčně modulovaný signál (Příloha 4)

Frekvenční modulaci vyjadřuje závislost okamžité frekvence nosné vlny na změnách amplitudy modulačního signálu. V našem případě, kdy je modulační signál harmonický, dochází k maximální odchylce od nosného kmitočtu v maximu amplitudy modulačního signálu. Modulovaný signál je tak v podstatě rozmítán v okolí nosného kmitočtu. Obdobně jako v předchozích případech je u frekvenční modulace vlastní princip efektivního rušení cíleného signálu realizován především vysokým výkonem rušičky. Frekvenčně modulovaný rušivý signál vyjádřený soufázovou a kvadraturní komponentou lze popsat následujícími vztahy:

$$I = x(t) = A_C \cos[\Delta_f \int_{-\infty}^{t} m(\sigma)d\sigma] = \cos[\beta \sin(2\pi f_m t)] \tag{6.8}$$

$$Q = y(t) = A_C \sin[\Delta_f \int_{-\infty}^{t} m(\sigma)d\sigma] = \sin[\beta \sin(2\pi f_m t)] \tag{6.9}$$

Kde A_C vyjadřuje jednotkovou amplitudu nosné vlny, $m(\sigma)$ je modulační signál, f_m je kmitočet modulačního signálu, Δ_f je špičková odchylka od nosného kmitočtu (frekvenční zdvih) a β je modulační index, který vyjadřuje poměr mezi špičkovou odchylkou od nosného kmitočtu a modulačním kmitočtem Δ_f / f_m. V sekci „**PŘÍLOHA 4**“ nalezneme skript pro generování I/Q vzorků tohoto signálu. Jedna perioda vygenerovaného rušivého signálu s harmonickým průběhem změny kmitočtu nosného signálu je znázorněna na následujícím obrázku:



Obrázek 21: Frekvenčně modulovaný signál

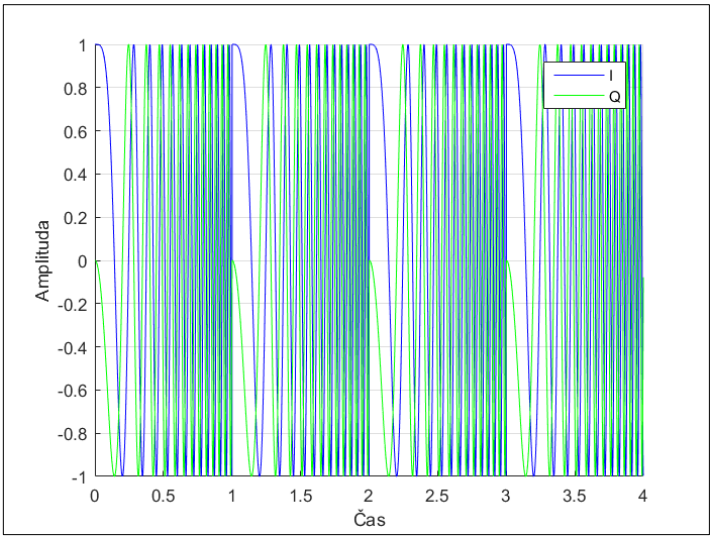
6.2 Lineárně rozmítané signály

V úvodu předchozí kapitoly jsme si řekli, že nejjednodušším způsobem, jak dosáhnout efektivního rušení určitého rádiového systému, je generovat rušivý signál na jeho nosném kmitočtu. Z hlediska realizace samotné rušičky to však nemusí být úplně pravda. Taková rušička totiž bude zcela jistě klást určité nároky na stabilitu kmitočtu. Mnohem jednodušší by tak bylo realizovat obvod založený na časovači a napětím řízeném oscilátoru, který by rušivý signál rozmítal v okolí nosného kmitočtu.

6.2.1 Chirp signál I (Příloha 5)

Průběh změny kmitočtu v čase má pilovitý průběh a je tak charakterizován lineárním nárůstem kmitočtu v rámci celého rozsahu rozmítání. Ten je u tohoto signálu zcela periodický a

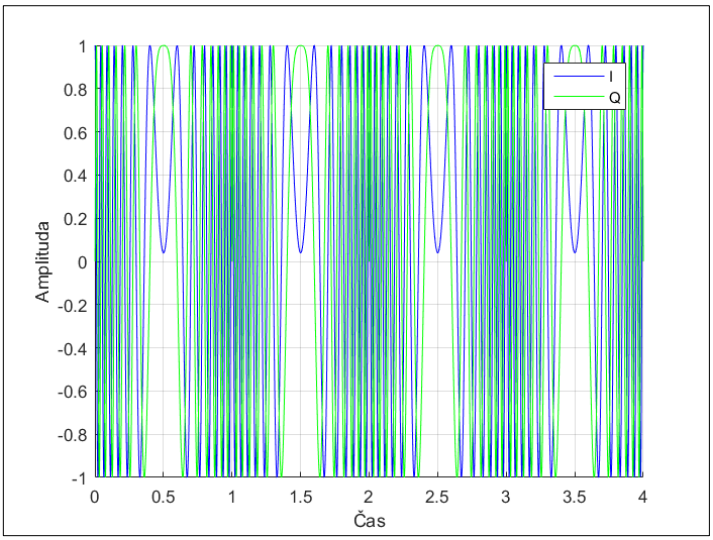
frekvenční charakteristika tak má pilovitý průběh. V sekci „**PŘÍLOHA 5**“ nalezneme skript pro generování I/Q vzorků tohoto signálu. Na následujícím obrázku jsou znázorněny celkem čtyři periody rozmítání:



Obrázek 22: Chirp signál I

6.2.2 Chirp signál II (Příloha 6)

Oproti předchozímu případu má tento signál jiný průběh přeladění kmitočtu. V rámci jedné periody rozmítaní je signál nejprve přeladěn z maximální kladné k maximální záporné odchylce a poté zpět k maximální kladné odchylce. V sekci „**PŘÍLOHA 6**“ nalezneme skript pro generování I/Q vzorků tohoto signálu. Na následujícím obrázku jsou znázorněny celkem čtyři periody rozmítání:



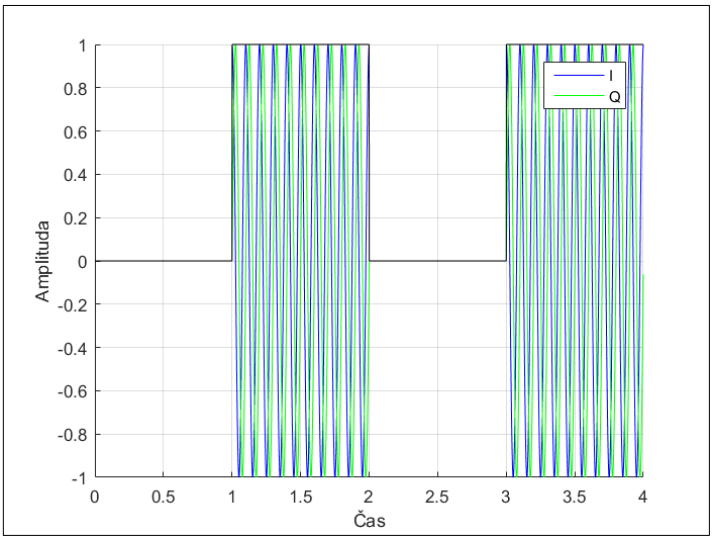
Obrázek 23: Chirp signál II

6.3 Impulsní signály

Pro testování vlivu rušivých signálů byly rovněž vygenerovány impulsní signály. Rušení způsobené energetickými pulsy totiž může mít na GNSS signál více devastující účinek než signály kontinuální.

