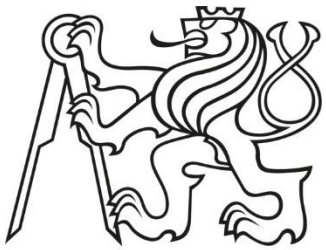


ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Martin Dostál

PROBLEMATIKA ZÁMĚRNÉHO OVLIVŇOVÁNÍ FUNKCE GNSS PŘIJÍMAČE

Bakalářská práce

2016

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
d ě k a n
Konviktská 20, 110 00 Praha 1

K616.....**Ústav dopravních prostředků**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Martin Dostál

Kód studijního programu a studijní obor studenta:

B 3710 – ITS – Inteligentní dopravní systémy

Název tématu (česky): **Problematika záměrného ovlivňování funkce GNSS přijímače**

Název tématu (anglicky): Problems of intentional degradation of performance of GNSS receivers

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte osnovou uvedenou v následujících bodech:

- prozkoumejte existující způsoby ovlivnění správné funkce GNSS přijímače
- definujte vhodné parametry definující „správnou funkci" GNSS přijímače
- práci koncipujte se zaměřením na užití v oblasti veřejné osobní dopravy
- prozkoumejte možnosti ochrany vůči zjištěným způsobům ovlivnění
- navrhněte eliminaci nebo snížení míry rizika použitím nalezených způsobů ochrany
- navrhněte doporučení pro využití GNSS v typických aplikacích pro oblast veřejné osobní dopravy

Rozsah grafických prací: dle pokynů vedoucího práce

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

Seznam odborné literatury:

Humphreys, T. E. et all, The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment, Proceedings of ION GNSS, 2010.

Hofmann-Wellenhof, B. et all, GNSS: GPS, GLONASS, Galileo and More, Springer, 2008.

Groves, P. D., Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, 2008.

Vedoucí bakalářské práce: **Ing. Milan Sliacky**

Datum zadání bakalářské práce: **15. června 2015**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání bakalářské práce: **25. srpna 2016**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

doc. Ing. Petr Bouchner, Ph.D.
vedoucí
Ústavu dopravních prostředků

prof. Dr. Ing. Miroslav Svítek, dr. h. c.
děkan fakulty

Potvrzuji převzetí zadání bakalářské práce.

Martin Dostál
jméno a podpis studenta

V Praze dne ..... 15. června 2015

Poděkování

Děkuji panu Ing. Milanu Sliackemu za jeho věnovaný čas, odborné vedení a konzultování práce. Dále bych rád poděkoval panu Ing. Petrovi Kačmaříkovi Ph.D. z firmy AŽD Praha s.r.o. za jeho cenné přípomínky.

Prohlášení

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

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 24. srpna 2016

Martin Dostál

Název práce: Problematika záměrného ovlivňování funkce GNSS přijímače

Autor: Martin Dostál

Obor: Inteligentní dopravní systémy

Druh práce: Bakalářská práce

Vedoucí práce: Ing. Milan Sliacky

Ústav dopravních prostředků K616

Fakulta dopravní

České vysoké učení technické v Praze

Abstrakt

Globální satelitní navigace je čím dál více využívána v civilní infrastruktuře, veřejnou dopravu nevyjímaje. Byla zjištěna řada případů, kdy byly přijímače satelitní navigace neschopny příjmu signálu díky jednoduchým, levným rušičkám. Dále existují i způsoby jak přijímač donutit určovat nesprávnou polohu vysíláním útočníkem vytvořeného signálu. Předmětem této práce je analýza způsobů záměrného negativního ovlivňování přijímačů globálních satelitních navigací, ochran proti těmto ovlivněním a následné uvedení základních doporučení pro vybrané aplikace ve veřejné dopravě.

Klíčová slova

GNSS, GPS, Galileo, GLONASS, přijímač, GNSS signál, rušení, rušička, spoofing, PPD, veřejná doprava

Title: Problems of intentional degradation of performance of GNSS receivers

Author: Martin Dostál

Study program: Intelligent transport systems

Document: Bachelor thesis

Supervisor: Ing. Milan Sliacky

Department of Vehicle Technology K616

Faculty of Transportation Sciences

Czech Technical University in Prague

Abstract

Global navigation satellite systems are becoming deeply ingrained in civil infrastructure, including public transportation systems. Events have been registered, where GNSS receivers were rendered unable to receive the signal from a satellite due to the jamming by simple, inexpensive, off the shelf jammers. There are ways of forging a signal similiar to the original one which causes the receiver to give incorrect navigational solution. The goal of this thesis is to analyse existing means, through which a potential attacker can degrade performance of GNSS receivers, to analyse existing defenses against such activities and to create basic recommendations for public transportation applications of GNSS.

Klíčová slova

GNSS, GPS, Galileo, GLONASS, receiver, GNSS signal, jamming, jammer, spoofing, PPD, public transport

Obsah

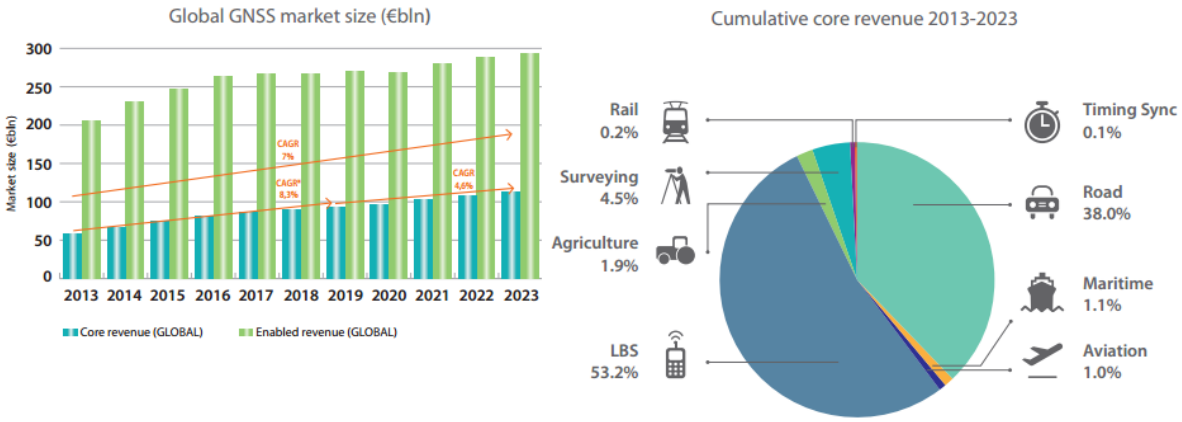
1 Seznam použitých zkratek

ADC	Analog to digital converter
ADS-B	Automatic dependent surveillance - broadcast
AGC	Automatic gain control
AVV	Automatické vedení vlaku
BLWN	Band limited white noise
BOC	Binary offset carrier modulation
BPSK	Binary phase-shift keying
CDMA	Code division multiple acces
C/N	Carrier to noise
CS	Commercial service (Galileo)
CW	Continuous wave
EGNOS	European geostationary navigation overlay service
ETCS	European train control system
FAA	Federal aviation administration
FDMA	Frequency division multiple acces
FPGA	Field programmable gate array
GBAS	Ground based augmentation system
GIB	Geodetické informační body
GLONASS	Globalnaja navigacionnaja sputnikovaja sistěma
GNSS	Global navigation satellite system
GPS	Global positioning system
GSA	European global navigation satellite systems agency
GSM-R	Global system for mobile communications - Railway
IFR	Instrument flight rules
ILS	Instrument landing system
IMU	Inertial measurment unit
INS	Inertial navigation system

ITU	International telecommunication union
J/S	Jammer to signal ratio
LBS	Location based service
LHCP	Left hand circular polarization
MBOC	Multiplexed binary offset carrier
MEO	Medium Earth orbit
MHD	Městská hromadná doprava
MIB	Magnetický informační bod
NMA	Navigation messsage authentication
OS	Open service (Galileo)
PPD	Personal privacy device
PRN	Pseudorandom noise
PVT	Position velocity time
QPSK	Quadrature phase-shift keying
QZSS	Quasi-Zenith Satellite System
RHCP	Right hand circular polarization
RNSS	Radio navigation satellite services
SCE	Spreading code encryption
SNR	Signal to noise ratio
SSZ	Světelné signalizační zařízení
VFR	Visual flight rules
VOR	VHF omnidirectional range
XOR	Exclusive OR

2 Úvod

Global navigation satellite system (GNSS) umožňuje uživateli určit jeho polohu a jeho rychlost vůči danému referenčnímu rámci (Zemi). Všechny fungující systémy, i ty ve vývoji, jsou koncipovány na základě dálkoměrného zjištění polohy uživatele. V provozu je nyní americký NAVSTAR GPS a ruský GLONASS. Oba systémy jsou si velmi podobné a oba jsou vojenské systémy, jejichž služba je pouze zpřístupněna široké veřejnosti. Evropská unie vyvíjí svůj vlastní navigační systém Galileo, který se liší od výše jmenovaných tím, že není koncipován primárně jako vojenský, nýbrž jako komerční. Přístup ke službě OS systému Galileo bude mít každý (obdobně jako u GPS a GLONASS). Pokud bude uživatel požadovat lepší službu, bude mít možnost si ji koupit (služba CS). Toto u GPS a GLONASS není možné, neboť lepší služby jsou u těchto vyhrazeny pro vlastní armády.



Obrázek 1 - Obrat a složení trhu s GNSS přijímači [1]

Na obrázku 1 je vidět velikost trhu (v € miliardách) s GNSS přijímači a jeho prognóza na příští léta. Modře je znázorněna cena GNSS chipsetů v zařízeních, zeleně je znázorněna cena zahrnující celkovou cenu GNSS zařízení. Na grafu vpravo je znázorněno rozdělení trhu. Největší díl zabírají LBS (Location Based Services) většinou využívané mobilními telefony. Nasledovány jsou silničními navigacemi. V železničních aplikacích zatím nejsou systémy GNSS zastoupeny velkou měrou, existuje ale spousta pilotních programů na otestování využití satelitních navigací v kolejové dopravě.

Dle posledního průzkumu trhu s GNSS přijímači agentury GSA z roku 2015 [1] existuje na Zemi 3.6 miliard GNSS zařízení. Toto číslo by se mělo postupně zvyšovat až k sedmi miliardám v roce 2019.

S rostoucím užitím GNSS v různých aplikacích dopravní infrastruktury rostou i potenciální škody způsobené útokem na slabý a nechráněný signál civilních služeb GNSS. Cílem této práce je vytvořit základní přehled o civilních GNSS signálech, o složitosti a možnostech jejich

zarušení či duplikování. V první části práce je popsána architektura signálu a základní principy fungování GNSS přijímače. V následujících částech jsou uvedeny způsoby záměrného ovlivnění signálu GNSS a existující mechanismy na zmírnění následků takovýchto útoků. V poslední části práce jsou doporučení pro vybrané okruhy veřejné dopravy.

3 GNSS signál a přijímače

V této kapitole je popsána architektura civilních GNSS signálů, včetně používaných modulací, a služby poskytované různými konstelacemi. Dále jsou zde uvedeny veličiny užívané k popisu síly či kvality signálu.

3.1.1 Síla signálu

Pro vyjádření poměru výkonu dvou signálů se používají jejich poměry na logaritmické škále. Tato je definovaná následovně:

$$n = 10log_{10}\frac{P_p}{P_v}\ [dB]\ (1.1)\ [2]$$

Označíme-li sílu signálu zachycovanou přijímačem jako P_p a sílu signálu vysílaného jako P_v, bude *n* nabývat hodnot n > 0 pro zisk signálu a naopak *n* < 0 pro útlum vysílaného signálu.

Výše uvedené jednotky jsou bezrozměrné a pro vyjádření absolutní hodnoty síly signálu nevhodné. Často se z tohoto důvodu používají jednotky vztažené k nějaké referenční hodnotě, například k wattu [dBW] nebo k miliwattu [dBm]. Předešlý vztah se pak jen upraví na takovýto tvar.

$$n = 10log_{10}\frac{P_p}{1[W]}\ [dBW]\ (1.2)\ [2]$$

Protože satelity GNSS obíhají Zemi v relativně velké vzdálenosti na středně oběžných drahách (MEO), signál, který doletí na zemský povrch, má negativní SNR, neboť má výkon okolo -130 dBm (10^-16 W), a tak se nachází přibližně 26dB pod hladinou okolního šumu. Signál může být díky použití kódového multiplexu a typického zisku GNSS přijímače 40 dB „vyextrahován“ z okolního šumu. [2]

Výkonovou bilanci spoje družice – přijímač lze popsat Friisovou (komunikační) rovnicí:

$$\frac{P_p}{P_v} = G_v G_p \left(\frac{\lambda}{4\pi r}\right)^2\ (1.3)\ [4]$$

Zde G_v a G_p jsou zisky antén vysílače, respektive přijímače. Kvadratický člen zastupuje ztráty způsobené šířením přímé elektromagnetické vlny v prostoru. Vzdálenost mezi vysílačem a přijímačem je označena jako r, vlnová délka nosné vlny jako λ.

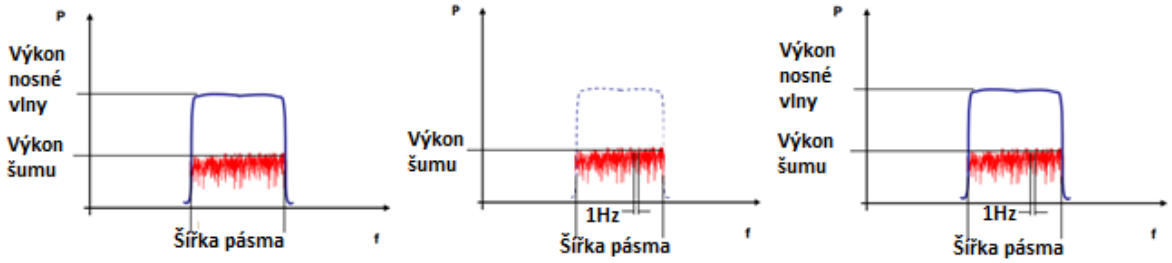
3.1.2 Kvalita signálu

Jedním z používaných ukazatelů kvality a síly signálu je podíl síly užitečného signálu k šumu (SNR). Tento podíl se používá k vyjádření kvality signálu v základním pásmu (nemodulovaného). Při užívání SNR je nutné definovat šířku pásma, pro kterou poměr platí, neboť výkon šumu roste se zvětšující se šířkou pásma.

$$SNR = \frac{P_{signál}}{P_{šum}} \qquad SNR_{dB} = 10\log\left(\frac{P_{signál}}{P_{šum}}\right) \quad (1.4)$$

Výše uvedené vztahy definují SNR jako bezrozměrnou veličinu respektive vyjádřenou v dB. [5]

Pro kvalitu modulovaného signálu na přenosovém médiu, který přijímá anténa přijímače, se užívá poměr výkonu nosné vlny k šumu v dané šířce pásma označovaný C/N. Spektrální hustota šumu, definována jako množství energie šumu na jednotku pásma [Hz], bývá značena jako N_0. Jako jednotky jsou většinou používány [Watt/Hz]. Posledním zmiňovaným podílem je výkon nosné vlny ke spektrální hustotě šumu, označována jako C/N_0, s jednotkou decibel na hertz [dB-Hz]. [6] Dále se v literatuře, zabývající se rušením signálu, používá poměr J/S – poměr výkonu rušícího a užitečného signálu.



Obrázek 2 – Zleva znázornění C/N, No, C/No [6]

3.2 Metody multiplexování pro vícenásobný přístup

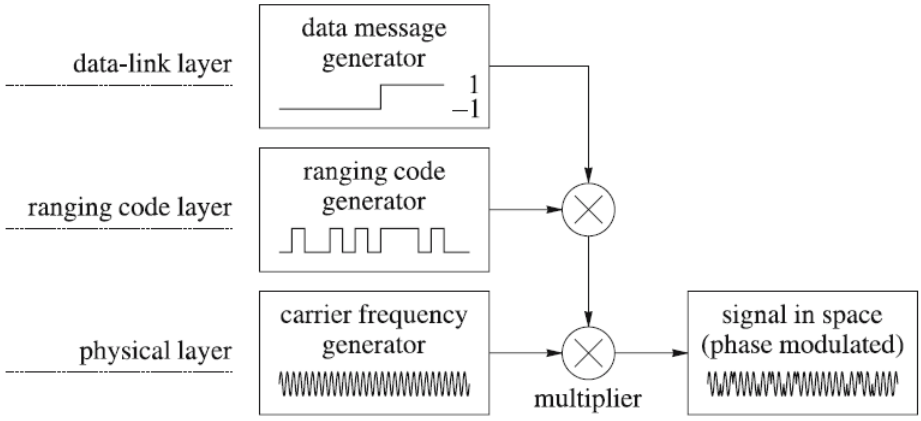
Neboť k určení polohy uživatelského přijímače je potřeba minimální počet 4 satelitů, využívají satelitní konstelace techniky sdílení přenosového kanálu, aby se zabránilo vzájemné interferenci mezi satelity vysílanými signály. Satelitní systémy GPS a Galilea používají techniku kódového multiplexu (CDMA, dále popsán v 3.3.2), aby mohl přijímač rozpoznat jednotlivé signály vysílané na jedné nosné frekvenci. [3] V systému GLONASS byla a dodnes i je používána technika frekvenčního multiplexu (FDMA). FDMA využívá spektrálního oddělení nosných vln pro různé satelity. Výhodou byla zvýšená odolnost systému proti rušení v úzkém pásmu – útočník takto mohl zarušit pouze omezený počet satelitů. V posledních letech ale GLONASS přechází také na CDMA, neboť FDMA již neposkytuje výhodu zvýšené robustnosti vůči úzkopásmé interferenci díky vývoji v rušící technice a také kvůli zvýšení interoperability s ostatními GNSS. [7]

3.3 Struktura signálu

Signál vysílaný satelitem užívajícím CDMA lze popsat jako:

$$s(t) = \sqrt{2P}d(t)c(t)\cos(2\pi ft) \quad (1.5)$$ [3]

kde P představuje výkon signálu (člen sqrt(2P) zastupuje amplitudu), d(t) je navigační datová zpráva, c(t) je PRN kód modulovaný na nosnou frekvenci a f je frekvence nosné vlny.