6.3.1 Impulsní signál I (Příloha 7)

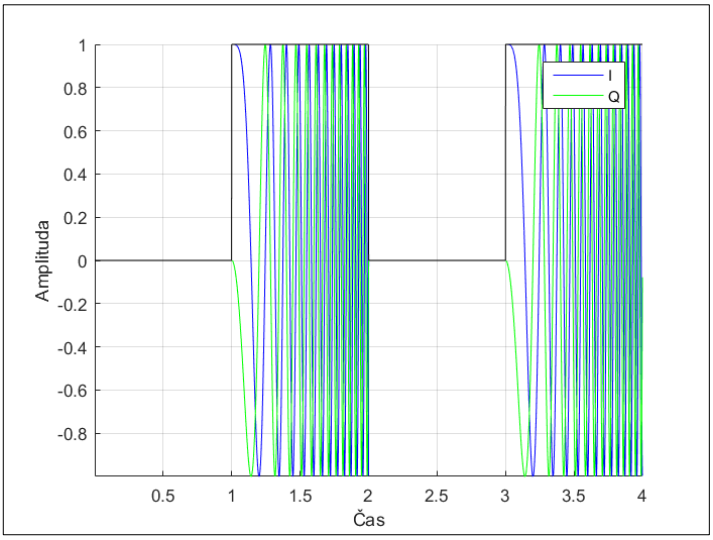
V sekci „**PŘÍLOHA 7**“ nalezneme skript pro generování I/Q vzorků tohoto signálu. Následující obrázek znázorňuje dvě opakovací periody impulsního signálu bez vnitro-pulsní modulace:



Obrázek 24: Impulsní signál I

6.3.2 Impulsní signál II (Příloha 8)

V sekci „**PŘÍLOHA 8**“ nalezneme skript pro generování I/Q vzorků tohoto signálu. Následující obrázek znázorňuje dvě opakovací periody impulsního signálu s vnitro-pulsní frekvenční modulací:



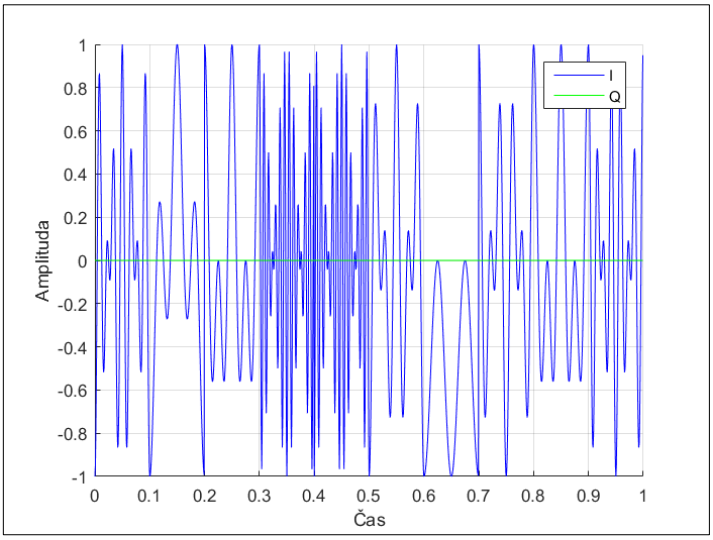
Obrázek 25: Impulsní signál II

6.4 Signály s rozprostřeným spektrem

Existují dva často využívané typy signálů s rozprostřeným spektrem. Prvním typem je signál rozprostřený pseudonáhodnou kódovou posloupností DSSS (*Direct Sequence Spread Spectrum*). Tento typ signálu využívá ke komunikaci např. systém GPS. Druhým typem je signál rozprostřený frekvenčními skoky FHSS (*Frequency Hopping Spread Spectrum*). Tento typ signálu je často využíván v armádních aplikacích, a to především díky jeho mimořádné odolnosti vůči rušení

6.4.1 Signál rozprostřený frekvenčními skoky (Příloha 9)

Signál typu FHSS jsme vybrali zejména z důvodu jeho potenciální schopností proniknout primární ochranou GNNS přijímačů. Jak již bylo zmíněno v kapitole **3.2.5** „Zvýšení účinku rušení“, běžně dostupné přijímače jsou zpravidla chráněny proti kontinuálnímu rušení pomocí adaptivní pásmové zádrže typu *Notch Filter*. Tento typ ochrany však může u signálů s rychlou změnou kmitočtu selhávat. Následující obrázek znázorňuje FHSS signál, jehož prostřednictvím je na šesti kmitočtech rozprostřena datová zpráva náhodného charakteru. V sekci „**PŘÍLOHA 9**“ nalezneme skript pro generování I/Q vzorků tohoto signálu.



Obrázek 26: Signál rozprostřený frekvenčními skoky

6.5 Inteligentní signály

Na základě kapitoly **3.4.5** „Semi-spoofing III. třídy“ byl realizován pokus o vygenerování slabě korelovaných rušivých signálů, které by svou signálovou strukturou vyvolaly krátkodobou synchronizaci přijímače na generovaný rušivý signál. Pro realizaci takových rušivých signálů je stěžejní dosažení určitého stupně korelace, která může být realizována prostřednictvím C/A kódu.

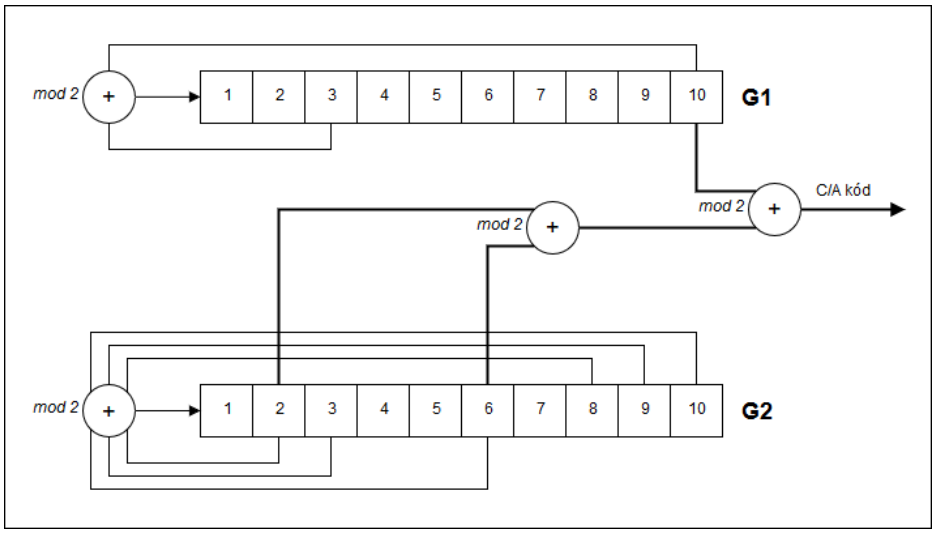
6.5.1 Generátor C/A kódu (Příloha 10)

C/A kód je tvořen pseudonáhodnou posloupností PRN (*Pseudo Random Number*). Tyto posloupnosti mají charakter náhodné bitové sekvence, nicméně jsou velmi přesně definovány a my proto říkáme, že jsou tzv. „pseudonáhodné“. Každá družice má svůj vlastní C/A kód. Jednotlivé C/A kódy jsou vybrány ze skupiny tzv. Goldových kódů, protože mají vhodné vlastnosti pro implementaci do CDMA schématu GNSS komunikace. Prvním důvodem, proč jsou zvoleny právě Goldovy kódy, jsou jejich výborné autokorelační vlastnosti. To v praxi znamená, že autokorelační funkce je velmi ostrá a její vedlejší maxima jsou zanedbatelná. Aby signál tyto vlastnosti splnil, musí mít statisticky náhodný charakter a neopakovat se v žádném bodě sekvence. Druhým důvodem, proč jsou tyto kódy zvoleny, je nutnost naprosto jednoznačného rozlišení signálů jednotlivých družic. Laicky řečeno, čím si budou signály méně podobné, tím lépe. Tuto vlastnost můžeme zajistit tak, že budou signály jednotlivých družic téměř ortogonální. V takovém případě budou vzájemně jen velmi málo korelované a vždy je dokážeme bezpečně rozlišit.

Aby C/A kód splňoval uvedené parametry, generujeme jeho posloupnost pomocí speciálního schématu, který je ilustrován na následujícím obrázku. Schéma je tvořeno dvěma posuvnými registry G1 a G2 [38]. Tyto registry jsou popsány prostými polynomy **6.10** a **6.11**, které určují pozice zpětnovazebních bitů ovlivňujících budoucí stav daného registru. Výsledná posloupnost C/A kódu generovaného na základě tohoto schématu je tvořena 1023 čipy. V praxi je pak vysílán s přenosovou rychlostí 1,023 *Mbit/s* a opakuje se tedy každou tisícinu sekundy. V sekci „**PŘÍLOHA 10**“ nalezneme skript pro generování libovolného C/A kódu.

$$G1(X) = 1 + X^3 + X^{10} \tag{6.10}$$

$$G2(X) = 1 + X^2 + X^3 + X^6 + X^8 + X^9 + X^{10} \tag{6.11}$$



Obrázek 27: Schéma generování C/A kódu [38]

Výstup registru G1 je vždy na pozici 10. bitu. Výstupy registru G2 jsou však variabilní. Pro každou družici (resp. C/A kód) je kombinace výstupů registru G2 jiná. V zobrazené konfiguraci je výstup na 2. a 6. pozici registru. To značí, že bude vygenerován C/A kód č. 1/37. V případě konfigurace 3. a 7. výstupní pozice bude vygenerován C/A kód č. 2/37. Každý C/A kód má svou unikátní kombinaci výstupních pozic registru G2 atd. viz [16].