Obrázek 3 -- Struktura GNSS signálu, odshora: datová zpráva, PRN kód, nosná frekvence [3]

Na obrázku 3 je schéma signálu, který vysílá jeden satelit. V dalším textu jsou rozebrány jednotlivé vyobrazené stavební bloky. K popisu základní architektury signálu budu používat jako příklad civilní signál GPS L1 C/A.

3.3.1 Navigační zpráva

Navigační zpráva, také nazývaná datová, je posloupnost dvou hodnot („1“ a „-1“) uspořádaná do rámců, které obsahují informace potřebné pro výpočet PVT přijímače. Data, která navigační zpráva obsahuje, jsou do družic nahrávána z nahrávacích stanic pozemního segmentu. Navigační zpráva má svou strukturu, pro každou službu odlišnou (např. C/A a L2C). Integrita (míra důvěryhodnosti, viz 3.6) zprávy je kontrolována pozemní infrastrukturou. Mezi data, které navigační zpráva obsahuje, patří:

- stav družice a její funkčnost (Health status)
- efemeridy satelitu – parametry dráhy družice
- parametry ionosférického modelu – lom radiového signálu je jedním z největších původců nepřesností určení polohy uživatele. Proto se vysílají korekce pro GNSS přijímače.

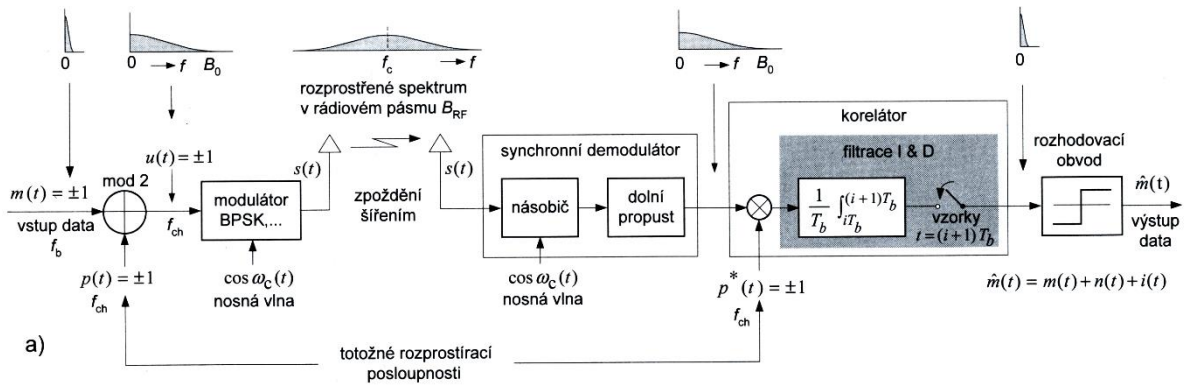
- korekce pro hodiny na palubě satelitu – odchylky palubních atomových hodin jsou sledovány pozemním segmentem GNSS a korekce pro jejich odchylky následně samotným satelitem vysílány.
- Almanach konstelace – obsahuje parametry (méně přesné než efemeridy samotného satelitu) efemerid ostatních satelitů v kosmickém segmentu. To umožňuje uživatelskému přijímači rychlejší zachycení signálů jím právě viditelných družic a tím rychlejší určení jeho polohy. [8]

3.3.2 CDMA a PRN

CDMA, známé také jako kódový multiplex je způsob vysílání, kdy několik uživatelů, vysílajících na stejném kanálu, používá různé rozprostírací kódy k rozprostření vysílání na širší přenosové pásmo. V případě GNSS jsou jako rozprostírací kódy používány PRN sekvence. PRN kód je pseudonáhodná, opakující se, deterministickým algoritmem generovaná sekvence chipů (neobsahují „informaci“ jako v případě datové zprávy) – jedniček a nul, která vykazuje statistické chování podobné šumu. Termín chip je v tomto kontextu používán pro rozlišení datových bitů, nesoucích data navigační zprávy a chipů, sekvence hodnot rozprostírajících navigační zpráv na širší frekvenční pásmo. Každý satelit patřící do konstelace má svůj přidělený kód, který ho odlišuje od ostatních družic vysílajících na stejné frekvenci. PRN kódy přidělené jednotlivým satelitům mají co nejmenší vzájemnou korelaci. Porovnáváním v přijímači lokálně generovaného PRN kódu s přijatým signálem je také GNSS přijímač schopen určit čas letu signálu od družice k přijímači (tím tedy určit pseudovzdálenost mezi ním a daným satelitem). [9]

Rozprostírací kód C/A má frekvenci 1,023 MHz, jedna epocha (perioda) má 1023 chipů a ta tedy trvá 1 ms. Bitová rychlost datové zprávy je 50 bps. Na jeden bit datové zprávy tedy připadá 20 epoch. [10]

Datová (navigační) zpráva se násobí pomocí logické operace XOR (exclusive OR) s PRN kódem. Díky mnohem vyššímu bitrate PRN kódu se datová zpráva rozprostře na mnohem širší vysílací pásmo (2 MHz v případě C/A na L1). Schéma CDMA je na obrázku 4, s jediným rozdílem – na obrázku se PRN kód s datovou zprávou násobí funkcí modulo-2, u GPS je použita funkce XOR. [10]



Obrázek 4 - Schéma CDMA s modulací BPSK [11]

Pro příklad mějme datovou sekvenci [0 1 0 1] kterou rozprostíráme pomocí kódu [1 0 0 1] (jedna epocha rozprostíracího kódu). Výsledný signál bude vypadat takto: 1001 0110 1001 0110. Vidíme, že se nám takto značně zvýšil rozsah hodnot – z 0 je 1001 atd. Dle Shannonova teorému se tedy při konstantním výkonu vysílání musí zvýšit vysílací pásmo. Vysílaný signál je velmi podobný bílému šumu. Pro úspěšnou demodulaci signálu potřebuje přijímač znát daný rozprostírací kód (v našem případě PRN sekvenci).

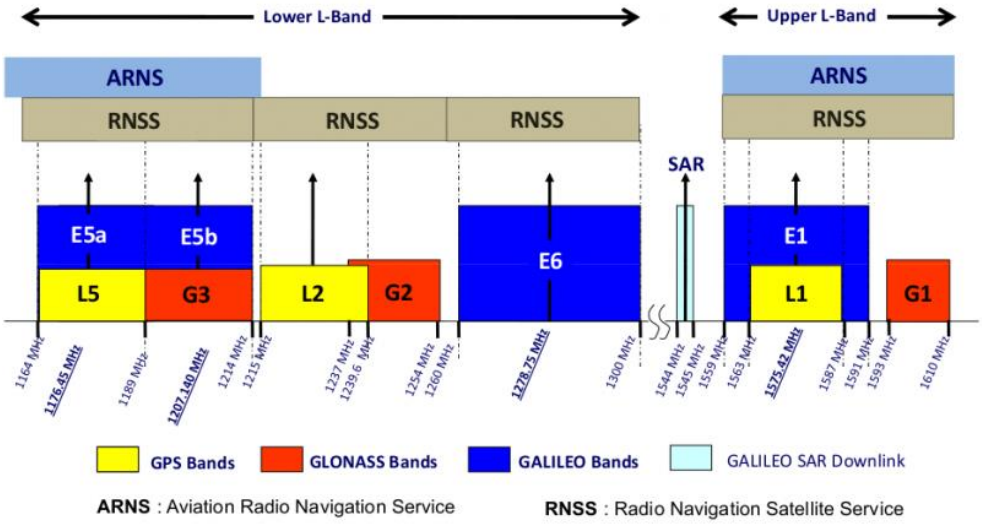
3.3.3 BPSK a nosná vlna

Nosná vlna je harmonický signál, na který je modulována PRN kódem rozprostřená datová zpráva. Nosné frekvence jsou voleny tak, aby byla minimalizována rádiová interference a aby se signál dobře šířil zemskou atmosférou. V tabulce 1 jsou vypsány frekvence nosných vln tří hlavních GNSS.

Tabulka 1 : Frekvence nosných vln GNSS [12]

GPS	GLONASS	GALILEO
L1 1575,42 MHz	L1 1602,00 MHz	E1 1575,42 MHz
L2 1227,60 MHz	L2 1246,00 MHz	E5A 1176,45 MHz
L5 1176,45 MHz	L3 1201,00 MHz	E5B 1207,14 MHz
-	-	E6 1278,75 MHz

Na obrázku 5 je zobrazena část elektromagnetického spektra obsahující v tabulce 1 uvedené nosné frekvence.



Obrázek 5 - Nosné vlny GNSS systémů [12]

Rozprostřený signál je na nosnou vlnu modulován ve většině případů pomocí BPSK. Plánovaný signál GPS L1C a signály E5 a E1 Galilea budou modulovány různými verzemi BOC modulace, ale všechny civilní signály, které jsou dnes dostupné, jsou modulovány pomocí BPSK.

BPSK přenáší na nosné vlně pouze dvě hodnoty : 1 a 0. Fáze nosné vlny se v případě změny z +1 na 0 posune o π, v případě opačném o –π. Výhodou BPSK je její jednoduchost a rigidnost vůči interferenci a nízká chybovost (BER). Signál BPSK lze popsat jako:

$$s(t) = \sqrt{2P}\cos(2\pi f_0 t) \quad pro\ binární\ hodnotu\ 1$$

$$s(t) = \sqrt{2P}\cos(2\pi f_0 t + \pi)\ pro\ binární\ hodnotu\ \ 0 \quad (1.6)\ [11]$$

Kde P zastupuje průměrnou hodnotu výkonu a f_0 označuje frekvenci nosné vlny. Neboť změna fáze nosné vlny o π má stejný efekt jako násobení ±1, lze jednodušeji znázornit modulaci jako:

$$s_k(t) = m(t)\sqrt{2P}\cos(2\pi f_0 t)\ (1.7)\ [11]$$

pokud je modulační signál m(t) posloupnost skládající se z množiny hodnot {±1}. Jak bylo vidět v předešlém textu, GNSS často vysílají v jednom pásmu více signálů, které modulují různými rozprostřovacími kódy. Toho je dosaženo pomocí vysílání dvou nosných vln, které jsou vzájemně posunuty o π/2 – tudíž je minimalizována vzájemná interference. Signál ve fázi se často v literatuře označuje jako I a signál posunutý o 90° jako Q.

Signál pak vypadá takto:

$$s(t) = \sqrt{2P_1}c_1(t)d_1(t)\cos(2\pi f t) + \sqrt{2P_2}c_2(t)d_2(t)\sin(2\pi f t)\ (1.8)\ [3]$$

Kde $c_x(t)$ a $d_x(t)$ zastupují dvě různé PRN sekvence respektive dvě navigační zprávy. Každý rozprostírací kód může posunout signál dvěma způsoby(BPSK - +π a –π), dohromady tedy musíme uvažovat 4 posuny fází. Tato modulace se tedy nazývá QPSK. [3]

Civilní signály GNSS

GPS

- C/A – první civilní signál, zatím jediný v plném provozu.
- L1C – čtvrtý civilní signál, vysílaný na stejné frekvenci jako C/A. Návrh nového signálu zlepší příjem v městských oblastech pomocí MBOC modulace. Do plného provozu by měl být uveden na konci dvacátých let 21. století.
- L2C – druhý civilní signál, po kombinaci s C/A na frekvenci L1, umožňuje korekci lomu signálu na ionosféře. Je vysílán s vyšším výkonem, a proto bude příjem signálu snazší např. v zalesněných oblastech. Signál je zatím předoperačně vysílán z 19 satelitů a okolo roku 2018 by měl být plně dostupný.
- L5 – třetí civilní signál vysílán v pásmu vyhrazeném pro bezpečnostní letecké služby. Signál využívá širšího vysílacího pásma, oproti L1 C/A vyššího výkonu a pokročilého návrhu architektury signálu. Vysílání je zatím prováděno z 12 satelitů, plně operační bude okolo roku 2024. [13]

GLONASS

- C/A – pro civilisty otevřená služba. Signál je možno přijímat buďto pomocí FDMA na frekvencích L1, L2 anebo pomocí CDMA na frekvenci L3. [14]

Galileo

- OS – otevřená služba zdarma pro všechny uživatele dostupná na frekvencích E1, E5A a E5B, která by měla být srovnatelná se službou C/A systému GPS.
- CS – placená šifrovaná služba, dostupná na frekvencích E1, E5A, E5B a E6. Bude zpřístupněna pouze pro registrované uživatele. Služba by měla být garantována. [15]

Tabulka 2 - služby GNSS [14], [13] (modře vyznačené – FDMA signály)

	L1		L2		L3	L5	E1	E5A	E5B	E6
	civ	voj.	civ	voj	civ	civ	civ	civ	civ	civ
GPS	C/A L1C	P(Y) M-code	L2C	P(Y) M-code		L5				
GLONASS	C/A	P	C/A	P	C/A					
Galileo							OS CS	OS CS	OS CS	CS

3.4 GNSS přijímače

Multikonstelační přijímače

Z důvodu existence více než jedné plně funkční GNSS dochází k rozšíření multikonstelačních přijímačů. Hlavní výhodou multikonstelačních přijímačů je mnohem vyšší počet viditelných družic. Tento fakt se promítne do několika výhod poskytovaných multikonstelačním přijímačem:

- Rychlejší akvizice signálu
- Zvýšená přesnost systému (viz 3.6)
- Zmenšení vlivu překážek pro signál (budovy apod.)
- Větší odolnost přijímače vůči interferenci [16]

Multifrekvenční přijímače

Přijímače schopné příjmu více signálů na více frekvencích jsou velmi efektivní v odstraňování chyby vytvořené lomem signálu na ionosféře (± 5m). Další výhodou poskytovanou těmito přijímači je vyšší odolnost vůči rušení (rušící signál by musel být vysílán na více frekvencích). [16]

Softwarově definované přijímače

Softwarově definovaný přijímač je přijímač, jenž má hardwareově řešenou pouze anténu a navigační přijímač. Následující digitální zpracování signálu je provedeno pomocí softwarově programovatelných obvodů (např. FPGA) a mikroprocesorů. Toto řešení velice zjednodušuje stavbu přijímače, jelikož není potřeba pokročilý hardware, jeho role je přebrána softwarovým

zpracováním. Další výhodou je snadná rekonfigurovatelnost přístroje, možnost přidání nových funkcí pouhou výměnou softwaru. [17]

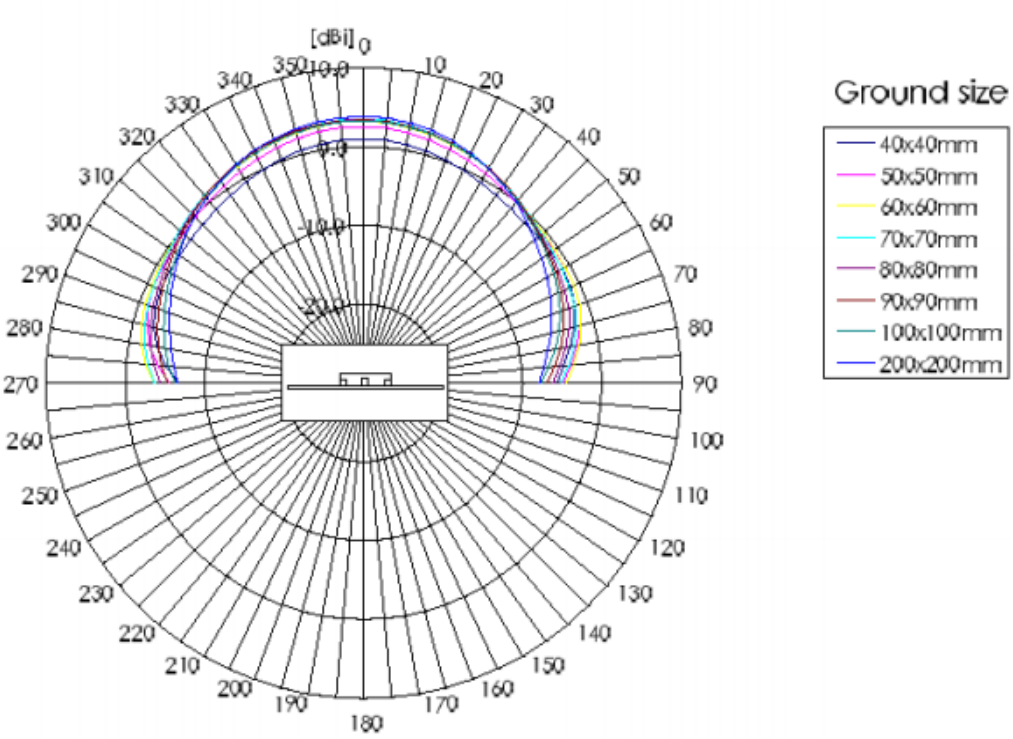
3.4.1 Konstrukce GNSS přijímačů

GNSS přijímače jdou obecně rozložit na 3 hlavní podsystémy - rádiová část přijímače (+ anténa), digitální signálový procesor a navigační počítač.

Rádiová část přijímače

Anténa přijímače převádí elektromagnetický signál vysílaný anténou družice na elektrický, který může být dále zpracován. Anténa musí mít maximální citlivost v oblasti frekvence nosné vlny, neboť zisk antény se mění se změnou frekvence. Pokud je přijímač multifrekvenční, musí být pro každé pásmo implementovaná dedikovaná anténa anebo musí být jedna anténa dostatečně citlivá ve všech potřebných pásmech.

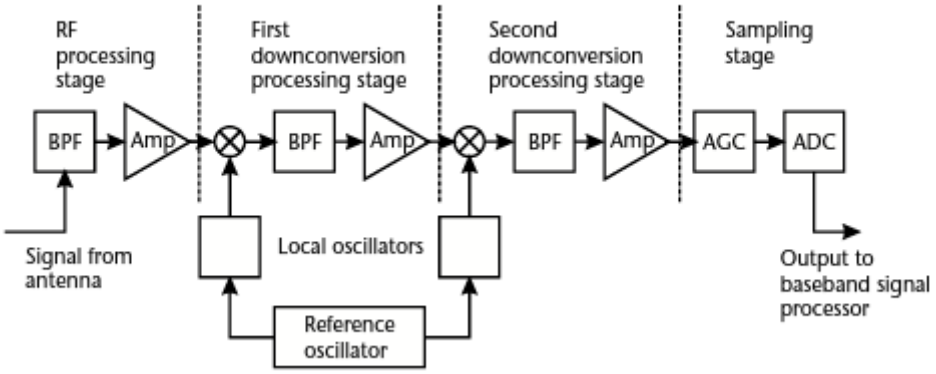
Anténa by měla být citlivá na signály přicházející směrem z volné oblohy. Na obrázku 6 jsou zobrazeny směrové charakteristiky mikropáskových antén různých rozměrů. Při dopadovém úhlu okolo 0° ve vertikální rovině má typická anténa přijímače zisk 2 až 4 dBic. Tento zisk klesá se zvětšováním úhlu dopadu a pro úhly větší než 50° je zisk negativní.



Obrázek 6 - Radiační charakteristika mikropáskové antény ve vertikální rovině [18]

Signály GNSS jsou vysílány s pravotočivou kruhovou polarizací (RHCP), po odrazu od zemského povrchu (nebo stěny domu apod.) se polarizace může změnit na levotočivou (LHCP). Z důvodu snížení chyby způsobené mnohacestným šířením signálu (multipath) jsou antény přijímačů citlivé jen na pravotočivě polarizované signály. [19]

Dále se signál zpracovává, digitalizuje a je předáván navigačnímu počítači. U vícefrekvenčních přijímačů je pro každé přijímací pásmo instalována dedikovaná radiová část na zpracování signálu.



Obrázek 7 - Architektura radiové části GNSS přijímače [19]

Nosná frekvence je konvertována z originální frekvence na nižší (mezifrekvenci). Díky nižší frekvenci může být použita nižší vzorkovací frekvence, což snižuje požadavek na výkon navigačního počítače a kvalitu použitých součástek. Nejčastější je použití dvou konverzních stupňů, lze jich ale použít i více či jen jeden. V každém stupni je přicházející signál násoben se sinusovou vlnou produkovanou lokálním oscilátorem.

$$\cos(2\pi f_r t)\cos(2\pi f_l t) = \frac{1}{2}[\cos(2\pi(f_r + f_l)t) + \cos(2\pi(f_r - f_l)t)] \quad (1.6)\ [3]$$

Harmonická vlna s vyšší frekvencí (f_r+f_l) je následně eliminována pásmovou propustí. Po konverzi signálu na nižší frekvenci je signál posílán do bloku automatického vyrovnávání citlivosti (AGC). Blok AGC přímo spolupracuje s AD převodníkem (ADC), neboť zesiluje příchozí signál tak, aby se optimálně využil dynamický rozsah ADC. Zisk AGC závisí na síle šumu v pásmu. Následuje diskretizace na číslicové hodnoty (kvantizace) v ADC. [3]

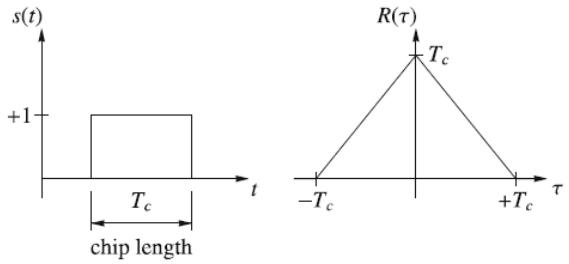
Digitální signálový procesor

Navigační počítač disponuje pro každý viditelný satelit kanálem. Typický přijímač pro C/A kód má okolo 10-12 kanálů. Navigační počítač demoduluje zpracovaný a navzorkovaný signál z rádiové části přijímače korelací s lokálně generovanými PRN kódy a vnitřně generovanou nosnou vlnou. Zde je v principu využívána autokorelační funkce. [19]

K porovnávání posunu fáze lokálně generované PRN sekvence a PRN sekvence přijímaného signálu je využíván princip matematicky popsatelný pomocí autokorelační funkce. Tato funkce popisuje podobnost dvou signálů o stejné periodě a časový posun mezi nimi. Je definována jako:

$$R(\tau) = \int_0^T s_1(t)s_2(t+\tau)d\tau \quad (1.6)\ [3]$$

Jak je vidět, výše uvedený vztah je funkcí časového posunu τ. Pro časový posun mezi signály s_1 a s_2 nabývá pro nějaké τ funkce maximální hodnoty (viz obrázek 8). τ pak je rovno časovému posunu mezi oběma signály. Od tohoto maxima na obě strany klesá až k nulové funkční hodnotě, která přísluší délce jednoho čipu PRN kódu.



Obrázek 8 - jeden chip PRN kódu (vlevo), autokorelační funkce (vpravo) [3]

Navigační procesor

V navigačním procesoru je z demodulovaného signálu dekódována navigační zpráva a následně zde probíhá výpočet PVT, řízení lokálního generátoru PRN kódu, akvizice a sledování signálu. [3] [19]

3.5 Akvizice a sledování signálu

Procesy, které musí přijímač po zapnutí provést, než je schopen přijímat informace obsažené v signálu a použít je, jsou:

Akvizice

1. Určit viditelné satelity
2. Určit přibližný Dopplerův posun pro každý určený satelit z předešlého kroku – v prvních dvou krocích využívá přijímač data uložená v paměti (almanach). Toto umožňuje zmenšit oblast, ve které musí přijímač hledat. Pokud nebyl dlouho přijímač zapnut, musí si stáhnout celý almanach pomocí signálu vysílaného satelity. Akvizice signálu pak trvá déle.

3. Hledat signál v časovem posunu (PRN kódy - délka letu signálu) a ve frekvenčním spektru (nosná vlna - Dopplerův posun) – nejnáročnější část procesu akvizice signálu, je nutné opět zkonstruovat rozprostřený signál, jež je skryt pod hladinou šumu. Pro získání použitelného SNR je nutné zprůměrovat signál pro daný korelační pokus po určitou dobu.
4. Určení frekvence nosné vlny a rozdíl fází lokálně generovaného a přijímaného PRN kódu

Sledování

5. Sledovat změny veličin uvedených v předešlém kroku [20]

3.6 Performační indikátory

Pro hodnocení kvality služeb poskytovaných GNSS se používají performační indikátory. V literatuře zabývající se problematikou GNSS se používají níže uvedené parametry v následujících definicích.

Přesnost – míra chyby, odchylka odhadované pozice přijímače od pravé, neznámé. V civilních aplikacích se vyjadřují pomocí chybových limitů „1-sigma“ a „2-sigma“, což jsou 63. respektive 95. percentily navigačních odchylek pro jednu dimenzi. Přesnost určuje odchylky za normálních okolností.

Integrita – vyjadřuje míru „normálního chování“ systému. Vyjadřuje, jakou měrou můžeme spoléhat, že nenastane odchylka určení polohy mnohem větší než přesnost systému. Kvantitativního vyjádření můžeme dosáhnout pomocí tří parametrů:

- Integrity risk – pravděpodobnost, že se v systému vytvoří nepřijatelná chyba bez včasného varování. Situace, kdy nelze důvěřovat výstupům systému se nazývají „loss of integrity“ (LOI).
- Alert limit – definuje hranici velikosti odchylky, která je z bezpečnostních důvodů neakceptovatelná. Tato hranice je pro každou aplikaci GNSS jiná. Kvantitativně je vyjádřena hodnotami odchylek od pravé pozice.
- Time to alert – časový interval mezi výskytem potenciálně nesprávné informace, kdy je překročen alert limit a časem vyslání varovné informace pro ochranu uživatele.

Kontinuita – je pravděpodobnost, že systém během daného časového intervalu či operace přestane dodávat navigační data dané kvality, za předpokladu, že data dosahovaly této kvality před začátkem daného intervalu/operace.

Ztráta kontinuity může nastat, pokud družice přestane vysílat signál nebo pokud je systémem identifikována chyba integrity.

Pro zhodnocení kontinuity lze použít další dva parametry – pravděpodobnost planého poplachu integritních monitorů a kritický satelit – satelit, jehož náhlé přerušení vykonávání funkce by zapříčinilo ztrátu kontinuity.

Dostupnost – procentuální vyjádření času, kdy tři výše uvedené parametry dosahují kvality požadované danou aplikací. Nejčastější definicí je dlouhodobý průměr pravděpodobností, že požadavky na přesnost, integritu a kontinuitu jsou zároveň dodrženy. [21]

4 Způsoby ovlivnění správné funkce GNSS přijímače

S čím dál rozšířenějším použitím GNSS v civilní infrastruktuře se společnost stále více vystavuje nebezpečí útoku na infrastrukturu využívající právě GNSS, která není ve velké většině případů proti takovým útokům chráněna. Vojenské signály GPS a GLONASS jsou zašifrované, tudíž zabezpečenější vůči spoofingu (nikoli rušení, termín vysvětlen dále v textu). V civilních aplikacích je ale dosud používán ve své podstatě nechráněný signál na L1. V této části práce tedy budou rozebrány vybrané způsoby negativního ovlivnění přijímaného civilního GNSS signálu.

Díky velice nízkému přijímanému výkonu signálu (sila signálu na zemském povrchu se pohybuje mezi -120 až -130 dBm [22]) se nejmyslitelnějším útokem na služby GNSS zdá zamýšlená interference (jamming). Spoofing, neboli poskytování cílovému přijímači falešný GNSS signál, není v současné době pravděpodobný, neboť by ho musela provést kvalifikovaná osoba, či organizace s potřebným know-how, ale není vyloučitelný, obzvláště díky rozšíření softwarově definovaných přijímačů, které činí takovýto útok o dost proveditelnějším (levnější součástky).

4.1 Interference

Interference rádiových vln bude v následujícím textu dělena na záměrnou a nezáměrnou. Mezi nezáměrnou se řadí vysílání způsobené chybnou funkcí technického vybavení, vyššími harmonickými frekvencemi například televizního vysílání, interference způsobená sluneční aktivitou a i jistá interference mezi samotnými navigačními satelity (intrasystémová interference) [23]. Do záměrné interference se řadí záměrné vysílání osoby způsobující interferenci v oblasti spektra vysílání GNSS – tedy záměrné koordinované útoky, ale i lidé využívající osobní rušičky rádiového spektra – také známy pod zkratkou PPD (Personal Privacy Device).

Existuje celá řada případů za posledních několik let, kdy byl výpadek služby GNSS zapříčiněn ať už záměrným rušením, tak i nezáměrnou interferencí. Jedním z takovýchto příkladů je incident, který se stal v roce 2009 na letišti Newark v New Jersey. Nově nainstalovaný systém GBAS vykazoval krátkodobé denní výpadky v příjmu signálu. Po dvou měsících vyšetřování ze strany FAA se podařilo identifikovat, co způsobovalo problém. Denně kolem letiště projížděl řidič nákladního vozidla vybavený, na trhu volně dostupnou, rušičkou signálů GPS (PPD). Během incidentu nedošlo k žádným škodám na majetku ani na životech, ukázalo se ale, jak je jednoduché narušit i poměrně sofistikovaný systém, pokud využívá GNSS. [24]

4.1.1 Charakteristiky interference

Interference lze popsat pomocí následujících charakteristik:

1. **Dle typu**
   - Interference sinusovou vlnou – vysílán signál o jednom tónu (frekvenci)
   - AM, FM, PM, či jinak modulovanými signály – signály modulované amplitudou, frekvencí nebo fází. Tyto modulace rozprostírají signál na širší pásmo spektra.
   - Šum – náhodné sečtené signály v pásmu rádiových frekvencí.
2. **Střední frekvence** - Podle toho, v jaké části spektra relativně k „našemu“ signálu, se interference nachází, rozdělujeme interference na nacházející se mimo pásmo (out of band), blízko pásma (near band) a uvnitř pásma (in band).
3. **Šířka pásma** – dle šířky pásma, na které je rušení vysíláno, charakterizujeme interference na širokopásmové anebo úzkopásmé. Při přiřazení záleží na relativních šířkách pásma našeho zájmu (GNSS) a pásma interferenčního
4. **Výkon** – poměr výkonu signálu a šumu či interference se vyjadřuje většinou pomocí C/N anebo lze použít i poměr rušení k signálu – jammer to signal J/S.
5. **Časová oblast** – interference může být vysílána kontinuálně nebo diskrétně v pulzech. Pulzní interferenci charakterizujeme pomocí těchto parametrů:
   - Šířka pulzu – délka trvání jednoho pulzu
   - Pulzní frekvence – počet pulzů za sekundu
   - Pulzní poměr (Duty cycle DC) – procentuální poměr času, kdy jsou vysílány pulzy DC = (PRF*PW)/1s [25]

4.1.2 Nezáměrná interference

Elektromagnetické spektrum je omezená komodita. O přiřazení částí rádiového spektra různým službám se proto stará odnož organizace ITU, ITU-R. Signály GNSS jsou vysílány ve frekvenční oblasti zvané RNSS, která je chráněná právě ITU-R. V této části nemá povolení vysílat nikdo jiný. Problémem jsou signály ze sousedících částí radiového spektra, které díky výkonu, kterým jsou vysílány zvyšují hladinu šumu právě v pásmu RNSS. Pokud je hladina šumu dostatečně vysoká, může projít i přes útlum kaskády pásmových propustí v GNSS přijímači. [26] V USA právě probíhá živá debata o instalaci širokopásmových vysílačů Lightsquared, které by mohly způsobovat vážné rušení signálů GNSS, neboť by měly vysílat přibližně o 90 dB silnější signál v blízkosti pásma RNSS. Tato práce se ale nezáměrným rušením nezabývá, o problému s Lightsquared více v [27].

4.1.3 Záměrná interference

Existují dva základní mechanismy záměrného rušení. Jeden ze způsobů využívá snižování poměru C/No na takovou hodnotu, že přijímač již není schopen sledovat užitečný signál. Za těchto okolností není přijímač schopen získávat data o své poloze. Druhým způsobem se útočník snaží přivést na vstup přijímače výkon, na který není přijímač stavěn. Tímto způsobem může dojít i k fyzickému poškození části přijímače. Rušení může mít na přijímač celou řadu dopadů:

1. Ztráta signálu – pokud je přijímač vystaven silnému rušení, může přestat sledovat signál. Při takto silném rušení je detekce interference snadná – přístroj nemá signál.
2. Zeslábnutí měřeného signálu – většina přijímačů měří přijímanou hodnotu C/N_0. Způsob detekce rušení a měření síly rušení je popsán v 5.2.1.
3. Zvýšení hladiny šumu na naměřených pseudovzdálenostech – rušení může zvětšit chybu na naměřené pseudovzdálenosti – tato se skládá z časové odchylky lokálního oscilátoru a šumu. [25]

4.1.4 Rušení vysokým výkonem

Díky nízkým hodnotám výkonu signálu u povrchu Země (okolo -120 dBm, viz 2.1.1) jsou GNSS přijímače postaveny na příjem nízkých hodnot signálu a tudíž je maximální síla signálu, kterou je možno přivést na jejich vstup relativně malá. Tato hodnota se pohybuje u klasických přijímačů okolo 15dBm [28] [29]. Nyní se pokusím pomocí Friisovy rovnice spočítat v jakém rozmezí by se musel pohybovat výkon, kterým by bylo nutno vysílat, pokud by útočník chtěl „oslepit“ přijímač – dodat příliš vysoký výkon na jeho vstup.

$$P_v = \frac{P_p}{G_v G_p}\left(\frac{4\pi r}{\lambda}\right)^2 \rightarrow P_v = \frac{P_p}{G_v G_p} L_0 \rightarrow \ zlogaritmování \rightarrow \ P_v = P_p + L_0 - G_v - G_p$$

$$P_v = 15[dBm] + 56{,}4[dB] - 4[dB] - 4[dB] = 63{,}4\ dBm \cong 2187W$$

Ve výpočtu předpokládáme rušení pásma L1 (λ = 0,19 m) na vzdálenost 10 m. Zisk obou antén je 4 dB. Tyto hodnoty se mohou lišit – u přijímače je pravděpodobná nižší hodnota zisku (viz 2.3.1), u rušičky je možnost výskytu vysoce ziskové antény. Z výpočtu vyšla hodnota, kterou by musel útočník rušit, aby dosáhl maximálního vstupního výkonu 15 dBm, 2187 W. To je výkon, kterým rušičky, vyskytující se ke koupi na internetu, nedisponují. Takováto rušička by také měla vysokou hmotnost a velké rozměry, tudíž by byla velice nápadná. Navíc, jak bude dále popsáno, k odepření služby GNSS, stačí rušit výkonem okolo 10 mW, možnost tohoto rušení tedy nepovažuji za atraktivní.