6.5.2 Inteligentní signál I (Příloha 11)

V rámci tohoto signálu je implementováno schéma uvedené v předchozí kapitole. Na základě vstupního požadavku je zvolena jedna z družic systému GPS a jí přidružený C/A kód. Vygenerovaný kód je následně převzorkován a zařazen do opakující se sekvence. Výsledný rušivý signál je tak korelovaný pouze s vybranou družicí. V sekci „**PŘÍLOHA 11**“ nalezneme skript pro generování I/Q vzorků tohoto signálu.

6.5.3 Inteligentní signál II (Příloha 12)

Na rozdíl od předchozího případu je zde vygenerováno všech 37 dostupných C/A kódů. Ty jsou rovněž převzorkovány a zařazeny do opakující se sekvence. Výsledná kódová sekvence je pak rozdělena na 37 intervalů. V každém z těchto intervalů je výsledný rušivý signál korelovaný pouze s jednou z dostupných družic. V sekci „**PŘÍLOHA 12**“ nalezneme skript pro generování I/Q vzorků tohoto signálu.

7 PLATFORMA PRO REALIZACI RUŠIČKY

Vstupním požadavkem volby platformy pro realizaci GNSS rušičky je možnost změny parametrů rušivého signálu. V takovém případě se přímo nabízí dvě možnosti realizace. V prvním případě můžeme jako rušičku použít signálový generátor. Toto řešení však z hlediska mobility není příliš praktické a hodí se spíše do laboratorních podmínek. V rámci budoucích experimentálních testů se totiž budeme zabývat i měřením ve volném prostotu. Rozměry, váha a nutnost síťového napájení signálového generátoru tak příliš nevyhovuje našim požadavkům. V druhém případě lze rušičku realizovat pomocí tzv. softwarově definovaného rádia, které v kombinaci s přenosným počítačem umožní generovat libovolný typ RF signálu a oproti běžným signálovým generátorům tak nabízí vysokou mobilitu.

7.1 Softwarově definované rádio

Rádiové komponenty jako např. modulátory, demodulátory, zesilovače nebo filtry byly donedávna čistě hardwarovou záležitostí. Vytrvalé navyšování výpočetního výkonu obvodů pro zpracování signálu však umožňuje tyto dříve čistě hardwarové komponenty implementovat softwarově. Za cenu několika desítek až stovek *USD* tak dnes lze získat zařízení, jehož funkční ekvivalent by ještě před několika lety byl otázkou několika tisíc *USD*.

Softwarově definované rádio SDR (angl. *Software Defined Radio)* pracuje na bázi běžného DVB-T tuneru. Prvotním impulsem, jež zažehl nebývalý zájem o softwarově definované rádio, bylo zjištění, že I/Q vzorky signálu lze z jakéhokoliv DVB-T tuneru získat relativně jednoduchým softwarovým zásahem. V rámci používaných DVB-T chipsetů totiž existuje možnost deaktivace OFDM demodulátoru. Deaktivací obejdeme příslušné zpracování signálu a získáme tak přístup k surovým I/Q vzorkům přijímaného spektra. Tyto soufázové „I“ (angl. *In-Phase*) a kvadraturní „Q“ (angl. *Quadrature*) vzorky vyjadřují tzv. analytickou formu signálu.

Při výběru vhodného SDR je třeba dbát na základní parametry zpracování signálu [36] jako je frekvenční rozsah, vzorkovací frekvence, rozlišení A/D převodníku, maximální okamžitá šířka pásma, schopnost RX/TX nebo zdali je vybaveno zabudovanými předřadnými filtry.

Příkladem nejjednoduššího softwarově definovaného rádia je RTL-SDR (20 *USD*) [36]. Toto zařízení má obrovskou uživatelskou základnu a je tak široce programově podporováno. Existují i dražší zařízení, které disponují především lepšími parametry zpracování signálu a také kvalitou provedení. Příkladem uvedeme Airspy (199 *USD*) nebo SDRPlay (149 *USD*). Tato

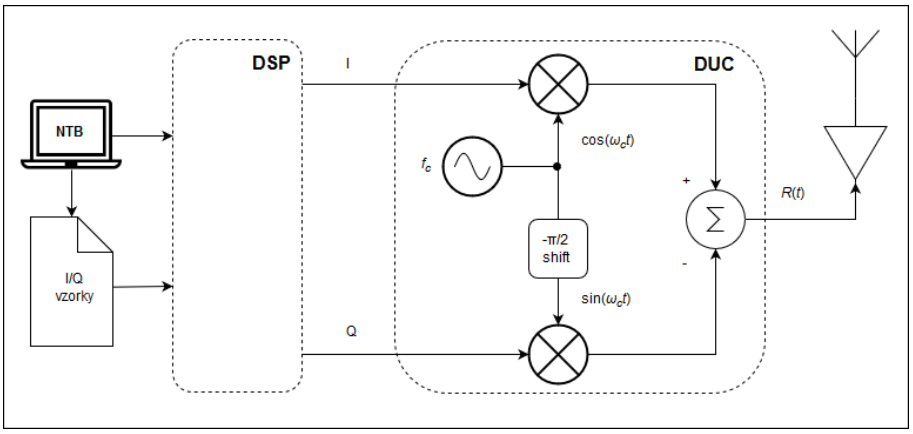
konkrétní zařízení jsou považována za nejlépe cenově dostupná [36]. Bohužel jsou ale vybavena pouze možností signál přijímat. Vzhledem k aktivní povaze aplikace, jež je předmětem této práce, potřebujeme signál v první řadě vysílat. Touto schopností disponují např. zařízení HackRF (300 *USD*) nebo BladeRF (až 650 *USD*) [36].

7.2 Implementace rušivých signálů

Jak již bylo zmíněno, v rámci SDR lze získat přístup k I/Q vzorkům signálu. Výrobci softwarově definovaných rádií, která disponují zároveň vysílacím režimem, umožnují uživateli v rámci tohoto režimu nahrát vlastní I/Q vzorky libovolného signálu. Pro implementaci rušivých signálů pro budoucí experimentální měření bylo zvoleno softwarově definované rádio HackRF od společnosti Great Scott Gadgets [37], které tímto režimem standardně disponuje. K zařízení přistupujeme v rámci operačního systému Linux přes příkazovou řádku. Soubor s I/Q vzorky rušivého signálu pak lze jednoduchým způsobem nahrát přímo do SDR.

Obrázek 28: Softwarově definované rádio HackRF [37]

Na následujícím obrázku je znázorněn funkční diagram vysílací části SDR. Nejprve jsou prostřednictvím simulačního prostředí Matlab vygenerovány 8-bitové I/Q vzorky požadovaného signálu. Ty musí mít vzhledem k parametrům SDR přesně daný formát. Soubor se vzorky je pak prostřednictvím příkazové řádky importován do SDR. Vzorky jsou dále zpracovány digitálním signálovým procesorem DSP (*Digital Signal Processor*), a v rámci bloku DUC (*Digital Up-Converter*) modulovány na požadovaný nosný kmitočet f_c. Modulovaný signál je poté zesílen a dále distribuován.



Obrázek 29: Funkční diagram vysílací části SDR

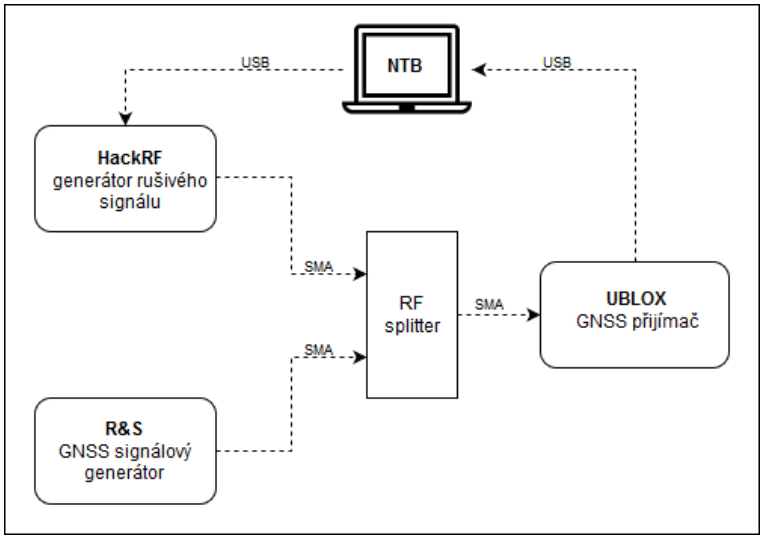
8 EXPERIMENTÁLNÍ MĚŘENÍ

Tato kapitola připravuje podmínky pro budoucí experimentální měření, které však není náplní této práce. V rámci experimentálních měření bude v budoucnu testován vliv vygenerovaných rušivých signálů na GNSS přijímač.

GNSS signály, které jsou ve spektru rozprostřeny pomocí pseudonáhodné posloupnosti, mají určitý zisk zpracování. Ten se pohybuje okolo 30-40 *dB* a je způsoben především výbornými korelačními vlastnostmi družicových signálů. Navíc přijímač pracuje s určitou rezervou, která se obvykle pohybuje okolo 10 *dB*. Zisk zpracování tak výrazně zlepšuje odstup přijatého signálu od šumu. Pokud tedy uvážíme, že systém přijímá signál úrovni -170 *dBm*, tak ho musíme rušit signálem o úrovni minimálně -130 *dBm*, abychom zahrnuli zisk zpracování (30 *dB*) i rezervu (10 *dB*) a systém tak nebyl schopný rušený signál zpracovat. Toto doporučení se samozřejmě týká pouze signálů typu *Jamming*, kde je efekt rušení realizován především velkým vysílacím výkonem.

8.1 Měření v laboratorních podmínkách

Zapojení experimentálního měřícího pracoviště umožnuje bezemisní vyhodnocení vlivu rušivých signálů na přijímač. Prvky zapojení jsou uspořádány dle následujícího schématu:



Obrázek 30: Laboratorní měřícího pracoviště

Zapojení se skládá ze softwarově definovaného rádia HackRF, GNSS generátoru Rohde&Schwarz, GNSS přijímače UBLOX, RF splitteru a přenosného počítače. Prostřednictvím simulačního prostředí Matlab je zajištěno generování I/Q vzorků vybraných signálů. Vzorky jsou

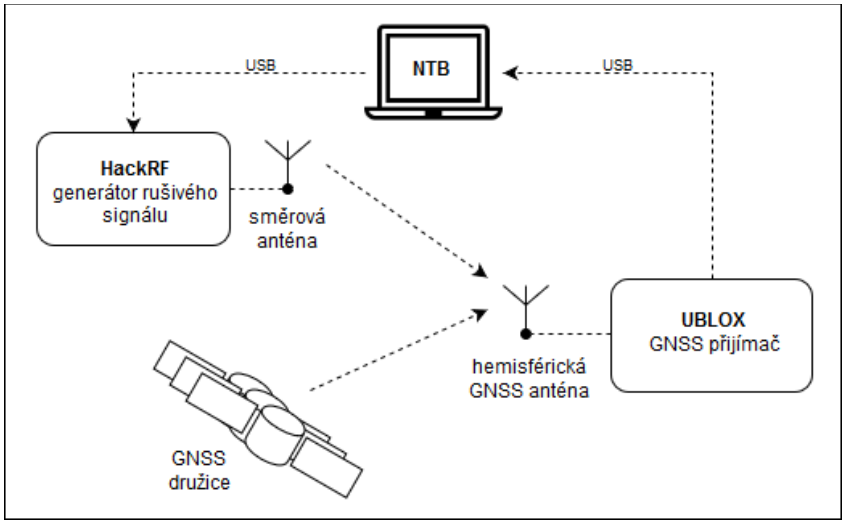
do SDR importovány přes USB rozraní. RF prvky jsou vzájemně propojeny pomocí SMA konektorů. Specializovaným softwarem UBLOX pak lze provádět nejrůznější analýzy přijímaného signálu.

8.2 Měření ve volném prostoru

Rušení GNSS signálů je stejně jako ve všech vyspělých státech také v České republice ilegální. Vyšetřit vliv rušení na přesnost určení polohy však lze nejlépe v reálných podmínkách. Měřící polygon ve volném prostoru je tedy nutné zabezpečit tak, aby nedošlo k ovlivnění funkčnosti jakéhokoliv systému či služby, jež GNSS signálů signál využívá. Během měření je tak nutné provést minimálně následující opatření:

I. Měřící polygon musí být vybrán v dostatečné vzdálenosti od obydlené aglomerace. Tato vzdálenost může být vypočtena dle rovnic popisujících šíření signálu ve volném prostoru a zároveň přiměřeně nadsazena.
II. Pro vysílání rušivého signálu byla zvolena směrová anténa, která elektromagnetické záření soustředí pouze do míst, kde se nachází experimentální GPS přijímač.
III. Umístění GPS přijímače musí být zvoleno tak, abychom minimalizovali vícecestné šíření vznikající na terénních překážkách za přijímačem.
IV. Během měření je třeba dbát na přítomnost nízko letících letadel průběžnou vizuální kontrolou.

Při dodržení těchto podmínek lze předpokládat, že nám bude Českým telekomunikačním úřadem vydáno časově omezené povolení, jež by nám umožňovalo provést plánovaná měření. Konfigurace měřícího polygonu je naznačena následujícím obrázkem:



Obrázek 31: Měřící pracoviště ve volném prostoru

Zapojení se skládá ze softwarově definovaného rádia HackRF, GNSS přijímače UBLOX a přenosného počítače. Obdobně jako v případě laboratorního měření je pomocí simulačního prostředí Matlab zajištěno generování I/Q vzorků vybraných RF signálů. Vzorky jsou do SDR importovány přes USB rozraní a dále distribuovány pomocí směrové antény. GNSS přijímač UBLOX je oproti tomu vybaven hemisférickou anténou pro všesměrový příjem GNSS signálů. Obdobně jako v předchozím případě pak lze pomocí specializovaného softwaru UBLOX provádět nejrůznější analýzy přijímaného signálu.

ZÁVĚR

Zabezpečit signály GNSS systémů vůči rádiovému rušení je vzhledem k jejich slabé výkonové úrovni velice obtížným úkolem. Problematika detekce a lokalizace rušení GNSS systémů doposud nebyla uspokojivě vyřešena. Úkolem této práce tak je provést podrobnou klasifikaci rušivých signálů, které mohou negativně ovlivňovat činnost GNSS systémů a věnovat se způsobům jejich detekce lokalizace.

Podařilo se nám nalézt několik rádiových systémů, které na svých harmonických kmitočtech interferují s GNSS signály a upozornit tak na možné riziko zhoršení jejich dostupnosti v blízkosti vysílacích prvků inkriminovaných rádiových systémů.

Dále jsme provedli podrobnou klasifikaci signálů a zařízení, které jsou konstruovány přímo za účelem rádiového rušení GNSS systémů. Provedli jsme také cenovou analýzu těchto zařízení a náročnost jejich případné realizace. Tím jsme pomohli poodhalit charakter potenciálního útočníka. Tato analýza dále upozorňuje na fakt, že i velice levným zařízením lze zcela vyřadit dostupnost GNSS signálů, a to až na vzdálenost několika kilometrů. Z navazujícího rozboru inteligentních rušivých signálů vyplývá, že sofistikované útoky je možné provádět až s několikanásobně nižšími vysílacími výkony, než je tomu u rušení „hrubou silou“.

Účinná prevence vůči těmto typům rušení v podstatě neexistuje a my se tak dále soustředili především na jejich detekci, která by nám umožnila varovat uživatele před možným útokem. V oblasti detekce rušivých signálů jsme analyzovali několik softwarově založených metod, které mají na úrovni přijímače potenciál k úspěšnému odhalení různých typů útoků. Metoda vyhodnocení odezvy AGC dokáže na základě nestandardních výkyvů úrovně přijímaného signálu odhalit rušení ještě v pre-korelační fázi. Metoda kontroly integrity signálů RAIM provádí nejrůznějších redundantní měření a rušení tak dokáže odhalit až v post-korelační fázi, na druhou stranu s větší úspěšností než metoda AGC. Tyto metody jsou aplikovatelné čistě softwarovým zásahem na úrovni uživatelského přijímače. Jejich mechanismy však trpí nedostatečnou ochranou vůči sofistikovanějším útokům. Věnovali jsme se proto i robustnějším metodám, které již vyžadují určitý hardwarový zákrok. Metoda DRCC dokáže na základě vztahu mezi vojenským a civilním družicovým signálem odhalit, zda je přijímaný GNSS signál pod vlivem rušení. Tato metoda vyžaduje konfiguraci dvou přijímačů, mezi kterými je provedena korelace. To vyžaduje zavedení komunikačního kanálu mezi oběma přijímači, z nichž jeden nesmí být vystaven vlivům rušení. Další diskutovaná metoda pak využívá více prvkové anténní konfigurace, díky které dokážeme určit směr příchodu signálu a spolehlivě tak detekovat bodový zdroj rušení. Problém

nastává v případě rušení soustředěného z více směrů, kdy tato metoda selhává. Poslední metodou, které jsme se věnovali, je ověření navigační zprávy NMA pomocí speciálních bezpečnostních klíčů, které jsou modulovány na družicový signál. Tato metoda má velký potenciál, nicméně vyžaduje výrazný zásah do celkové infrastruktury.