4.1.5 Dostupnost rušiček GNSS

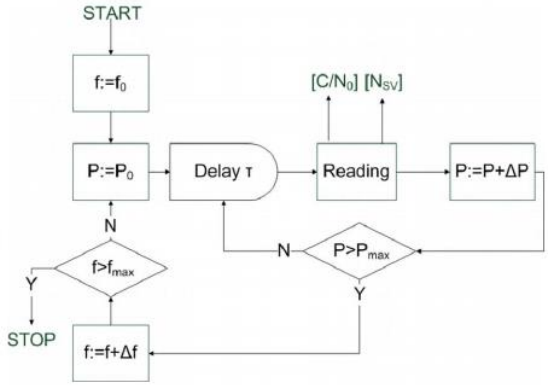
Dle názoru autora největší nebezpečí pro aplikace využívající službu GNSS neplyne z koordinovaných útoků specializovaných osob, ale z neregulovaného množství osobních rušiček radiového spektra v oblasti RNSS. Tato domněnka je rozvedena v následujícím textu. Osobní rušičky, které jsou často napájeny napětím 12V z palubního zapalovače silničních vozidel začínají být hojně využívány například řidiči nákladních automobilů, firemními řidiči nebo i lidmi, kteří se obávají z ne nutně fakty podložených důvodů sledování, z důvodu zachování soukromí anebo i kvůli snaze obejít systém výběru mýtného vybíraného na bázi GNSS. Tyto rušičky do zapalovačů, ač je jejich použití ve velké většině zemí postihováno zákonem, se dají bez problému zakoupit na internetu od základních modelů za ceny začínající na několika desítkách dolarů až po sofistikované rušičky v cenách za několik stovek dolarů například na [30].

Na internetových stránkách obchodů, nabízejících tyto rušičky, jsou většinou uvedeny poloměry efektivního rušení (vzdálenost od rušičky, při které přijímač přestane být schopen sledovat signál GNSS) v řádech metrů až do řádu desítek metrů. Efektivní rušení ale tyto přístroje poskytují i ve vzdálenostech mnohem větších (viz 4.1.9).

4.1.6 Důsledky záměrné interference na přijímač

Následky, které může mít vysílání rušení GNSS signálu, budu ilustrovat na výsledcích pokusu týmu z university v Gdaňsku z roku 2011 [31], který zkoušel v laboratorním prostředí odolnost GPS vůči záměrnému rušení. K pokusu byl použit kvalitní multikonstelační GPS/GLONASS přijímač, jenž lze používat na přesná geodetická zaměření s frekvencí obnovy PVT 1Hz. Přijímač je také vybaven soustavou adaptivních filtrů, která chrání přijímač před interferencí uvnitř pásma. Signál a rušící signál byly generovány signálovým generátorem, následně mixovány dohromady a přijímány přijímačem.

Nejdříve bylo změřeno SNR za normálních podmínek, bez rušení. Generátorem byl vysílán signál jednoho GPS satelitu výkonem -88dBm, celková úroveň šumu v pásmu užitečného signálu byla změřena na -72dBm. SNR bylo tedy rovno -16dB. Dále byl pokus prováděn dle algoritmu vyobrazeného na obrázku 9. Rozsah frekvencí je ±10MHz okolo střední frekvence. Frekvenční krok používaný v algoritmu je 100kHz. Rozsah výkonu rušičky je od -65dBm do -15dBm s krokem 0,5dB. Při měření rušení v akviziční fázi byl výkon rušičky postupně dekrementován narozdíl od případu, kdy se měřilo rušení ve sledovací fázi a výkon byl inkrementován.



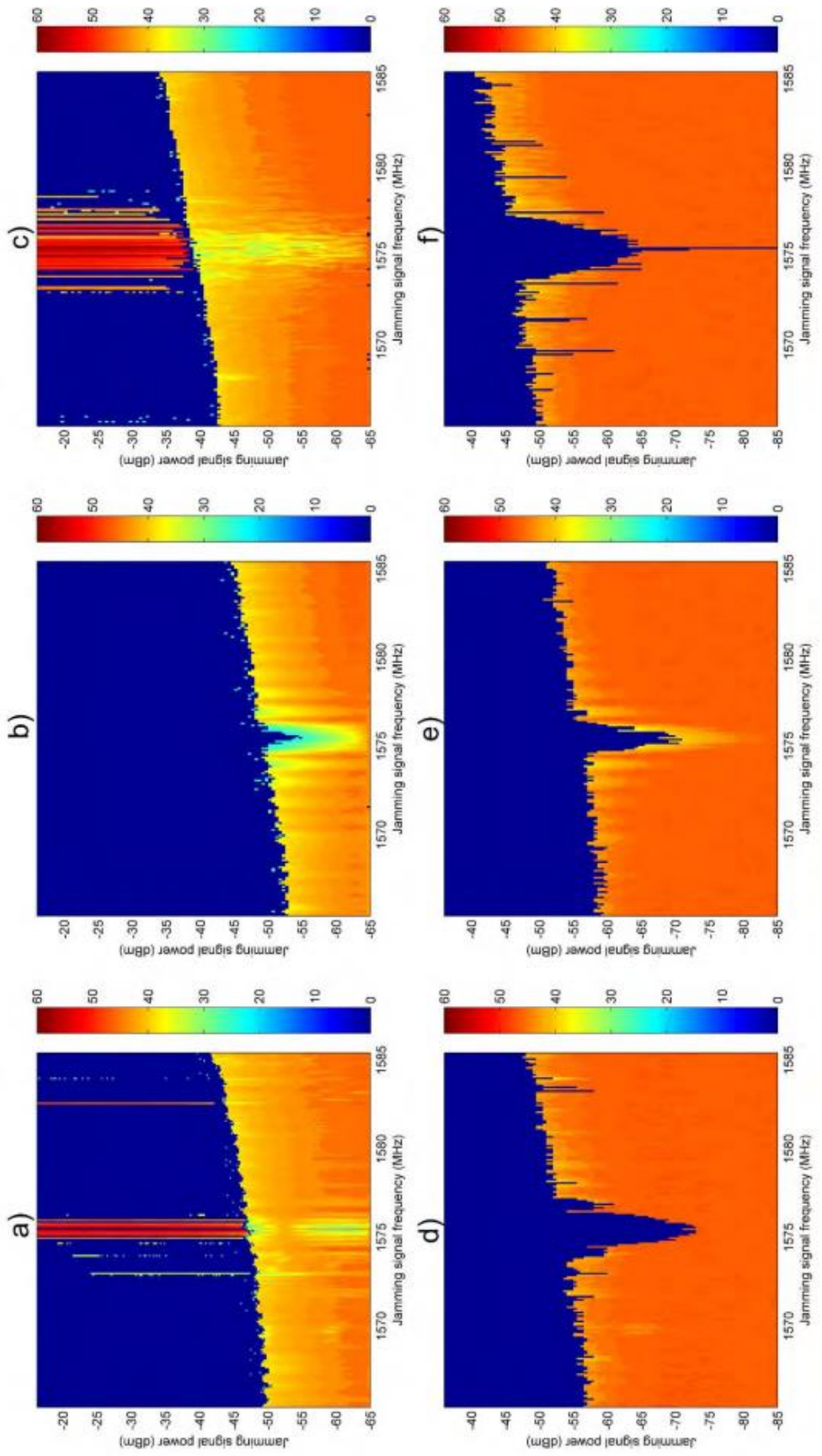
Obrázek 9 - Algoritmus pokusu [31]

Výsledky pokusu jsou vidět v grafech uvedených na obrázcích 10 a 11, kde hodnoty na ose X reprezentují frekvence rušícího signálu a hodnoty na ose Y výkon rušícího zařízení. Barvy reprezentují C/N_0 signálu přijímaného GNSS přijímačem. Rozsah barevné škály je dán od 0dBHz (modrá barva), kdy není přijímačem užitečný signál GNSS rozpoznán až po 60dBHz (červená barva). Přijímač potřebuje hodnotu alespoň 30dBHz a více, aby úspěšně demoduloval přijímaný signál.

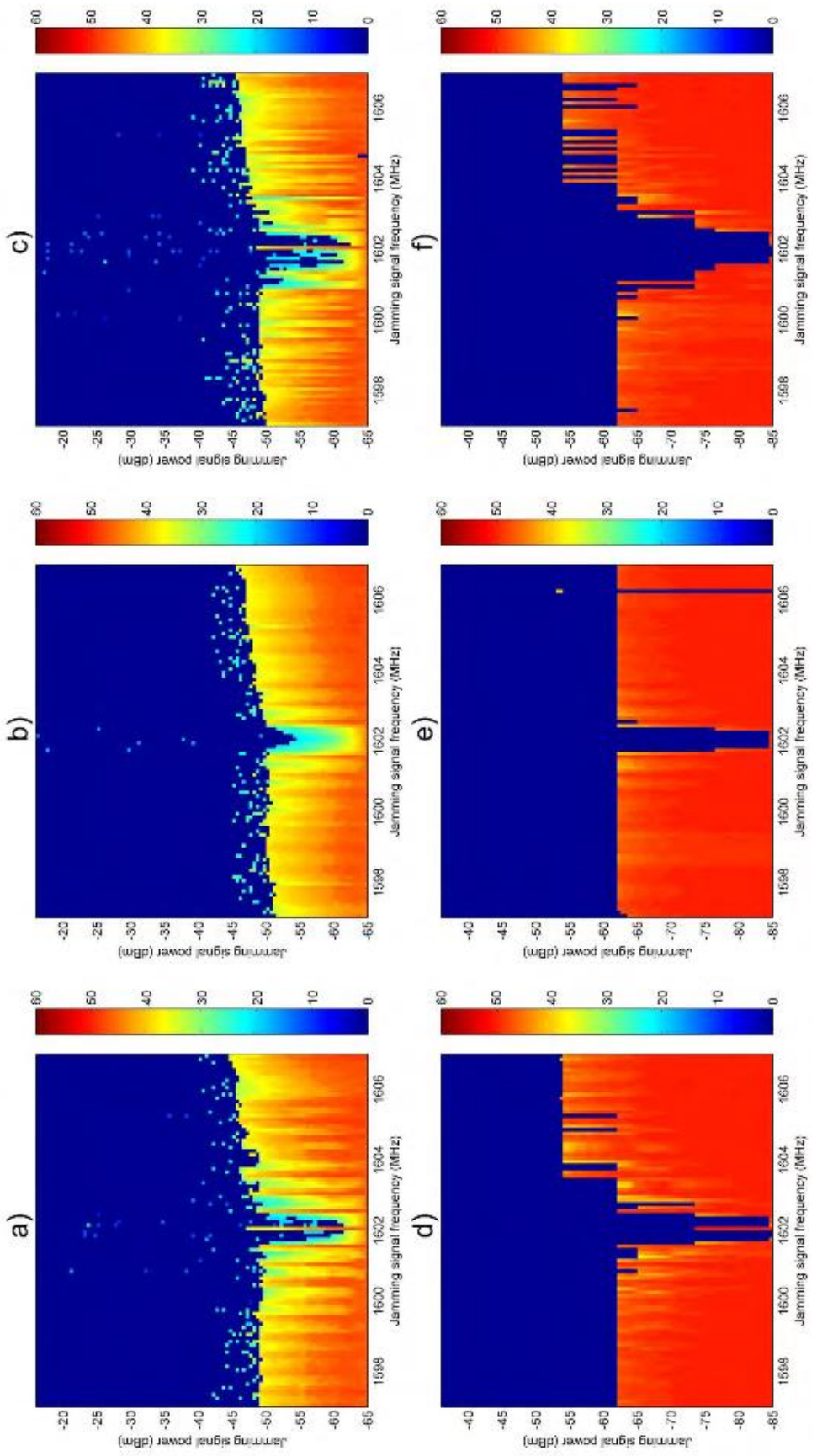
V první řadě na obrázku 10 jsou zobrazeny průběhy při rušení ve sledovací (tracking) fázi. V tomto případě byl nejdříve zapnut přijímač, následně úspěšně prošel akviziční fází (nalezl GNSS signál) a až poté byl zapnut rušící signál. Druha řada zobrazuje průběhy rušení při akviziční fázi (GNSS signál nebyl přijímačem před začátkem rušení nalezen).

V prvním sloupci na obrázcích 10 a 11 je užitečný signál rušen sinusovkou, ve druhém pomocí BPSK signálu o šířce pásma 50 kHz a ve třetím sloupci byl použit k rušení signál, jenž byl rozprostřen pomocí stejných PRN kódů jako signál užitečný. [31]

Jak je vidět na 10a a 10c, testovaný GNSS přijímač je vybaven ochranou vůči interferenci, která je poměrně účinná vůči rušení uvnitř pásma, není ale efektivní v ochraně proti rušivým vysíláním mimo pásmo. Rušení pomocí BPSK modulovaným signálem se ukázalo ve sledovací fázi jako nejefektivnější ze všech zkoušených rušících signálů uvnitř i vně pásma. Největšího rušícího efektu pomocí tohoto signálu lze dosáhnout při rušení na střední frekvenci užitečného signálu. V případě, že je prováděno rušení ve fázi akvizice GNSS signálu, vede si celkově přijímač hůře. Na obrázcích 10 (d, e, f) vidíme, že obzvláště interference uvnitř pásma činí přijímači službu GNSS nepřístupnou. Signál rozprostřený PRN kódem se ukazuje jako nejrušivější uvnitř pásma. Vně pásma je ale nejúčinnější rušení pomocí BPSK signálu.



Obrázek 10 - Rušení GPS, v horní řadě sledovací fáze, v dolní fáze akviziční, typ rušení od levého sloupce: CW, BPSK, signál rozprostřený stejným PRN kódem jako signál satelitu, osa X - frek.,Y - výkon rušení přiložený na vstup přijímače, barevná škála - C/N_0 [31]



Obrázek 11 - Rušení GLONASS, v horní řadě sledovací fáze, v dolní fáze akviziční, typ rušení od levého sloupce: CW, BPSK, signál rozprostřený GPS PRN kódem, osa X - frek., osa Y - výkon rušení přiložený na vstup přijímače, barevná škála - C/N_0 [31]

Jak je vidět na obrázku 11, algoritmus potlačující rušení je ve své podstatě neúčinný, je-li použit na systém GLONASS. Pro úspěšné zarušení signálu při rušení mimo pásmo je nutné vysílat rušivý signál pod vyšším výkonem než při rušení uvnitř pásma. Účinnost rušení během sledovací fáze je nejvyšší pro CW a PRN kódem rozprostřený signál (ruší užitečný signál podobně efektivně). Jejich efekt je největší pokud se střední frekvence rušících signálů pohybuje v blízkosti střední frekvence. Pokud se ale střední frekvence rušícího a rušeného signálu rovnají, efekt rušení je výrazně zmenšen. V akviziční fázi, je podobně jako u GPS nejúčinnější rušení uvnitř pásma. Podobně jako u systému GPS je také uvnitř pásma nejrušivější PRN kódem rozprostřený signál.

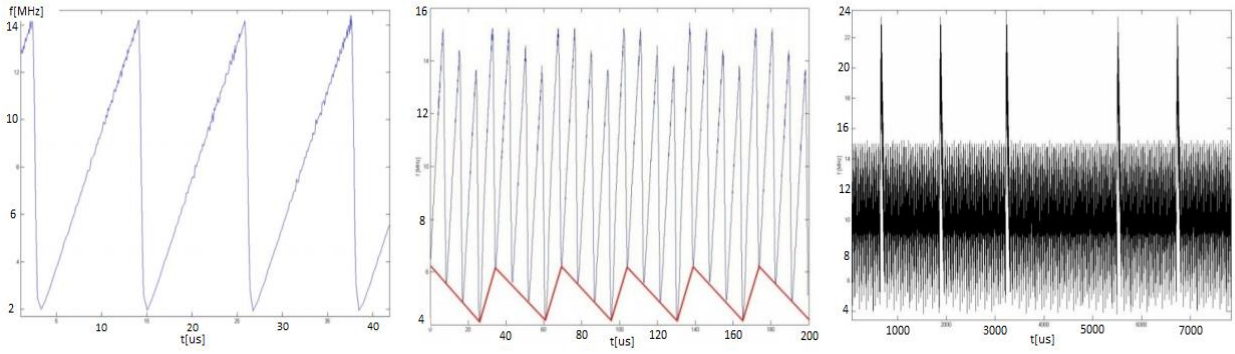
4.1.7 Charakteristiky civilně dostupných rušiček

V posledních deseti letech se z důvodu přibývajících incidentů s rušením GNSS signálu podobných výše uvedenému v Newarku, obrátila pozornost na schopnosti a výkony civilně dostupných levných rušiček signálu. Většina těchto rušiček vysílá signál v pásmu L1/E1. Rušící signál je ve velké většině tzv. „chirp“ signál. To je signál jehož frekvence lineárně roste, či klesá jako funkce času.

4.1.8 Signály vysílané rušičkami

Pomocí rozdílného signálu vysílaného rušičkami, můžeme uvést rozdělení:

1. Rušička vysílající kontinuální vlnu (CW)
2. Rušička vysílající chirp signál – pilovitou vlnu (saw wave)
3. Rušička vysílající chirp signál s pilovitou vlnou modulovanou pilovitou vlnou
4. Rušička vysílající chirp signál, s velkými frekvenčními zákmity



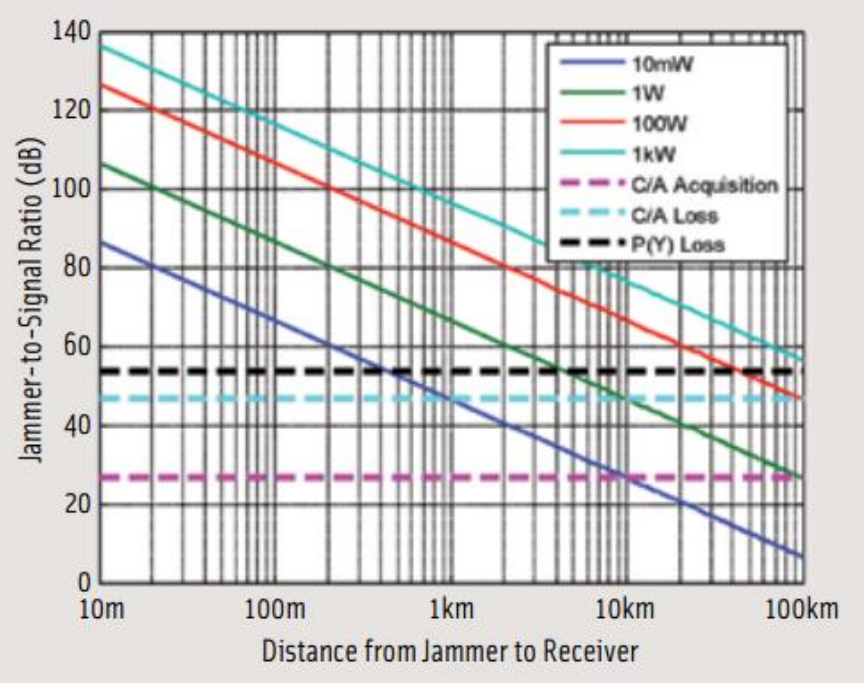
Obrázek 12 - Signály rušiček zleva 2., 3., 4. typu, osa x – čas v [μs], y – frekvence v [MHz] [32]

Většina rušiček do automobilových zapalovačů na trhu patří do skupiny 2. Šířka pásma, kterou jsou tyto přístroje schopny pokrýt, se pohybuje mezi 10,72MHz a 44,9MHz a čas překmitnutí signálu přes všechny frekvence se pohybuje mezi 8,62μs a 18,97μs [32]. Z důvodu nízké ceny a tudíž nekvalitního zpracování vykazují některé z volně dostupných PPD rušiček chybnou

funkčnost. Mezi tato chybná chování patří: nepravidelnosti v překmitu okolo střední frekvence a měnící se maximální frekvence lineární modulace (variabilní okrajové frekvence „chirp“ signálu). K nejzajímavějším chybám patří příliš velký posun střední frekvence od střední frekvence L1. Takovéto chování je například vidět v následujícím odstavci v tabulce 3 u čtvrté rušičky. Takovýmto posunem ztrácí PPD na efektivnosti, ovšem pokud vysílání probíhá pod dostatečným výkonem, dostane se rušící signál přes filtry přijímače i přes to, že vysílá mimo pásmo [33] Katalogový list klasického PPD je uveden v příloze práce i s uživatelským manuálem.

4.1.9 Dosah rušiček

Na obrázku 13 jsou znázorněna rušení o různých výkonech a jejich dopad na přijímač v závislosti na vzdálenosti mezi rušičkou a přijímačem. Tento graf je vytvořen pro typické hodnoty J/S, při kterých přijímač nemůže dále sledovat (modrá, čárkovaná čára pro C/A, černá pro P(Y)) či akvizovat (fialová čárkovaná) signál. Samozřejmě, přijímače se mezi sebou liší a hodnoty J/S při kterých dochází k neschopnosti sledování signálu také. Záleží také na rušičce, na signálu, který vysílá, a na prostředí a překážkách v něm se nacházejících. Nicméně lze tento graf použít jako přibližné pravidlo a dobře znázorňuje zranitelnost přijímačů. Z grafu vyplývá, že u rušení výkonem o velikosti 10mW můžeme zarušit zařízení v okruhu skoro jednoho kilometru.



Obrázek 13 - Dopad rušení (o různých výkonech) na přijímač [34]

Vzdálenost, na kterou je schopno PPD ovlivnit příjem signálu, je jedním z nejdůležitějších parametrů, pro zhodnocení rizika rušení, vzniklého právě těmito přístroji. Proto připojuji výsledek testu v [33]. V tabulce 3 jsou spočteny teoretické přibližné maximální vzdálenosti, na které jednotlivé PPD úspěšně zabrání přijímači Novatel ProPakII-RT2 [35] sledování/akvizici signálu. Jak je jasně vidět, vzdálenosti dosahují vyšších hodnot, než často výrobci avizovaných několik metrů. PPD jsou často vyrobeny velmi nekvalitně, nicméně tento fakt automaticky neznamená nepoužitelnost, pokud je rušička dostatečně výkonná. Například u čtvrté rušičky je vidět posun střední frekvence, kdy vysílaný výkon v pásmu 2 MHz (šířka C/A) je roven nule.

Tabulka 3 - Poloměry efektivního rušení pro různé typy rušiček [33]

	Výkon vysílání P [mW] v pásmu L1 o šířce:			Maximální radius pro zabránění sledování signálu [m]	Maximální radius pro zabránění akvizice signálu [m]
	2 [MHz]	20 [MHz]	50 [MHz]		
1	1,7	9,5	22	308	973
2	1,2	6,5	19	308	614
3	244	642	642	6140	8670
4	0	43	107	173	689

4.1.10 Napadnutelnost přijímačů

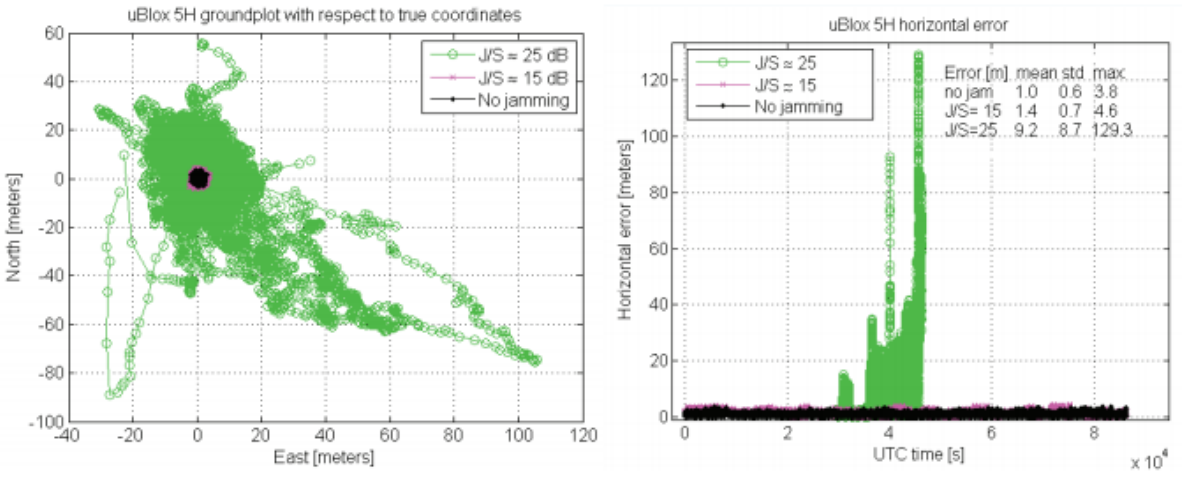
Různé přijímače reagují na rušící signál různým způsobem, i když většina civilních přijímačů dosud nedisponuje ochranami vůči rušení. Je to z důvodu různě řešených navigačních přijímačů a různých algoritmů užitých ke zpracování signálů. Rušení může způsobit zhoršení přesnosti vypočtené polohy či úplnou ztrátu zaměření signálů z družic. Pro ilustraci vlivu rušení na přijímače uvedu výsledky testu z [36] v tabulce 4.

Přijímače zahrnuty ve výše uvedené tabulce byly podrobeny testu, při kterém byly po dobu 24 hodin rušeny civilně dostupnou rušičkou pásma L1. Rušení bylo prováděno chirp signálem (typ 2 z 4.1.8) vysílaného ve dvou různých výkonech – jednou s poměrem J/S=15dB, podruhé s J/S=25dB. Jak je z tabulky vidět, přesnost všech přijímačů byla rušením poznamenána.

Tabulka 4 - Vliv rušení na přijímače – průměr, standardní odchylka, maximální odchylka (vše horizontální) a dostupnost(viz 3.6) [36]

	J/S [dB]	Stř. hod. [m]	Std. Odch. [m]	Max. odch [m]	Dostupnost [%]
uBlox 5H	0	1,0	0,6	3,8	100
	15	1,4	0,7	4,6	100
	25	9,2	8,7	129,3	16
uBlox 5T	0	1,0	0,6	4,0	100
	15	1,5	0,8	6,5	100
	25	4,2	5,5	94	26
Fastrax IT500	0	2,2	1,0	5,3	100
	15	2,3	1,0	6,5	100
	25	3,7	5,2	85,4	16
Fastrax IT600	0	1,3	0,6	3,2	100
	15	1,3	0,7	3,2	100
	25	5,9	3,6	16,4	100
Nokia N8	0	2,6	2,4	32,4	100
	15	3,1	3,8	34,0	100
	25	3,9	2,2	22,4	16
NovAtel (typ neuveden)	0	1,0	0,7	4,8	100
	15	2,4	3,9	90,5	30
	25	5,4	7,3	92,1	8

Při J/S=15dB nedošlo k nijak zásadnímu ovlivnění výkonu u většiny testovaných subjektů mimo NovAtel, jemuž dramaticky vzrostla velikost max. chyby a klesla dostupnost. Na obrázku 14 jsou znázorněny odchylky přijímače uBlox 5H, který nedisponuje žádnou ochranou proti rušení. Jak je vidět, J/S o přibližné velikosti 15 dB má na přijímač zanedbatelný vliv. Při J/S = 25 dB se maximální chyby a hodnoty dostupnosti nijak nechráněného přijímače dostávají na



Obrázek 14 - Zaznamenané pozice přijímače uBlox 5H během 24 hodin, pod různým rušením; vlevo: horizontální rovina, vpravo: horizontální chyba [36]

nepoužitelnou úroveň. Jediný Fastrax IT600 si zachoval solidní funkčnost a to díky zabudované Anti-jamming ochraně. [37][38] Z testu jasně vyplývá, že i malé, levné, volně dostupné rušičky s malým výkonem mohou mít vysoce degradující efekt na kvalitu určení pozice přijímačem bez odpovídajících ochran.

4.2 Spoofing

GNSS spoofing je technika ovlivňování GNSS přijímače, při níž je záškodníkem vysílán falešný signál podobný nebo stejný (podvratný signál) jako signál GNSS, který je uživatelovým přijímačem považován za pravý. Lze také vysílat dříve zachycený GNSS signál a odvysílat ho s časovým zpožděním pod vyšším výkonem (meaconing). Díky příjmu falešného signálu vyhodnotí přijímač chybně svou polohu. [39]

4.2.1 Motivace spoofingu

Útočníka a jeho motivaci můžeme dělit na dva druhy:

1) Útočník záměrně vysílá podvratné informace přijímači v užití strany, která nemá o útoku ponětí. Tento útok by se mohl vyskytnout při pokusu o vytvoření škod jiné straně. Motivace můžou být různé – může jít o pokus o obohacení útočníka nebo jen o pokus o vytvoření chaosu.
2) Útočník záměrně vysílá podvratné informace přijímači ve svém užití. Tento druh útoku by se mohl objevit například při pokusu o obejití systému placení elektronického mýta využívajícího systému GNSS, jaké jsou instalovány v Německu a na Slovensku.

4.2.2 Mechanismus spoofingového útoku

Záškodník se snaží generovat signál co nejpodobnější signálu přijímaného přijímačem uživatele, na nějž je prováděn útok. Uživatelův přijímač za normálního stavu přijímá signál, který lze napsat jako:

$$y(t) = Re\left\{\sum_{i=1}^{N} A_i D_i\left[t - \tau_i(t)\right] C_i[t - \tau_i(t)] e^{j[\omega_c t - \phi_i(t)]}\right\} \quad (3.1)\ [39]$$

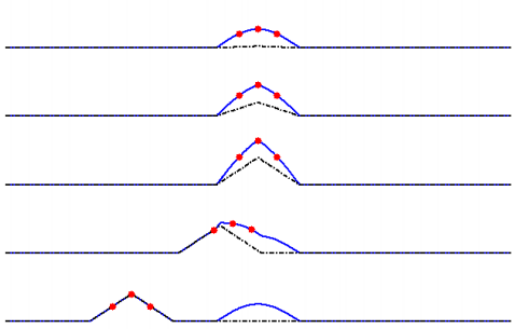
Zde suma i do N značí součet signálů ze všech viditelných (N) satelitů. Amplituda nosné vlny je značena A, D je označena datová navigační zpráva a její argument značí posun fáze PRN kódu. Rozprostírací kód je značen jako C se stejným argumentem jako datová zpráva D. Úhlová rychlost nosné vlny je značena ω_c a ϕ je pro její fázový posun. Podvratný signál tedy bude vypadat podobně – musí mít stejný rozprostírací signál. Součásti signálu, které se liší, jsou označeny apostrofem.

$$y'(t) = Re\left\{\sum_{i=1}^{N'} A'_i D_i\left[t - \tau'_i(t)\right] C_i[t - \tau'_i(t)] e^{j[\omega_c t - \phi'_i(t)]}\right\} \quad (3.2)\ [39]$$

Existují dva hlavní způsoby, jak přinutit přijímač ke sledování podvratného signálu. Jedním z nich je vysílání rušících signálů v pásmu a následné využití probíhající re-akvizice přijímače.

Pokud je při re-akvizici podvratný signál silnější ($A'_i >> A_i$, pro i = 1:N) než pravý, začne sledovat přijímač s vysokou pravděpodobností právě jej.

Druhým způsobem je vysílání signálu zesynchronizovaného se signálem pravým. Průběh je vidět na obrázku 15. Vysílání podvratného signálu začíná na malém výkonu $A'_i \sim 0$ s fází rozprostíracího kódu $\tau'_i \sim \tau_i$. Výkon je postupně zvětšován, až dosáhne větší síly signálu než pravý signál. Po tom, co začne přijímač sledovat podvratný signál, může útočník začít posouvat signály v časové doméně. Tento typ útoku je hůře detekovatelný, díky nepoužití interference, která funguje jako ukazatel nestandartního stavu.



Obrázek 15 - Korelační funkce během spoofing útoku - černě kor. fce s podvratným signálem, modře s pravým signálem [39]

Vysílač podvratného signálu musí být v případě druhého typu útoku zároveň i přijímačem, neboť je pro něj nutná znalost pravých hodnot A_i a τ_i. Také musí být umístěn v dostatečné blízkosti cílového přijímače, aby pracoval se stejnými hodnotami. Druhou možností je přibližná extrapolace výše uvedených veličin s pomocí znalosti relativního umístění útočníkova a cílového přijímače. [39]

4.2.3 Možnosti provedení spoofingového útoku

Dle týmu inženýrů z texaské univerzity v Austinu, kteří vytvořili GPS spoofer a následně jej úspěšně vyzkoušeli na zaoceánské jachtě [40], můžeme dělit spoofing útoky na:

Útoky skrze simulátor GNSS signálů

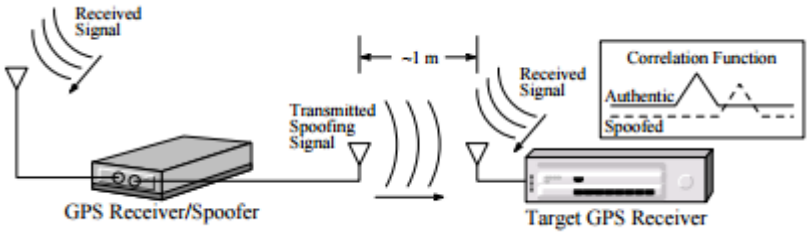
Tato forma útoku využívá skutečnosti, že převážná většina GNSS přijímačů, co jsou dnes na trhu, nedisponují žádnými prostředky pro zvýšení odolnosti vůči spoofingu. Princip je následující: útočník použije jako generátor signálu GNSS simulátor, jehož výstup pomocí zesilovače zesílí a dále vysílá pomocí antény.