V další části této práce jsme se věnovali metodám lokalizace rušivých signálů. Pro budoucí realizaci lokalizačního systému bychom na základě provedeného rozboru doporučili metodu TDoA. Tato metoda se jeví jako nejpřesnější, a to zejména díky její odolnosti vůči vícecestnému šíření.

Těžištěm této práce bylo vygenerovat vzorky vybraných rušivých signálů. Pomocí softwarového prostředí Matlab se nám podařilo vytvořit skripty zajišťující generování širokého spektra rušivých signálů, které co nejlépe vystihují povahu reálného útoku. Dále bylo zajištěno, aby byly vygenerované signály kompatibilní s vybraným softwarově definovaným rádiem a komplet tak byl připraven k budoucímu měření.

Závěrem této práce jsou nastíněny podmínky pro testování odolnosti GNSS přijímačů vůči rušení. Na základě navržených konfigurací testovacích pracovišť mohou být v budoucnu provedena příslušná měření. Výsledky těchto měření pak poslouží k realizaci konkrétních systémů detekce a lokalizace.

SEZNAM POUŽITÉ LITERATURY

[1] Zpracování navigačních signálů. KOVÁŘ, Pavel. *Družicová navigace: Od teorie k aplikacím v softwarovém přijímači*. 1. Praha: ČVUT, 2016, s. 77-103. ISBN 978-80-01-05989-0.

[2] BORIO, Daniele, Fabio DOVIS, Heidi KUUSNIEMI a Letizia LO PRESTI. Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. *Proceedings of the IEEE*. IEEE, 2016, (104), 1233 - 1245. DOI: 10.1109/JPROC.2016.2543266.

[3] SCOTT, Logan. Spoofing: Upping the Anti. *InsideGNSS* [online]. 2013. [cit. 2017-05-25]. Dostupné z: http://www.insidegnss.com/node/3636

[4] MITCH, Ryan, Ryan DOUGHERTY, Mark PSIAKI, Steven POWELL, Brady O'HANLON, Jahsan BHATTI a Todd HUMPHREYS. Signal Characteristics of Civil GPS Jammers. ION GNSS, 2011.

[5] BOROWSKI, Holly, Oscar ISOZ, Fredrik MARSTEN EKLÖF, Sherman LO a Dennis AKOS. *Detecting False Signals with Automatic Gain Control* [online]. 2012 [cit. 2017-05-25]. Dostupné z: http://gpsworld.com/detecting-false-signals-automatic-gain-control-12804/

[6] *THE EUROPEAN TABLE OF FREQUENCY ALLOCATIONS AND APPLICATIONS IN THE FREQUENCY RANGE 8.3 kHz to 3000 GHz: ECA TABLE*. In: Electronic Communications Committee (ECC), 2016. Dostupné také z: http://www.erodocdb.dk/docs/doc98/official/pdf/ERCRep025.pdf

[7] Front End. *European Space Agency* [online]. GMV, 2011 [cit. 2017-05-25]. Dostupné z: http://www.navipedia.net/index.php/Front_End

[8] PSIAKI, Mark, Brady O'HANLON, Jashan BHATTI, Deniel SHEPARD a Todd HUMPREYS. GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals. *IEEE Transactions on Aerospace and Electronic Systems*. IEEE, 2013, (49), 2250 - 2267. DOI: 10.1109/TAES.2013.6621814.

[9] *Všeobecné oprávnění č. VO-R5/07.2005-18 k provozování uživatelských terminálů rádiových sítí standardů TETRA a TETRAPOL*. In: . Praha: Český telekomunikační úřad, 2005, číslo 18. Dostupné také z: https://www.ctu.cz/cs/download/vseobecna-opravneni/archiv/vo-r_05-07_2005-18.pdf

[10] *Plán přidělení kmitočtových pásem: Národní kmitočtová tabulka*. In: Praha: Český telekomunikační úřad, 2004. Dostupné také z: http://www.crk.cz/FILES/NKT.PDF

[11] Massive GPS Jamming Attack by North Korea. *GPS World* [online]. 2012 [cit. 2017-05-25]. Dostupné z: http://gpsworld.com/massive-gps-jamming-attack-by-north-korea/

[12] GPS Jammers. *5Gjammers.com* [online]. [cit. 2017-05-25]. Dostupné z: http://www.5gjammers.com/gps-jammers

[13] *DIY Trade: Global B2B Trading Platform* [online]. [cit. 2017-05-25]. Dostupné z: http://www.diytrade.com/

[14] UCLASS: Unmanned Carrier Launched Airborne Surveillance and Strike. *Lockheed Martin* [online]. [cit. 2017-05-25]. Dostupné z: http://www.lockheedmartin.com/us/products/uclass.html

[15] GNSS Simulator for the R&S SMBV100A Vector Signal Generator. *Rohde&Schwarz* [online]. [cit. 2017-05-25]. Dostupné z: https://www.rohde-schwarz.com/us/product/gnss-productstartpage_63493-11461.html

[16] *Interface Specification IS-GPS-200: Navstar GPS Spece Segment / Navigation User Interfaces*. Global Positioning Systems Directorate - Systems Engeneering & Integration, 2013.

[17] ERA has completed the SAT of its system deployed at Baku Airport. *ERA* [online]. 2014 [cit. 2017-05-25]. Dostupné z: http://old.era.aero/news/197/59/ERA-has-completed-the-SAT-of-its-system-deployed-at-Baku-Airport/

[18] BROWN, Alison, Jarrett REDD a Mark-Anthony HUTTON. Simulating GPS Signals: It Doesn't Have to Be Expensive. *GPS World* [online]. 2012 [cit. 2017-05-25]. Dostupné z: http://www.gpsworld.com/wp-content/uploads/2012/09/gpsworld_Innovation_0512.pdf

[19] *ROGER GNSS repeater* [online]. [cit. 2017-05-25]. Dostupné z: http://www.gps-repeating.com/

[20] *GPS Source: Oprations Enabled* [online]. [cit. 2017-05-25]. Dostupné z: https://www.gpssource.com/pages/all-products

[21] CAPARRA, Gianluca, Christian WULLEMS, Silvia CECCATO, Silvia STURARO, Nicola LAURENTI, Oscar POZZOBON, Rigas IOANNIDES a Massimo CRISCI. *Design Drivers and New Trends for Navigation Message Authentication Schemes for GNSS Systems* [online]. InsideGNSS, 2016, 64-73 [cit. 2017-05-26]. Dostupné z: http://www.insidegnss.com/auto/sepoct16-WP.pdf

[22] LEVIN, Peter, David S. DE LORENZO, Per K. ENGE a Shermen C. LO. *Authenticating a signal based on an unknown component thereof*. 2008. USA. US7969354 B2. Uděleno 28. července 2011. Zapsáno 2. února 2008.

[23] Receiver Autonomous Integrity Monitoring. W. PARKINSON, Bradford, Per ENGE, Penina AXELRAD, James J. SPILKER JR. a R. Grower BROWN. *Global Positioning System: Theory and Applications*. 2. Washington: American Institute of Aeronautics and Astronautics, 1996, s. 143-165. ISBN 978-1-56347-107-0.

[24] POZZOBON, Oscar. Keeping the Spoofs Out: Signal authentication Services for Future GNSS. *InsideGNSS* [online]. 2011, 48-55 [cit. 2017-05-25]. Dostupné z: http://www.insidegnss.com/auto/mayjune11-Pozzobon.pdf

[25] DANESHMAND, Saeed, Ali JAFARNIA - JAHROMI, Ali BROUMANDAN a Gérard LACHAPELLE. *A Low - Complexity GPS Anti - Spoofing Method Using a Multi - Antenna Array* [online]. ION GNSS, 2011 [cit. 2017-05-25]. Dostupné z: http://plan.geomatics.ucalgary.ca/papers/iongnss2012_sdaneshmand_26sep12.pdf

[26] BAUERNFEIND, R., T. KRAUS, A. SICRAMAZ AYAZ, D. DÖTTERBÖCK a B. EISSFELLER. *ANALYSIS, DETECTION AND MITIGATION OF INCAR GNSS JAMMER INTERFERENCE IN INTELLIGENT TRANSPORT SYSTEMS* [online]. Institute of Space Technology and Space Applications, University FAF Munich, Germany, 2012 [cit. 2017-05-25]. Dostupné z: http://www.dglr.de/publikationen/2013/281260.pdf

[27] BORIO, Danielle, Cillian O'DRISCOLL a Joaqim FORTUNY. *GNSS Jammers: Effects and countermeasures* [online]. Noordwijk, Netherlands: IEEE, 2013 [cit. 2017-05-25]. DOI: 10.1109/NAVITEC.2012.6423048. Dostupné z: http://ieeexplore.ieee.org/document/6423048/

[28] B. MONTMINY, Myrna. *Passive Geolocation of Low-Power Emitters in Urban Environments Using TDOA* [online]. Wright-Patterson Air Force Base, Ohio, 2007 [cit. 2017-05-25]. Dostupné z: www.dtic.mil/get-tr-doc/pdf?AD=ADA471571. Air Force Institute of Technology.