Tato forma útoku je jednoduchá na provedení, ale skýtá pro potenciálního útočníka řadu nevýhod. Jednou z nich je cena simulátoru signálu, která se pohybuje okolo 350 tis. € (červen 2016, přibližně 9,5 miliónu korun). Dalším je špatná mobilita simulátoru, neboť většina simulátorů je rozměrná a těžká. Největší překážkou při provedení tohoto útoku je

synchronizace signálu ze simulátoru s pravými signály v oblasti, ve které se právě nachází. Pokud není signál synchronizován, funguje simulátor jako rušička, což zvyšuje nápadnost samotného útoku. Díky těmto překážkám je tento způsob vhodnější pro útočníka 2. druhu. [41]

Útoky s využitím přenosného přijímače-spooferu

Jedním z hlavních problémů spoofingu, který byl zmíněn již v předešlém odstavci, je nezbytnost získání přesné informace o pozici a rychlosti přijmače, kterému chceme vysílat podvratný signál. K vyřešení tohoto problému je možné zkonstruovat kombinaci přijímače a vysílače – spooferu, neboli přijímač-spoofer. Takovýto přístroj lze sestrojit dostatečně malý, a tak je možné ho umístit do dostatečně malé vzdálenosti od cílového přijímače. Přijímač-spoofer získává informace o pozici a rychlosti sebe (a tedy přibližně i cílového přijímače) z GNSS. Na základě těchto informací následně vysílá podvratný signál přijímači.



Obrázek 16 - Útok pomocí přijímače-spooferu [41]

Jak je vidět na obrázku 16, korelační funkce pro pravý signál je nejdříve posunuta, neboť má větší τ, díky zpoždění způsobeném útočníkovou manipulací se signálem. Podvratný signál je následně upraven, aby korelační funkce nabývaly svých maxim ve stejný čas. Po tomto kroku je postupně zvyšován výkon vysílání podvratného sigálu a eventuálně cílový GNSS přijímač začne sledovat útočníkem vysílaný signál místo pravého GNSS signálu. [41]

Narozdíl od generátoru GNSS signálů nelze přijímač-spoofer koupit na trhu. Hardwarovou část lze sestavit z normálně dostupných elektrotechnických součástek díky existenci softwarově definovaných přijímačů (viz 3.4), které pro zpracování signálu používají výkonné procesory. Softwarové vybavení nelze nikde koupit a musí být pro úspěšný útok poměrně sofistikované, ale není vyloučená možnost sestavení erudovanou osobou, obzvláště přihledneme-li k faktu, že C/A signál GPS je detailně zdokumentován v [9] a existuje natolik dlouho, že je velmi dobře popsán v mnohé literatuře. Tento způsob útoku by mohl být použit útočníky obou typů.

Útoky využívající několik přenosných přijímačů-spooferů

Vysoce účinným protiopatřením prot předešlému způsobu útoku by bylo rozlišení dopadového úhlu příchozího signálu a jeho fáze. S jedním přijímačem-spooferem by nebylo možné replikovat několik signálů a jejich rozdílné fáze najednou. Z tohoto důvodu byla vytvořena třetí skupina útoků, které by měly být schopné tuto ochranu obejít. Několik přijímačů-spooferů je rozmístěno v určité konstelaci kolem cílového přijímače, sdílejí referenční oscilátor a jsou chráněny proti spoofingu ze svých řad. V tomto případě by i výše uvedená ochrana selhala. Tento způsob útoku je velmi nepravděpodobný z důvodu velmi vysoké složitosti systému. Jeho velkou výhodou ale je skutečnost, že proti němu neexistuje ochrana, kterou by bylo možné implementovat do uživatelského přijímače. Jediným obranným mechanismem proti tomuto ataku je tedy kryptografická autentikace. [41]

5 Detekce rušení a spoofingu

Jelikož nalezení parametrů definující správnou funkci GNSS přijímače není triviální úkol a, tak dalece, jak je autor s problematikou obeznámen ani není v literatuře příliš řešen, je v práci předpokládáno, že přijímač funguje správně, pokud není detekována chybná funkce. Tato kapitole je věnována různým způsobům detekce nesprávné funkce. Nezbytnou součástí ochrany před rušením, či spoofingem je schopnost detekovat, že je na přijímači právě takovýto útok prováděn. V následující části jsou popsány způsoby, kterými lze určit, zdali je GNSS přijímač ovlivňován.

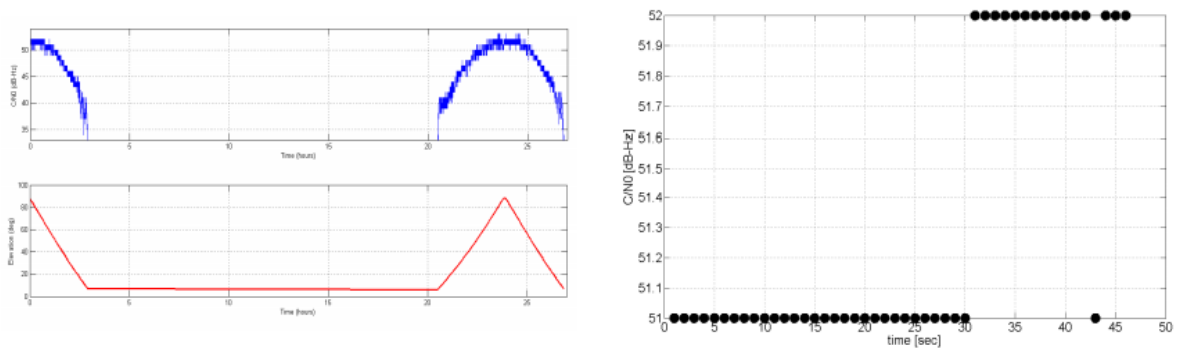
5.1 Detekce interference

Jelikož rušení služby GNSS nemusí znamenat totální ztrátu signálu a nefunkčnost, ale i degradaci určení polohy, je důležité poznat, kdy je signál rušen, aby bylo možno považovat data za pravdivá.

5.1.1 Detekce pomocí C/No

Jedním z důsledků interference je zhoršení poměru C/N_o na vstupu přijímače. Všechny přijímače na trhu poskytují tuto hodnotu a tak se C/N_o jeví jako vhodný kandidát na detekci rušení i když způsoby, jakými ji přijímače odhadují, jsou odlišné a uživateli neznámé, jelikož know-how výrobců bývá tajné. Nejprve je nutné definovat nominální hodnotu C/N_{0_nom}.Tato bohužel nemůže být spočtena pomocí komunikační rovnice z důvodu velkého počtu faktorů, ovlivňujících propagaci signálu. Z tohoto důvodu je k výpočtu C/N_{0_nom} použito velké množství přijímačem experimentálně naměřených dat.

C/No se mění v závislosti na poloze vysílajícího satelitu. Nejvyšších hodnot dosahuje, pokud je přímo nad přijímačem, jak je vidět vlevo na obrázku 17. Vpravo je vidět C/N_o v krátkých časových (sekundových) intervalech, ve kterých je možno C/N_o brát jako konstantní hodnotu. Pokud se získá dostatečně reprezentativní vzorek těchto hodnot,

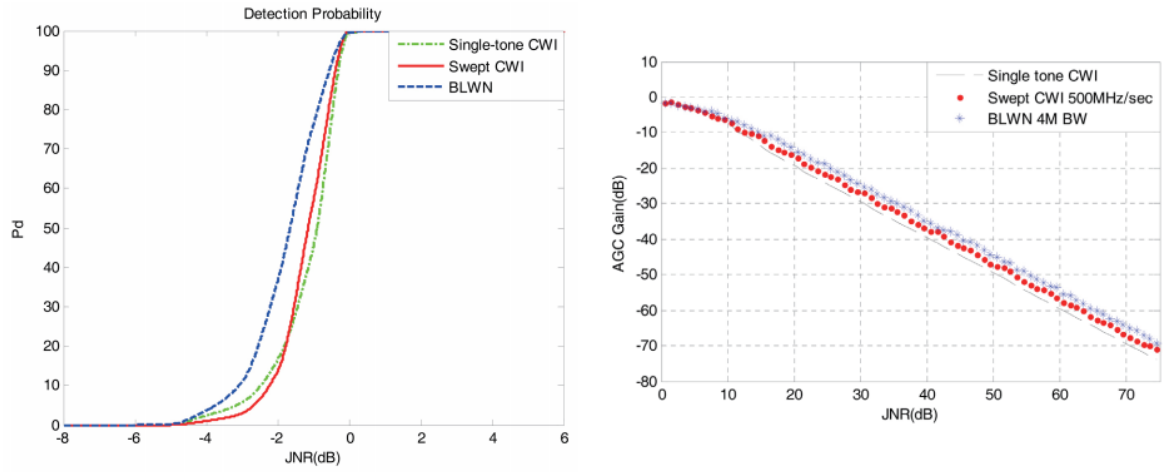


Obrázek 17 - Vlevo nahoře - závislost C/No na čase, vlevo dole - závislost elevace satelitu na čase; vpravo – C/No je v malých časových úsecích konstantní [42]

bude mít normální rozdělení. Další analýza spočívá v použití plovoucího okénka o šířce N vzorků, ve kterém se průměruje střední hodnota a rozptyl. Zde je důležitý výběr šířky okénka, neboť zde existují protichůdné požadavky. Na jednu stranu chceme co nejmenší rozptyl za normálních okolností, kterého dosáhneme zvětšením okénka, ale na druhou se snažíme o detekci nepředvídaných změn (rušení). Podle uživatelského požadavku na pravděpodobnost výskytu planého poplachu, je pak možno s pomocí vztahů uvedených v [42] stanovit funkci prahové hodnoty závislou na elevaci satelitu a použitém PRN kódu.

5.1.2 Detekce pomocí AGC

Tento způsob detekce využívá AGC – součásti rádiové části přijímače (viz 3.4.1). Úloha AGC spočívá v zesilování signálu na vstupu v závislosti na okolním šumu (nebo i interferenci,je-li přítomna), neboť užitečný signál je hluboko pod hladinou šumu. [43] AGC je citlivé na změny širokopásmového šumu i na interference kontinuální vlnou a na tyto reaguje charakteristickou změnou zisku. Pokud je tedy přijímač vystaven rušení, silnější (interferující) signál přebere ovládání AGC. Graf vpravo na obrázku 18 znázorňuje snižování zesílení v AGC způsobené rostoucí hladinou šumu. Jak je vidět, rušení vlnou o jedné frekvenci snižuje zisk AGC nejvíce, nejméně jej ovlivňuje bílý šum. Pokud tedy před samotným rušícím útokem empiricky naměříme reakci AGC na různé typy interference (charakterizujeme na interferenci) a víme, zda jsme schopni odhadnout její typ, je možno zjistit výkon interference ze zisku AGC a tedy i samotnou veličinu J/N (rušení vůči šumu). [23]



Obrázek 18 – Vlevo: Pravděpodobnost detekce interference v závislosti na JNR (dB) pro různé druhy rušení šumu [44] vpravo: Změna zisku AGC v závislosti na zvyšování výkonu různých druhů rušení (JNR – Jamming to noise ratio) [44]

5.2 Detekce spoofingu

5.2.1 Detekce na základě skokového zvýšení výkonu

Detekovat nepravý signál lze pomocí sledování jistých veličin signálu, které by za normálních podmínek neměly důvod se měnit. Jednou z nich je celkový výkon přijímaného signálu za

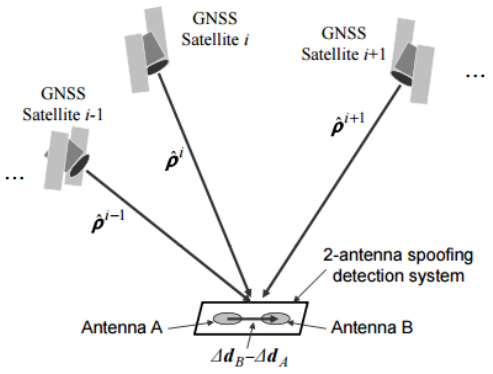
časový úsek. Jak bylo zmíněno v 3.4.2, po synchronizaci korelační funkce nepravého signálu s PRN přijímače, útočník postupně zvyšuje výkon, pod kterým vysílá. Takovýto skok ve výkonu přijímaného signálu je možné identifikovat porovnáváním přijatých hodnot Ai (viz 3.4.2) a referenční hodnoty automatického vyrovnávání citlivosti. Zároveň by naznačoval snahu o spoofing útok, obzvláště pokud by výkonový skok byl větší než 1 či 2 dB. [39]

5.2.2 Detekce sledováním odchylky oscilátoru/pozice

Sledováním časové odchylky lokálního oscilátoru přijímače od systémového času je také možné detekovat potenciální spoofing útok. Způsob spočívá ve sledování chyby hodin přijímače, která, mění-li se příliš rychle oproti standardní předpokládané chybě dané třídy instalovaných hodin (chyby se liší pro krystalové oscilátory, tepelně kompenzované kr. osc., rubidiové osc.), napovídá na probíhající útok podvratným signálem. Další veličinou, jejíž odchylku je možno sledovat je samotná pozice přijímače. Pokud se přijímač propojí s IMU (Inertial Measurment Unit), je možné porovnávat případné nereálné, změny pozice, či rychlosti. Například nemůže být překročena maximální rychlost vozidla, či minimální rádius zatočení lodi apod. Dále je možné, po propojení s kvalitnější IMU, detekovat spoofing (i rušení) pomocí porovnávání svých absolutních pozic. [39]

5.2.3 Detekce na základě vzájemné geometrie

Tento způsob detekce je založen na sledování směru (vektoru ρ^i), ze kterého přichází signál. Aby se tento vektor dal zjistit, je potřeba k přijímači připojit pole antén s nejméně třemi anténami s různými vzdálenostmi od přijímače. Moderní přijímače dokáží určit fázi nosné vlny ϕ_i s takovou přesností, že je možné dostat se na hodnoty se standardní odchylkou pouze 3° za použití vzdáleností mezi přijímačem a anténou ~ 0,1 m. Za normálních podmínek ukazují vektory ρ^i rozprostřeně na viditelnou oblohu, v závislosti na tom, v jaké konstelaci jsou družice GNSS (viz obrázek 19). Takováto detekce je vhodná zejména proti vysílačům falešného signálu, které jsou vybaveny jednou anténou. [39]



Obrázek 193 – Vektory ρ^i za normálních okolností [39]

6 Možnosti ochrany ze strany přijímače a autentikační techniky

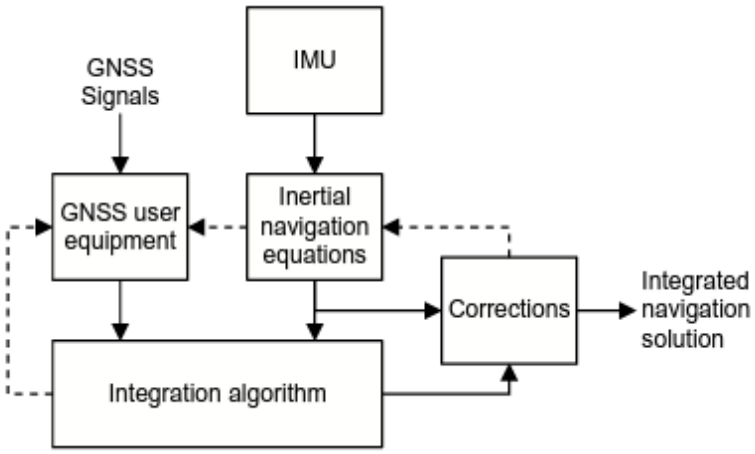
6.1.1 Propojení s INS

Inerciální navigační systém (INS) je přístroj používající informace o akceleraci a rotaci pocházející z inerciální měřící jednotky (IMU) k výpočtu relativní pozice, natočení vůči referenčnímu systému a rychlosti vzhledem k referenčnímu bodu. IMU se skládá ze tří akcelerometrů měřících lineární akceleraci podél přidělené osy a ze tří gyroskopů měřících rotační akceleraci. Velkou výhodou, kterou inerciální navigace poskytuje, obzvláště v našem případě, je její neovlivnitelnost rádiovým vysíláním a vysoká frekvence vypočtených pozic na výstupu. Nevýhodou, která neovlivnitelnost vyvažuje, je postupná kumulace chyb v čase při určování pozice a nutnost počáteční inicializace polohy (neboť IMU určuje polohu relativně). Díky zmíněné kumulaci chyb musí být jednotka během svého chodu průběžně reinicializována, právě třeba pomocí GNSS, která naopak vykazuje nižší přesnost v krátkých časových úsecích. Jak je tedy vidět, jsou výhody a nevýhody INS a GNSS poměrně komplementární. [45]

Jsou rozlišovány hlavní dva způsoby propojení INS s GNSS – volné a těsné.

Volné propojení

Pokud je GNSS propojeno s INS volně, pak obě části pracují jako nezávislé navigační systémy. Z výstupů obou systému jsou sbírány informace a ty jsou pomocí algoritmu dávány dohromady. Existují dvě verze volného propojení. Uzavřená konfigurace implementuje zpětnou vazbu, která kompenzuje chybné navigační řešení vzniklé kumulací malých chyb měřících členů. V otevřené konfiguraci taková zpětná vazba nefunguje. Aby dávalo volnézapojení smysl, musí být použita kvalitní INS, jinak nemůže být považována za nezávislé navigační řešení, neboť by se správnost jejího výstupu rapidně zmenšovala díky rychlé kumulaci chyb. Volné propojení poskytuje přesnější a robustnější řešení než samotná služba GNSS a není složité na implementaci. Nevýhodou je vysoká cena za kvalitní INS. [46]



Obrázek 20 – Schéma volného propojení INS a GNSS v uzavřené konfiguraci [19]

Těsné propojení

V těsném propojení již neexistují dvě nezávislá (nebo v případě uzavřené konfigurace skoro nezávislá) navigační řešení jako tomu bylo v případě propojení volného. INS (v tomto případě pouze IMU) a GNSS přijímač zde fungují pouze jako senzory – u GNSS přijímače je přijímaný signál zpracován na základě hodnoty pseudovzdáleností, IMU dodává data o zrychleních ve směrech os a úhlových rychlostech souřadnicové soustavy. Tato data (pseudovzdálenosti a zrychlení) jsou poté používána k vytvoření jednoho navigačního řešení.

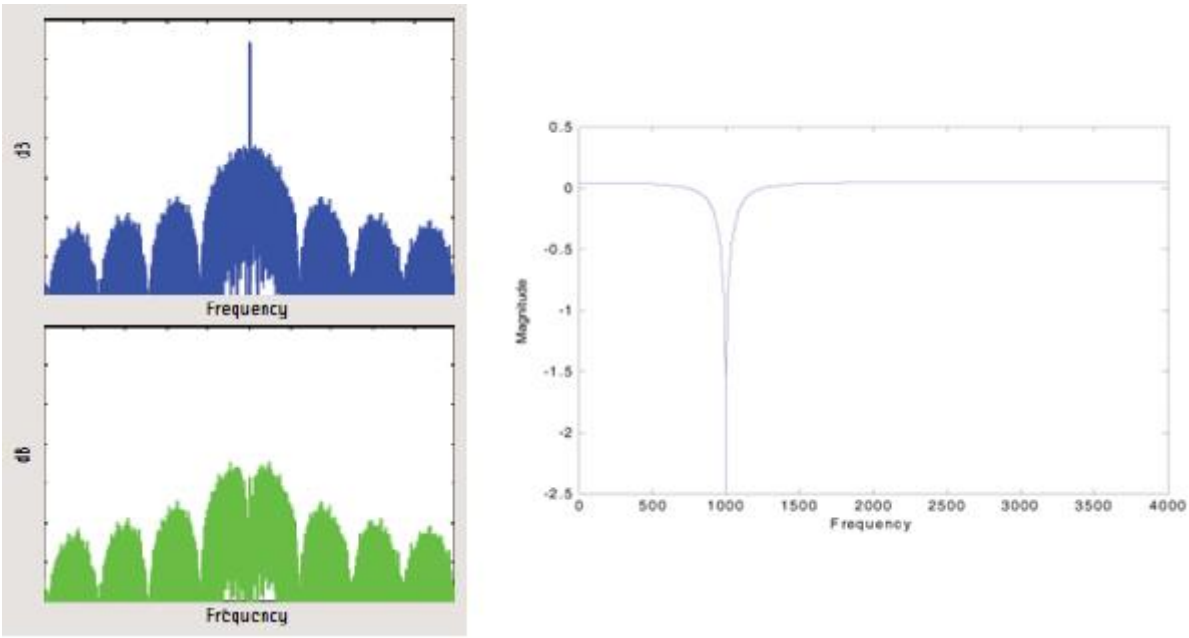
Obecně jsou řešení poskytovaná těsným propojením přesnější a odolnější vůči vnějším vlivům (robustnější). Jednou z věcí, co činí systém robustnějším, je schopnost vytvářet použitelné navigační řešení za situace, kdy je vidět méně než 4 satelity (min. potřebný počet pro výpočet pozice pouze pomocí GNSS). Za této situace bude dostupné navigační řešení, kterému se ale budou kumulovat chyby nejen z IMU, ale i z nepřesnosti oscilátoru přijímače. Další výhodou je možnost použití levnějších IMU než v případě volného propojení a navigační řešení těsně propojeného systému IMU-GNSS je pak možné porovnávat s pozicí vypočtenou pouze pomocí GNSS. Nevýhodou je vyšší složitost systému a v případě chybné IMU i permanentně negativně ovlivněná kvalita navigace. [46]

6.1.2 Charakterizace zisku AGC propojená s pásmovou zádrží

V 5.1.2 byla popsána možnost charakterizace zisku AGC v závislosti na druhu použité interference. Po propojení AGC s filtrem úzkopásmové zádrže, je možno vytvořit systém zamezující rušení v úzkém pásmu. Tento způsob ochrany je poměrně přímočarý – snaha spočívá ve vyfiltrování rušivého signálu.

Filtrování úzkopásmou zádrží (notch filter, obrázek 21) je destruktivní proces vhodný pouze k potlačování rušení kontinuální vlnou. Filtrováním se ztrácí část satelitem vysílané informace, a tak je tato metoda nevhodná pro ochranu proti širokopásmému rušení. [34] S použitím

rekurzivního algoritmu nejmenších čtverců (RLS - podrobněji popsáno v [44]) lze odhadnout středovou frekvenci rušení kontinuální vlnou a případně ji „sledovat“, pokud je její středová frekvence např. lineárně modulovaná.



Obrázek 214 – vlevo, nahoře:signál GNSS rušený jedním tónem, dole: po použití úzkopásmé zádrže [34] vpravo:charakteristika úzkopásmé zádrže [44]

Algoritmus, který má za úkol charakterizaci rušení, porovnává nejdříve zisk AGC se zvolenou referenční hodnotou. Pokud tato hodnota zisku není překročena, není důvod obavy z rušícího útoku. Pokud naopak přerušena je, porovnává se hodnota parametru získaného algoritmem RLS – tímto je možné rozlišit mezi rušením bílým šumem a kontinuální vlnou. Třetí rozhodovací krok porovnává standardní odchylku s referenční hodnotou odchylky. Pokud je větší, je interference klasifikovaná jako rušení vlnou s proměnnou (většinou lineárně modulovanou) frekvencí, jinak jako rušení kontinuální vlnou. [44]

6.1.3 Přepínání frekvencí/konstelací

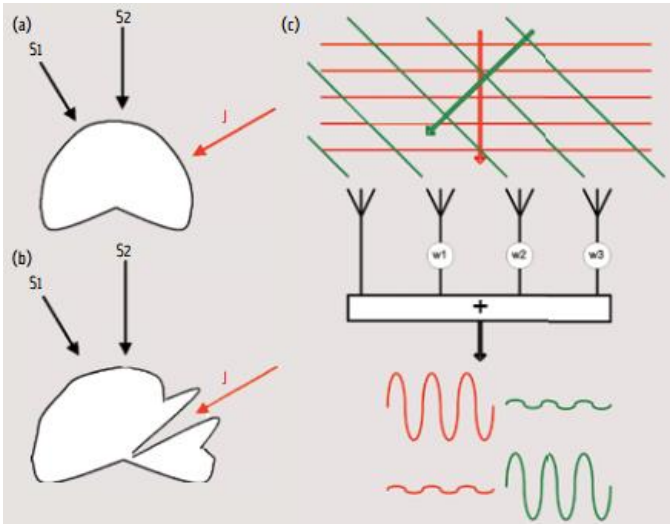
V případě, že je GNSS kanál rušen, je možno přepnout na jinou frekvenci – pokud existuje, či je dostupná. GPS zatím neposkytuje druhý civilní signál. L2C (1227 MHz) není plně operativní, nachází se v testovací fázi (zatím je vysílán z 19 satelitů, z 24 by měl být vysílán okolo roku 2018). Signál L5 (1176 MHz), speciálně vytvořen pro civilní letecké aplikace, by měl být uveden plně do provozu v roce 2024, s tím, že je nyní vysílán ze 12 satelitů. [47] Galileo bude poskytovat možnost dvou civilních signálů v případě zaplacení CS (Commercial Service na 1273,75 MHz), jinak poskytuje pouze službu na E1(L1). GLONASS samotný, díky použití FDMA, je odolnější vůči úzkopásmé interferenci, nicméně, jak bylo v předešlém textu uvedeno, také se chystá, z důvodu interoperability systémů, přechod na CDMA. Nicméně nyní vysílá

dva FDMA signály použitelné civilním sektorem a to na 1602 (± 3,375) MHz a na 1246 (±2,625) MHz. [48]

Nyní je tedy možnost takovéto ochrany dostupná pouze pro vojenský sektor. Přepínání mezi frekvencemi ale bude možné i pro civilního uživatele v časovém horizontu několika let. Zatím je tedy možné pouze použití multikonstelačního přijímače (tedy GPS + GLONASS). V roce 2020 přibyde ještě Galileo, tím se možnosti rozšíří [49]. Nevýhodou tohoto způsobu ochrany je fakt, že výroba multikonstelačního přijímače je dražší než výroba rušičky, která pokrývá více frekvencí. [34]

6.1.4 Null steering

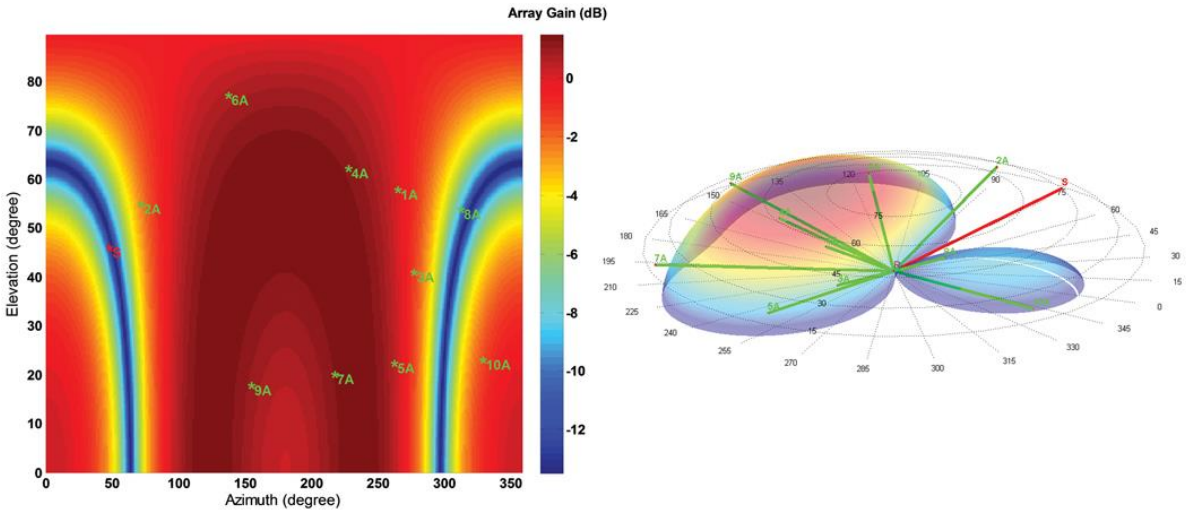
I v případě rušení lze využít faktu, že signály od satelitů přicházejí z různých směrů a případné rušení pouze z jednoho. Na tomto základě staví anténová protirušící technika nazývaná „null steering“. Princip je následující: místo klasické antény s hemisférickou směrovou charakteristikou je použita tzv. adaptivní anténa – tato se skládá z několika menších antén instalovaných v určitých vzdálenostech, jejichž výstup se sčítá.



Obrázek 22 - Princip adaptivní antény, vlevo nahoře:směr. char. klasické antény, dole: směr. char. adaptivní antény; vpravo: schéma principu [34]

Obrázek 22 ilustruje proměnitelnou směrovou přijímací charakteristiku adaptivní antény. Pokud je zaznamenáno rušení, upraví se přijímací charakteristika antény tak, aby byl minimalizován její zisk ve směru, odkud rušení přichází. Směr, odkud signál přichází, je určen pomocí rozdílných časů, kdy dopadá na jednotlivé dílčí antény. V závislosti na tomto směru je pak možno sčítat signály konstruktivně (se silným výstupem) nebo destruktivně (se slabým výstupem). Aby se zabránilo příjmu interferenčních signálů a jelikož jsou signály GNSS skryté pod hladinou šumu (mají nízký výkon), je snaha antény výkonově minimalizovat svůj výstup (rušení se předpokládá silnější než GNSS signály). Null steering lze použít i na ochranu vůči spoofingu, neboť narozdíl od pravých signálů, signály podvratné (za předpokladu, že je signálů

modulovaných různými PRN kódy ze spooferu vysíláno více), pokud jsou vysílány pomocí jedné antény, budou incidovat s anténami přijímače z jednoho směru. Jestli tomu tak je (vysílání více signálů z jednoho směru), lze zjistit rozdílem fází nosných vln při incidencích se subanténami tvořícími adaptivní anténu. V případě nepravých signálů totiž budou tyto rozdíly fází stejné. [34]



Obrázek 23 - Vlevo: Zisk adaptivní antény v závislosti na azimutu a elevaci, vpravo: 3d schéma situace [50]

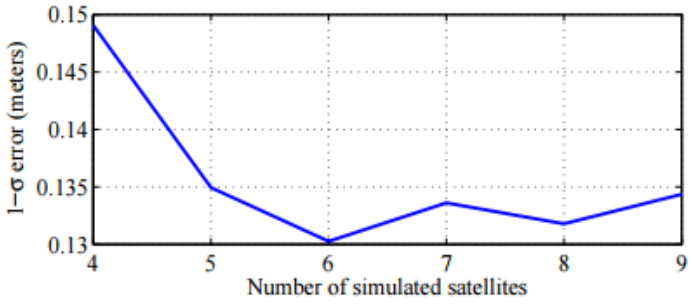
V [50] byl proveden test, ve kterém bylo vysíláno 10 pravých, různě rozmístěných GPS signálů a 10 nepravých signálů vysílaných z jedné pozice. Podvratné signály byly vysílány pod větším výkonem - průměrný u pravých signálů činil -128,5 dBm a u nepravých -126,5 dBm. Na obrázku 23 je zobrazena situace pokusu (červená úsečka vyznačuje směr nepravých signálů) a zisk adaptivní antény s vyznačenými směry přijímaných signálů. Jak je vidět, útlum podvratných signálů činí okolo 11 dB (výkonpřijatých pak činí -137,5 dBm).

6.1.5 Příležitostné využití ostatních radiových signálů

Pro zvýšení odolnosti vůči útokům podvratným signálem je možné využít ostatních existujících rádiových signálů, které ani nemusí být zamýšlené pro navigaci, ale jdou použít pro přibližné určení polohy. Mezi tyto signály patří samozřejmě ostatní GNSS, či regionální navigační systémy (např. QZSS), signály z mobilních BTS či signály ze satelitů pro satelitní telefony (satelity Iridium). Z těchto signálů lze vypočíst přibližná poloha (nepřesná, pokud není dostupná žádná satelitní navigační služba). Jelikož přijímače dostupné na trhu z převážné části nedisponují ochranami proti spoofingu a jelikož by u některých implementací byla výměna přijímačů finančně náročná, existuje koncept „Assimilator“. Projekt spočívá v připojení externího modulu k radiovému vstupu přijímače. Tento modul by syntetizoval GNSS signály z výše uvedených zdrojů a ty by dodával na vstup příjímače.

Vysílání by dávalo největší smysl na L1 s kódem C/A, neboť tento umí přijímat skoro všechny přijímače. Přesnost určení pozice může být zvýšená díky možnosti simulovat optimální

geometrii konstelace. Neplatí ale přímá úměra čím více simulovaných signálů, tím větší přesnost (viz 2.5), jelikož každý další simulovaný signál snižuje C/No (signály mezi sebou interferují). Nejlepším možným počtem simulovaných signálů je 6, jak je vidět z obr. 21.



Obrázek 24 - 1-sigma v závislosti na počtu simulovaných satelitů [51]

Rušení takto vybaveného přijímače je mnohem složitější proces, neboť signály mobilních sítí, satelitů Iridium a dalších jsou o desítky dB silnější než signály GNSS a pracují na jiných frekvencích. Spoofing se také zkomplikuje, díky nutnosti syntetizovat více typů signálů najednou. [51]

6.2 Autentikace signálu

Pro ztížení provedení spoofing útoku existuje celá řada navrhovaných autentikačních systémů. Systém autentikace signálu zaručuje uživateli, že signály obdržené jeho přijímačem jsou pravé. Takovýto systém by učinil provedení spoofing útoku pro útočníka komplikovanějším, díky složitější duplikaci pravých signálů. Zatím žádná plně operační konstelace (GPS, GLONASS) nemá implementovaný systém autentikace pro civilní signály, který by zaručil, že signál, který uživatel přijímá, je pravý. Služba CS konstelace Galileo by měla být autentikována pomocí šifrovaných rozprostíracích kódů (SCE) přístupných pouze uživatelům CS. [52] Dále GSA zkoumá implementaci kombinace NMA a SCE v CS. [53] Pro všechny uživatele bude ve službě OS zprovozněna autentikace pomocí NMA. [54]

6.2.1 NMA

Jedním z datových autentikačních schémat je Navigation Message Authentication (NMA). K datové navigační zprávě se přidávají ověřovací zprávy, které dokazují pravost zdroje. Potenciální útočník by neměl být schopen nasimulovat ověřovací zprávu NMA, jelikož by nedisponoval klíčem nutným ke generování zpráv. Nechráněné přijímače, které v sobě nemají implementovaný systém ověření pravosti dat pomocí NMA, by fungovaly stejně, jako fungují civilní přijímače dnes – části NMA datové části by byly ignorovány a nebyla by zaručována autentická data. Certifikovaný přijímač vybavený algoritmem pro zpracování NMA by byl schopen zaručit autenticitu dat. [55]

6.2.2 SCE

SCE je koncept autentikace užívající šifrování rozprostíracího kódu pomocí symetrického klíče a dané posloupnosti číslic. Demodulace signálu z rozprostřeného spektra je tak tedy možná pouze, pokud je uživateli přístupný onen symetrický klíč. Smysluplné fungování systému SCE je podmíněno existencí zabezpečeného mechanismu distribuce a provozování klíčů. [55]

6.2.3 Metrika hodnocení autentikačních systémů

Navrhované autentikační systémy jdou hodnotit dle:

- Výkonu systému – Time To Authentication (TTA) – čas, po který trvá systému zjistit anomálii a reagovat na ni. Tento čas by tedy měl být co nejkratší, neboť během nějje přijímač pod vlivem rušení či spoofingových aktivit.
- Pravděpodobnost selhání – určuje kvantitativně důvěru, kterou můžeme vložit do správného fungování systému. Tato hodnota tedy zahrnuje pravděpodobnosti nedetekování provedeného útoku a detekce útoku neexistujícího.
- Robustnost – určuje schopnost systému odolávat útokům a zmírňovat jejich následky.
- Interoperabilita – schopnost systému pracovat správně při implementaci v různých aplikacích a prostředích [56]

7 Užití GNSS ve veřejné dopravě

V této kapitole jsou uvedeny vybrané oblasti veřejné dopravy ve kterých jsou využívany systémy GNSS. V práci záměrně vynechávám veřejnou vodní dopravu, neboť zastává, obzvláště v České republice okrajovou roli.