[29] PAGES-ZAMORA, A., J. VIDAL a D.H. BROOKS. Closed-form solution for positioning based on angle of arrival measurements. *Personal, Indoor and Mobile Radio Communications* [online]. Pavilhao Altantico, Lisboa, Portugal: IEEE, 2002 [cit. 2017-05-25]. DOI: 10.1109/PIMRC.2002.1045433. Dostupné z: http://ieeexplore.ieee.org/document/1045433/

[30] KRIZMAN, K.J., T.E. BIEDKA a T.S. RAPPAPORT. Wireless position location: fundamentals, implementation strategies, and sources of error. *Vehicular Technology Conference* [online]. Phoenix, AZ, USA: IEEE, 2002 [cit. 2017-05-25]. DOI: 10.1109/VETEC.1997.600463. Dostupné z: http://ieeexplore.ieee.org/document/600463/

[31] DOSHI, Bharat, Emre GUNDUZHAN, Jay CHANG a Osama FARRAG. Mobile geolocation techniques for location-aware emergency response services. *Military Communications Conference, MILCOM 2015* [online]. Tampa, FL, USA: IEEE, 2015 [cit. 2017-05-25]. DOI: 10.1109/MILCOM.2015.7357676. Dostupné z: http://ieeexplore.ieee.org/document/7357676/

[32] PIERCE, J.A. An Introduction to Loran. *IEEE AES Magazine* [online]. IEEE, 1990 [cit. 2017-05-25]. Dostupné z: http://ieeeghn.com/wiki/images/archive/7/70/20111005125450!Pierce_Loran.pdf

[33] RAPPAPORT, T.S., J.H. REED a B.D. WOERNER. Position location using wireless communications on highways of the future. *IEEE Communications Magazine* [online]. IEEE, 1996, (34), 33-41 [cit. 2017-05-25]. DOI: 10.1109/35.544321. Dostupné z: http://ieeexplore.ieee.org/document/544321/

[34] LINDSTRÖM, Jonas, Dennis AKOS, Oscar ISOZ a MArcus JUNERED. GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules. *Proceedings of the 20th International Technical Meeting of the Satellite Division of the Institute of Navigation* [online]. Fort Worth, Texas, 2007 [cit. 2017-05-26]. Dostupné z: https://www.diva-portal.org/smash/get/diva2:1011883/FULLTEXT01.pdf

[35] BARTOLUCCI, Marco, Roberta CASILE, Giovanni CORAZZA, Alessandro DURANTE, Giulio GABELLI a Alessandro GUIDOTTI. Cooperative/distributed localization and characterization of GNSS jamming interference. *Localization and GNSS (ICL-GNSS)* [online]. Turin, Italy: IEEE, 2013 [cit. 2017-05-26]. DOI: 10.1109/ICL-GNSS.2013.6577274. Dostupné z: http://ieeexplore.ieee.org/document/6577274/

[36] Roundup of Software Defined Radios. *RTL-SDR* [online]. 2014 [cit. 2017-05-25]. Dostupné z: http://www.rtl-sdr.com/roundup-software-defined-radios/

[37] HackRF One. *Great Scott Gadgets* [online]. 2016 [cit. 2017-05-25]. Dostupné z: https://greatscottgadgets.com/hackrf/

[38] JOHANSSON, Fredrik, Rahman MOLLAEI, Jonas THOR a Jorgen UUSITALO. *GPS Satellite Signal Acquisition and Tracking* [online]. 1998 [cit. 2017-05-25]. Dostupné z: http://www.sm.luth.se/csee/courses/sms/019/1998/navstar/navstar.pdf

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA 1

```
%% Harmonický signál:
freq = 1;
samplesperperiod = 100;
time = 0 : 1/samplesperperiod : 1-1/samplesperperiod;
I = sin(2*pi*freq*time);
Q = zeros(1,length(time));
IQ = I + 1i*Q;

%% Zobrazení vygenerovaného signálu:
figure(1);
hold on;
plot(time, real(IQ),'b')
plot(time, imag(IQ),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')

%% Formátování pro 1GB výstup:
multiplier = ones(1, 5000000);
I = kron(multiplier, I);
Q = kron(multiplier, Q);

%% Konverze dat do 8-bitového tvaru:
maxquant = 127;
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('harm1_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 2

```
%% Amplitudová modulace s harmonickou změnou amplitudy:
freq = 1;
samplesperperiod = 100;
time = 0 : 1/samplesperperiod : 1-1/samplesperperiod;
depth = 0.8;
I = 1+depth*sin(2*pi*freq*time);
Q = zeros(1,length(time));
IQ = I + 1i*Q;

%% Grafické znázornění:
figure(1);
hold on;
plot(time, real(IQ),'b')
plot(time, imag(IQ),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')

%% Formátování pro 1GB výstup:
multiplier = ones(1, 5000000);
I = kron(multiplier, I);
Q = kron(multiplier, Q);

%% Konverze dat do 8-bitového tvaru:
maxquant = 127/(1+depth);
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('am1_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 3

```
%% Fázová modulace s harmonickou změnou fáze:
freq = 1;
samplesperperiod = 100;
time = 0: 1/samplesperperiod : 1-1/samplesperperiod;
phasedev = pi;
I = cos(phasedev*sin(2*pi*freq*time));
Q = sin(phasedev*sin(2*pi*freq*time));
IQ = I + 1i*Q;

%% Grafické znázornění:
figure(1);
phi = phase(IQ);
plot(time,phi,'y')
xlabel('Čas')
ylabel('Okamžitá fázová odchylka')
figure(2);
hold on;
plot(time, real(IQ),'b')
plot(time, imag(IQ),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')

%% Formátování pro 1GB výstup:
multiplier = ones(1, 5000000);
I = kron(multiplier, I);
Q = kron(multiplier, Q);

%% Konverze dat do 8-bitového tvaru:
maxquant = 127;
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru
fid = fopen('pm1_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 4

```
%% Frekvenční modulace s harmonickou změnou kmitočtu:
freq = 1;
samplesperperiod = 100;
time = 0: 1/samplesperperiod : 1-1/samplesperperiod;
freqdev = 10;
beta = freqdev/freq;
I = cos(beta*sin(2*pi*freq*time));
Q = sin(beta*sin(2*pi*freq*time));
IQ = I + 1i*Q;

%% Grafické znázornění:
figure(1);
hold on;
plot(time, real(IQ),'b')
plot(time, imag(IQ),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')

%% Formátování pro 1GB výstup:
multiplier = ones(1, 5000000);
I = kron(multiplier, I);
Q = kron(multiplier, Q);

%% Konverze dat do 8-bitového tvaru:
maxquant = 127;
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('fm1_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 5

```
%% Chirp signál I:
sweeptime = 1;
samplespersweep = 1000;
sweeprange = 25;
time = 0 : 1/samplespersweep : sweeptime-1/samplespersweep;
I = chirp(time, 0, sweeptime-1/samplespersweep, sweeprange, 'linear',
0);
Q = chirp(time, 0, sweeptime-1/samplespersweep, sweeprange, 'linear',
90);
Ipulsecycle = [I I I I I];
Qpulsecycle = [Q Q Q Q Q];
pulse = I + 1i*Q;
pulsecycle = [pulse pulse pulse pulse];

%% Zobrazení vygenerovaného signálu:
figure(1);
hold on;
plot((1 : length(pulsecycle))/samplespersweep, real(pulsecycle),'b')
plot((1 : length(pulsecycle))/samplespersweep, imag(pulsecycle),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')
axis tight;

%% Formátování pro 1GB výstup:
multiplier = ones(1, 100000);
I = kron(multiplier, Ipulsecycle);
Q = kron(multiplier, Qpulsecycle);

%% Konverze dat do 8-bitového tvaru:
maxquant = 127;
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Prevod do tvaru pro SDR
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru
fid = fopen('chirp1_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 6

```
%% Chirp signál II:
sweeptime = 1;
samplespersweep = 1000;
sweeprange = 50;
time = 0 : 1/samplespersweep : sweeptime-1/samplespersweep;
I = chirp(time, -sweeprange/2, sweeptime-1/samplespersweep,
sweeprange/2, 'linear', 0);
Q = chirp(time, -sweeprange/2, sweeptime-1/samplespersweep,
sweeprange/2, 'linear', 90);
Ipulsecycle = [I I];
Qpulsecycle = [Q Q];
pulse = I + 1i*Q;
pulsecycle = [pulse pulse pulse pulse];

%% Zobrazení vygenerovaného signálu:
figure(1);
hold on;
plot((1 : length(pulsecycle))/samplespersweep, real(pulsecycle),'b')
plot((1 : length(pulsecycle))/samplespersweep, imag(pulsecycle),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')
axis tight;

%% Formátování pro 1GB výstup:
multiplier = ones(1, 250000);
I = kron(multiplier, Ipulsecycle);
Q = kron(multiplier, Qpulsecycle);

%% Konverze dat do 8-bitového tvaru:
maxquant = 127;
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('chirp2_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 7

```
%% Impulsní signál I:
pulsewidth = 1;
samplesperpulse = 1000;
freq = 10;
pulseperiod = 2*pulsewidth;
time = 0 : 1/samplesperpulse : pulsewidth-1/samplesperpulse;
I = cos(2*pi*freq*time);
Q = sin(2*pi*freq*time);

%% Vytvoření pulsní formy signálu:
gaptime = 0 : 1/samplesperpulse : pulseperiod-pulsewidth-
1/samplesperpulse;
gap = zeros(1, length(gaptime));
Ipulsecycle = [gap I gap I];
Qpulsecycle = [gap Q gap Q];
pulse = I + 1i*Q;
pulsecycle = [gap pulse gap pulse];

%% Zobrazení vygenerovaného signálu:
figure(1);
hold on;
plot((1 : length(pulsecycle))/samplesperpulse, real(pulsecycle),'b')
plot((1 : length(pulsecycle))/samplesperpulse, imag(pulsecycle),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')
axis tight;

%% Formátování pro 1GB výstup:
multiplier = ones(1, 125000);
I = kron(multiplier, Ipulsecycle);
Q = kron(multiplier, Qpulsecycle);

%% Konverze dat do 8-bitového tvaru:
maxquant = 127;
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('pulse1_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 8

```
%% Impulsní signál II:
pulsewidth = 1;
samplesperpulse = 1000;
sweeprange = 25;
pulseperiod = 2*pulsewidth;
time = 0 : 1/samplesperpulse : pulsewidth-1/samplesperpulse;
I = chirp(time, 0, pulsewidth-1/samplesperpulse, sweeprange, 'linear',
0);
Q = chirp(time, 0, pulsewidth-1/samplesperpulse, sweeprange, 'linear',
90);

%% Vytvoření pulsní formy signálu:
gaptime = 0 : 1/samplesperpulse : pulseperiod-pulsewidth-
1/samplesperpulse;
gap = zeros(1, length(gaptime));
Ipulsecycle = [gap I gap I];
Qpulsecycle = [gap Q gap Q];
pulse = I + 1i*Q;
pulsecycle = [gap pulse gap pulse];

%% Zobrazení vygenerovaného signálu:
figure(1);
hold on;
plot((1 : length(pulsecycle))/samplesperpulse, real(pulsecycle),'b')
plot((1 : length(pulsecycle))/samplesperpulse, imag(pulsecycle),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')
axis tight;

%% Formátování pro 1GB výstup:
multiplier = ones(1, 125000);
I = kron(multiplier, Ipulsecycle);
Q = kron(multiplier, Qpulsecycle);

%% Konverze dat do 8-bitového tvaru:
maxquant = 127;
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('pulse2_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 9

```
%% Signál rozprostřený frekvenčními skoky:
samplesperperiod = 120;
t = 0 : 2*pi/samplesperperiod : 2*pi-1/samplesperperiod;% Nosný signál
samplesperperiod1 = 10;
t1 = 0 : 2*pi/samplesperperiod1 : 2*pi-1/samplesperperiod1; % Subnosná
č. 1
samplesperperiod2 = 20;
t2 = 0 : 2*pi/samplesperperiod2 : 2*pi-1/samplesperperiod2; % Subnosná
č. 2
samplesperperiod3 = 30;
t3 = 0 : 2*pi/samplesperperiod3 : 2*pi-1/samplesperperiod3; % Subnosná
č. 3
samplesperperiod4 = 40;
t4 = 0 : 2*pi/samplesperperiod4 : 2*pi-1/samplesperperiod4; % Subnosná
č. 4
samplesperperiod5 = 60;
t5 = 0 : 2*pi/samplesperperiod5 : 2*pi-1/samplesperperiod5; % Subnosná
č. 5
samplesperperiod6 = 120;
t6 = 0 : 2*pi/samplesperperiod6 : 2*pi-1/samplesperperiod6; % Subnosná
č. 6

%% Vygenerování datové zprávy:
message = round(rand(1, 10));
minusones = -1 * ones(1, length(t));
plusones = +1 * ones(1, length(t));
data = [];
for i = 1:(length(message))
    if message(1, i) == 0
        data = [data minusones];
    else
        data = [data plusones];
    end
end

%% Nosný signál:
period = cos(t);
carrier = kron(ones(1, length(message)), period);

%% Subnosné signály:
period1 = cos(t1);
subcarrier1 = kron(ones(1, 12), period1);
period2 = cos(t2);
subcarrier2 = kron(ones(1, 6), period2);
period3 = cos(t3);
subcarrier3 = kron(ones(1, 4), period3);
period4 = cos(t4);
subcarrier4 = kron(ones(1, 3), period4);
period5 = cos(t5);
subcarrier5 = kron(ones(1, 2), period5);
period6 = cos(t6);
subcarrier6 = kron(ones(1, 1), period6);
```

```
%% Vygenerování signálu s frekvenčními skoky:
spreadingsignal = [];
for i = 1 : length(message);
    carrierselect = randi(6,1); % Náhodný výběr nosné
    switch(carrierselect)
        case(1)
            spreadingsignal = [spreadingsignal subcarrier1];
        case(2)
            spreadingsignal = [spreadingsignal subcarrier2];
        case(3)
            spreadingsignal = [spreadingsignal subcarrier3];
        case(4)
            spreadingsignal = [spreadingsignal subcarrier4];
        case(5)
            spreadingsignal = [spreadingsignal subcarrier5];
        case(6)
            spreadingsignal = [spreadingsignal subcarrier6];
    end
end

%% Modulace:
bpsksignal = data.*carrier;
fhsssignal = bpsksignal.*spreadingsignal;

%% Zobrazení signálu
figure(1);
hold on;
plot(0:1/length(fhsssignal):1-1/length(fhsssignal),
real(fhsssignal),'b')
plot(0:1/length(fhsssignal):1-1/length(fhsssignal),
imag(fhsssignal),'g')
xlabel('Čas')
ylabel('Amplituda')
legend('I','Q')

%% Formátování pro 1GB výstup:
multiplier = ones(1, 400000);
I = kron(multiplier, fhsssignal);
Q = zeros(1, length(I));

%% Konverze dat do 8-bitového tvaru:
maxquant = 127;
I = I*maxquant;
Q = Q*maxquant;
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i)= Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('hopping1_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

PŘÍLOHA 10

```
%% Vygenerovaní C/A kódu konkrétní družice:
function PRN = prngen1(satellite, samplerate)

%% Inicializační naplnění registrů:
G1shift = ones(1,10);
G2shift = ones(1,10);

%% Maska zpětné vazby:
G1mask = [0 0 1 0 0 0 0 0 0 1]';
G2mask = [0 1 1 0 0 1 0 1 1 1]';

%% Výstupní pozice registru G2:
G2outmask = zeros(10, 37);
G2outmask([2, 6], 1) = 1; % PRN = 1
G2outmask([3, 7], 2) = 1; % PRN = 2
G2outmask([4, 8], 3) = 1; % PRN = 3
G2outmask([5, 9], 4) = 1; % PRN = 4
G2outmask([1, 9], 5) = 1; % PRN = 5
G2outmask([2, 10], 6) = 1; % PRN = 6
G2outmask([1, 8], 7) = 1; % PRN = 7
G2outmask([2, 9], 8) = 1; % PRN = 8
G2outmask([3, 10], 9) = 1; % PRN = 9
G2outmask([2, 3], 10) = 1; % PRN = 10
G2outmask([3, 4], 11) = 1; % PRN = 11
G2outmask([5, 6], 12) = 1; % PRN = 12
G2outmask([6, 7], 13) = 1; % PRN = 13
G2outmask([7, 8], 14) = 1; % PRN = 14
G2outmask([8, 9], 15) = 1; % PRN = 15
G2outmask([9, 10], 16) = 1; % PRN = 16
G2outmask([1, 4], 17) = 1; % PRN = 17
G2outmask([2, 5], 18) = 1; % PRN = 18
G2outmask([3, 6], 19) = 1; % PRN = 19
G2outmask([4, 7], 20) = 1; % PRN = 20
G2outmask([5, 8], 21) = 1; % PRN = 21
G2outmask([6, 9], 22) = 1; % PRN = 22
G2outmask([1, 3], 23) = 1; % PRN = 23
G2outmask([4, 6], 24) = 1; % PRN = 24
G2outmask([5, 7], 25) = 1; % PRN = 25
G2outmask([6, 8], 26) = 1; % PRN = 26
G2outmask([7, 9], 27) = 1; % PRN = 27
G2outmask([8, 10], 28) = 1;% PRN = 28
G2outmask([1, 6], 29) = 1; % PRN = 29
G2outmask([2, 7], 30) = 1; % PRN = 30
G2outmask([3, 8], 31) = 1; % PRN = 31
G2outmask([4, 9], 32) = 1; % PRN = 32
G2outmask([5, 10], 33) = 1; % PRN = 33
G2outmask([4, 10], 34) = 1; % PRN = 34
G2outmask([1, 7], 35) = 1; % PRN = 35
G2outmask([2, 8], 36) = 1; % PRN = 36
G2outmask([4, 10], 37) = 1; % PRN = 37
```

```
%% Vlastní generování:
for i = 1:1023
    G1out(i) = G1shift(10);
    G2jout = mod(G2shift * G2outmask(:,satellite), 2);
    G1shift = [mod(G1shift * G1mask, 2), G1shift(1:9)];
    G2shift = [mod(G2shift * G2mask, 2), G2shift(1:9)];
    PRN(i) = xor(G1out(i), G2jout);
end

%% Převzorkování na specifický vzorkovací kmitočet:
if samplerate ~= 1
    count = 0;
    for sample = 1/samplerate : 1/samplerate : 1023
        count = count + 1;
        if ceil(sample) > 1023
            PRNconverted(:, count) = PRN(:, 1023);
        else
            PRNconverted(:, count) = PRN(:, ceil(sample));
        end
    end
    PRN = PRNconverted;
end
PRN = 1 - 2.*PRN;
end
```

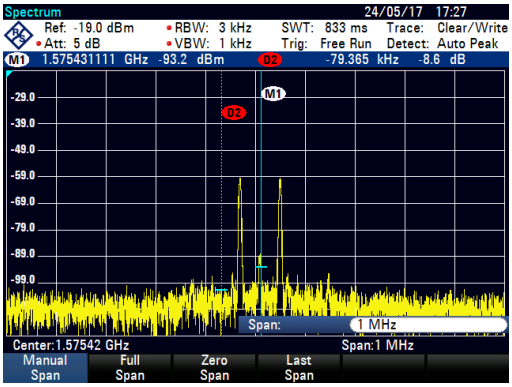
PŘÍLOHA 11

```
%% Inteligentní signál I:
satellite = 8;
samplerate = 1;
PRN = prngen1(satellite,samplerate);
Ns = 8;
PRN = upsample(PRN, Ns);

%% Formátování pro 1GB výstup:
multiplier = ones(1, 900);
sequence = kron(multiplier, PRN);

%% Modulace náhodné zprávy:
message = rand(1, 100);
message = 1 - 2.*round(message);
data = kron(message, sequence);
pulse = rcosine(1,Ns);
Q = conv(pulse, data);
I = zeros(1, length(Q));

%% Konverze dat do 8-bitového tvaru:
maxquant = 127/(max(Q));
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(I);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('semispoofing1_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

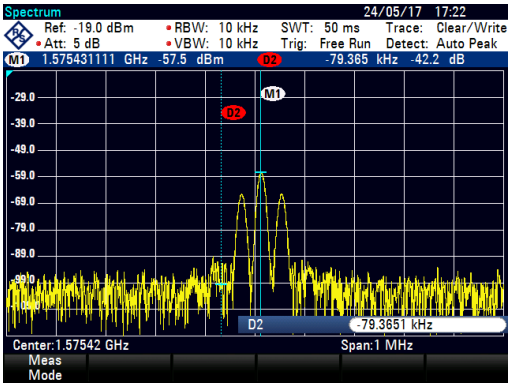
PŘÍLOHA 12

```
%% Inteligentní signál II:
for i = 1:37
PRNtable(i,:) = prngen1(i,1);
end
Ns = 8;
for i = 1:37
PRNupsampled(i,:) = upsample(PRNtable(i,:), Ns);
end

%% Formátování pro 1GB výstup:
multiplier = ones(1, 16);
for i = 1:37
PRNsequence(i,:) = kron(multiplier, PRNupsampled(i,:));
end

%% Modulace náhodné zprávy:
message = rand(1, 100);
message = 1 - 2.*round(message);
for i = 1:37
data(i,:) = kron(message, PRNsequence(i,:));
end

%% Sekvence všech dostupných C/A kódů:
datastream =
[data(1,:),data(2,:),data(3,:),data(4,:),data(5,:),data(6,:),data(7,:)
,data(8,:),data(9,:),data(10,:),data(11,:),data(12,:),data(13,:),data(
14,:),data(15,:),data(16,:),data(17,:),data(18,:),data(19,:),data(20,:
),data(21,:),data(22,:),data(23,:),data(24,:),data(25,:),data(26,:),da
ta(27,:),data(28,:),data(29,:),data(30,:),data(31,:),data(32,:),data(3
3,:),data(34,:),data(35,:),data(36,:),data(37,:)];
pulse = rcosine(1,Ns);
Q = conv(pulse, datastream);
I = zeros(1, length(Q));

%% Konverze dat do 8-bitového tvaru:
maxquant = 127/(max(Q));
I = I*maxquant;
Q = Q*maxquant;
I = round(I, 0);
Q = round(Q, 0);
I = int8(I);
Q = int8(Q);

%% Převod do tvaru pro SDR:
N = length(Q);
for i = 1:N
    IQ(1,2*i-1) = I(1,i);
    IQ(1,2*i) = Q(1,i);
end

%% Vygeneorvání .bin souboru:
fid = fopen('semispoofing2_8bit.bin', 'w');
fwrite(fid, IQ, 'int8');
fclose(fid);
```

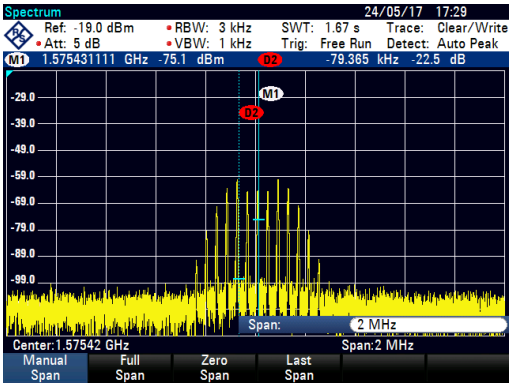
PŘÍLOHA 13



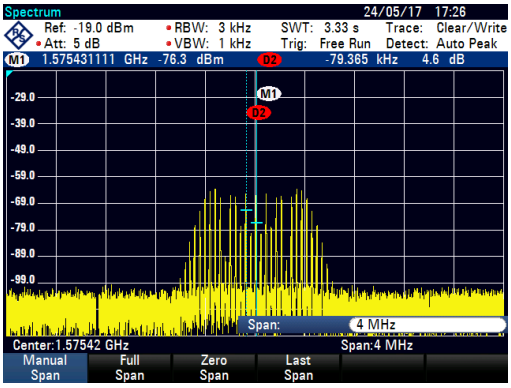
Harmonický signál



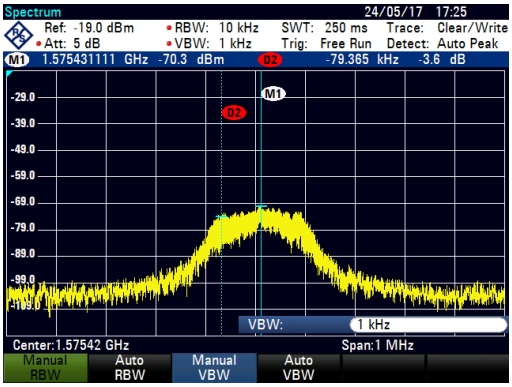
Amplitudově modulovaný signál



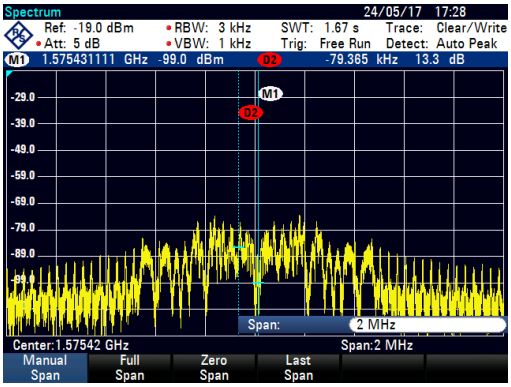
Fázově modulovaný signál



Frekvenčně modulovaný signál



Chirp signál II



Signál rozprostřený frekvenčními skoky