7.1 Nekritické aplikace

7.1.1 Městská a příměstská hromadná doprava

Informace cestujícím, návaznost linek a hodnocení kvality služeb dopravce

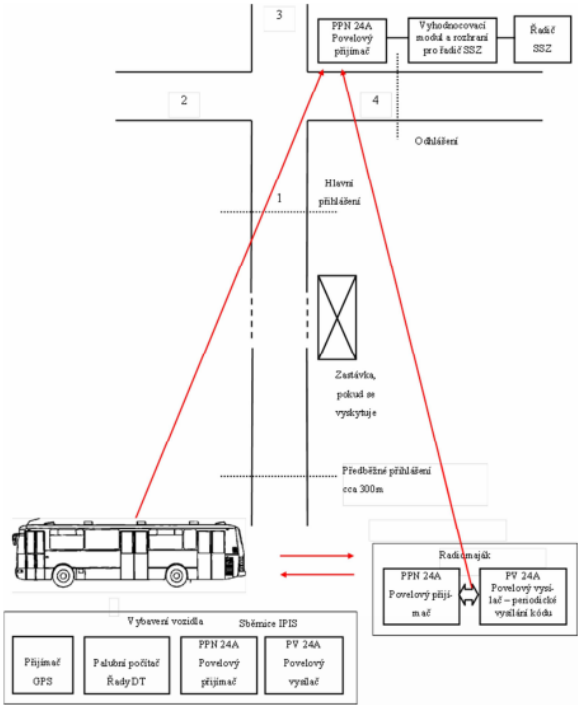
V systému jsou zasílána data o poloze a rychlosti vozidla pořízená palubním modulem GPS zasílána do centrálního dispečinku. Zde jsou na základě pořízených vozidlových dat identifikovány návaznosti, které nemusí proběhnout díky zpoždění jednoho z vozidel. Dispečeři pak následně mohou na základě identifikovaných rizikových návazností zaslat řidiči příkaz prodloužení čekací doby na opožděný spoj, pokud to situace vyžaduje. Informace o zpoždění jednotlivých spojů jsou také poskytovány cestujícím prostřednictvím zobrazovacích jednotek na zastávkách linek mobilní aplikace. Takovýto systém provozuje například integrovaný dopravní systém jihomoravského kraje. [57] Informace o poloze vozidla není nikterak kritická, nedostupnost informací je pro cestující pouze nepříjemnost – řidiči vozidel mají za povinnost dodržovat jízdní řád. Garantované přestupy jsou také dány jízdním řádem. Dále je satelitní navigace využívána také jako nástroj k hodnocení kvality služeb dopravce. Zde je GNSS využíváno pro získávání dat o zpožděních či předčasných odjezdech vozidel daného dopravce. Tato data pak hrají roli ve finančním vyrovnání mezi dopravcem a objednací stranou.

Preference MHD

Díky křižovatkám s instalovanou preferencí MHD jsou zkráceny čekací časy vozů veřejné městské dopravy. Na obrázku 25 vidíme schéma křižovatky vybavené systémem pro preferenci vozidel MHD založeného na principu určování polohy vozidla pomocí GNSS.

Každý vůz MHD je vybaven přijímačem GNSS připojeným na datovou sběrnici vozidla. Při průjezdu místem předběžného přihlášení, což je místo pevně definované pomocí souřadnic a uložené v databázi palubního počítače vozidla, vyšle rádiovou zprávu například na frekvenci 86,79 MHz (existuje více použitelných frekvencí) radiomajáku, který ji dále předá řadiči SSZ. Poloha místa předběžného přihlášení se volí ve vzdálenostech několika set metrů před samotnou křižovatkou. Více o přesnosti GNSS v městské zástavbě v [58].

Pokud se mezi bodem předběžného přihlášení a křižovatkou nachází zastávka, vysílá vozidlo MHD směrem k SSZ zprávu o zavření dveří. Oblast hlavního přihlášení se nachází v definováném okruhu kolem bodu v definované vzdálenosti od křižovatky (jejího středu). [59]



Obrázek 25 - Schéma preference MHD na bázi GNSS [59]

7.1.2 Železniční doprava

Řízení návaznosti – uvedeno výše v 7.1.1

Zpřesnění odometrie ETCS

Současné systémy odometrie existují v podobě palubních senzorů – IMU, tachometry, dopplerovské radary. Poloha vlaku se v ETCS získává přičtením najeté vzdálenosti k poslednímu referenčnímu bodu – eurobalíze. Z důvodů uvedených např. v [60] je určení rychlosti v některých případech nedostatečně přesné. Zde by bylo vhodné využít dostupné systémy GNSS s přidanou službou integrity a zvýšené přesnosti poskytované systémem EGNOS, které by zvyšovaly přesnost hodnoty rychlosti a ujeté vzdálenosti vlaku určené dosavadními systémy.

7.2 Kritické aplikace

7.2.1 Letecká doprava

Přiblížení k letišti

GNSS s podporou GBAS může být použit jako navigační nástroj pro přiblížení letadla k letištní dráze. Buďto může doplňovat již existující infrastrukturu, anebo může být implementován na

menších letištích jako levnější verze pozemní výbavy nutné pro přistání ILS. Přiblížení se dělí na přesné a nepřesné. Přesné má za úkol navádět letadlo na přistávací dráhu pomocí kurzu a strmosti sestupu, zatímco nepřesné přiblížení pouze navede pilota dostatečně blízko k dráze, aby byl schopen provést přistát za podmínek VFR. [61]

Nicméně komerční letadla veřejné dopravy jsou stále vybavena systémy ILS využívajících pozemní VOR majáky k přiblížení. Jelikož VORy vysílají pod značně vyšším výkonem než je síla GNSS signálu u zemského povrchu, je složitější je zarušit či zmást palubní ILS nepravým signálem. Toto zdvojení systémů přiblížení k letišti poskytuje možnost porovnávat jejich výstupy a tímto zvýšit bezpečnost letadla proti útokům na služby GNSS. [62]

Řízení letového provozu

ADS-B je systém na vysílání informací o vlastní pozici letadla ostatním letadlům a pozemní infrastruktuře v oblasti civilního letectví. Systém by měl v příštích letech nahrazovat radary jako hlavní způsob určení pozice a rychlosti letadel. Letadla vybavena ADS-B získávají informace o jejich současné poloze z GNSS a ty vysílají společně s údaji o rychlosti a identifikací. Systém by měl prudce zvýšit přehlednost situace pro pilota díky možnosti přeposílat si informace například o počasí mezi jednotlivými letadly. [63] Doba, do které je povinnost vybavit letadlo ADS-B se v různých částech světa liší. V USA by ale do roku 2020 měla být převážná většina letadel systémem vybavena. [64]

Letadla veřejné dopravy bývají vybavena kvalitními IMU, které mohou být použity pro kontrolu pozice určované GNSS. [62]

7.2.2 Železniční doprava

I přes fakt, že kolejová doprava je ze všech zmiňovaných doprav s implementací GNSS řešení nejvíce pozadu, existují snahy o snížení nákladnosti železniční infrastruktury právě s pomocí systémů využívajících GNSS. Zavedení takových systémů by zjednodušilo určení aktuální polohy vlaku. Také by bylo možno zavedení menších rozestupů, mezi jednotlivými vlaky. Z důvodu přísných požadavků na bezpečnostně kritické systémy, jako výše uvedené, nemohou tyto systémy spoléhat na informace poskytované systémy GNSS, ani po spřažení s INS. Problém pro systém založený na GNSS vzniká hlavně díky problematickému prostředí, ve kterém se vlaky pohybují (tunely, lesy apod.). Pokud odhlédneme od těchto kritických aplikací, je možné GNSS využívat v informačních systémech, jejichž výstupy jsou využívány jak výpravčími/dispečery, tak cestujícími. [65]

V Evropě je snaha o standardizaci vlakových zabezpečovacích systémů. Evropský univerzální zabezpečovač ETCS používá k udělování jízdních povolení a sledování polohy vlaku systém

eurobalíz a GSM-R. Takovýto systém je poměrně nákladný, složitý a ve vysokých rychlostech se dokonce ukázalo nepřesný v měření rychlosti vlaku.

Automatické vedení a sledování vlaku

Na regionálních tratích, kde je nízká intenzita provozu, by bylo ekonomicky značně nevýhodné budovat systém automatického vedení vlaku AVV s magnetickými informačními body (MIB). MIBy určují polohu železničního vozidla v okamžiku jejich přejetí. Místo MIBů by měly být na tratích využívajících AVV s GNSS používány virtuální geodeticky zaměřené body (GIB) [67]. Po propojení systému GNSS s odometrem je možné použít soustavu systémů ke sledování pozice železničního vozdila v reálném čase. Pokud se v dohlížené oblasti sblíží dvě vozidla na limitní vzdálenost, spustí se v obou vozidlech varování. [68] Zodpovědnost je ale zatím stále na strojvedoucím, který musí dávat pozor na návěstění a na trať. Počítá se s pilotním vybavením dvou tratí tímto systémem a to na tratích Brno-Jihlava a Jaromeř-Trutnov. [69]

Zabezpečení regionálních tratí

Pro regionální trati, na kterých existuje snaha o minimalizaci nákladů na zabezpečení, je vyvíjen společností AŽD Praha systém Radioblok. Toto zabezpečovací zařízení funguje na principu vydávání povolení železničním vozidlům. Pokud by strojvedoucí přejel hranici úseku, pro který má povolení, systém Radioblok zastaví vozidlo vypuštěním vzduchu z brzd. Systém GNSS je zde použit právě pro kontrolu polohy vozidla – sleduje, zda je v úseku pro který má dané vozidlo povolení od dispečera. Systém GNSS je zde tedy nasazen jako záloha lidského činitele. Jelikož lidský činitel je častou příčinou mimořádných událostí napříč všemi módy dopravy, zařadil jsem tuto aplikaci GNSS mezi „kritické“ aplikace. V ČR je zatím Radioblok v ověřovacím provozu na trati Číčenice – Volary. [69] [70]

8 Návrhy implementace ochran

V této části práce jsou nejdříve odhadnuty dopady útoků na přijímače GNSS v různých aplikacích veřejné dopravy. Dále jsou vytvořeny návrhy na ochrany proti rušícím/spoofing útokům. Tyto ochrany by mohly mít za následek zvýšení bezpečnosti dopravy v dané aplikaci a její větší robustnost proti útokům na signály GNSS. Na rušení reagují přijímače různými způsoby (viz tabulka 5) – v závislosti na síle a přijímači, můžou být uživateli předávána buď data chybná anebo žádná.

8.1 Odhad dopadů útoků ve veřejné dopravě

Tabulka 5 - Předpokládané odezvy systémů využívající GNSS na rušení/spoofing

	Interference	Spoofing
Nekritické aplikace		
Informace cestujícím a návaznost linek	Výpadek informací pro cestující, dispečeři neschopni řídit návaznosti	Falešné informace o zpoždění vozidel
Preference MHD	Nefunkčnost/chybná preference	Zmatení signálních programů křižovatek – prodloužení cestovních dob všech účastníků provozu
Zpřesnění odometrie ETCS	Nefunkčnost systému, nutnost spolehnutí se na odometr apod.	Nutnost spolehnout se na odometr při velké odchylce GNSS odometru
Kritické aplikace		
Přiblížení k letišti	Možné zmatení pilota, nutnost použít VOR, srovnávací navigaci	Možnost havárie při špatné viditelnosti
Řízení letového provozu	Nemožnost vysílat svou pozici	Možnost havárie
Automatické vedení a sledování vlaku	Neoptimální/potenciálně nebezpečné vedení vlaku	Možnost havárie – např. moc vysoká rychlost v oblouku
Zabezpečení regionálních tratí	Neexistující záloha lidského činitele - strojvedoucího	Možnost havárie díky nesprávným přijímaným informacím

8.2 Zhodnocení dopadů a pravděpodobnosti útoků

Sledování vozidel a informace o odjezdech linek

Při rušení služby sledování vozidel a návaznosti linek je omezena možnost koordinace návazností v reálném čase a dohled nad vozidly. Tímto nevzniká žádný zásadní problém – pouze mírné zhoršení kvality dopravní obslužnosti – stále platí „papírové“ jízdní řády, podle kterých se mohou řidiči orientovat. Jedinou skutečně zasaženou službou by byla nedostupnost informací o zpoždění spoje uživatelům dopravního systému. Instalace jakýchkoli systémů detekce, či ochran se zdá nepotřebná.

Útok podvratným signálem je velice nepravděpodobný – komplexnost provedení naprosto převažuje jakoukoli motivaci takovýto útok provést.

Preference MHD

Nedostupnost služby způsobená rušením má za důsledek nefunkční preferenci – vozidlo MHD nevyšle řadiči křižovatky signál o své přítomnosti, či chybnou preferenci – vozidlo vyšle signál na nepravém místě. Pokud by bylo rušení GNSS zaznamenáváno často, bylo by záhodné instalovat systém detekce rušení, který by v případě detekování interference zakázal vysílání přihlašovacího signálu či využít multikonstelační přijímač, který by bylo složitější zarušit.

Zasílání nepravého signálu vozidlům MHD má také potenciál způsobit dopravní kongesce. Tento případ je opět velice nepravděpodobný díky komplexnosti útoku a díky možnosti dosáhnout podobného výsledku použitím rušiček.

Přiblížení k letišti

Letadla využívána provozovateli osobní letecké dopravy jsou vybavena systémem na přijímání signálu z majáků VOR a tak nejsou závislá pouze na přiblížení pomocí GNSS. Přesto je nevhodné nechat systém bez odpovídajících ochran, neboť zarušením signálu GNSS při přiblížení k letišti, ať přesném či nepřesném, se zvyšuje psychický tlak na pilota v nejnáročnější části letu. Nezbytné jsou systémy detekce rušení, aby mohl v případě útoku pilot využít přiblížení pomocí radiomajáků. Detekce spoofingu by se zdála být také vhodnou, nicméně, domnívám se, že stačí počkat na zprovoznění Galilea a jeho systémy autentikace ať v OS či CS. V případě, že by takové opatření nedostačovalo, bylo by možno instalovat systém detekce rušení.

Řízení letového provozu

V případě rušení by nebylo ADS-B schopno vysílat svou pozici ostatním letadlům ani pozemní infrastruktuře. Rušení ze zemského povrchu je nejspíše proveditelné díky nízkému výkonu potřebnému k zarušení přijímače (viz 4.1.6). Nicméně útočník by musel počítat s vysíláním pod vyšším výkonem už jen díky faktu, že anténa je umístěna na horní části trupu (záporný zisk, viz obrázek 6) rychle se pohybujícího letounu. Pro útočníka ještě ale existuje možnost propašování rušičky přímo na palubu letadla. Díky tomu je naprosto nezbytné implementovat systém detekce rušení – v jeho případě by byla poloha letadla určována pomocí radarů. Tento by mohl být doplněn sadou ochran dle potřeby. Samotné ochrany ale nejsou bezprostředně potřebné, neboť v případě detekce rušení může letoun začít využívat službu určování polohy pomocí radarů.

Pokud by palubní ADS-B začal vysílat nesprávnou polohu, tato by se řetězově šířila přes vysílače ADS-B dalších letadel dále. Tímto by mohlo dojít k ohrožení bezpečnosti letounů v oblasti, kde je vysílán nepravý signál. Provedení útoku by útočníkovi zkomplikovala autentikace systému Galileo.

Zpřesnění odometrie ETCS

Rušení přijímače má za následek chybné hodnoty na výstupu přijímače anebo, pokud je dostatečně silné, hodnoty žádné. V této aplikaci je GNSS přijímač spřažen s dalšími způsoby zjištění rychlost (odometr atd.), tudíž stačí odstavit jednotku přijímače v případě velké odchylky hodnot rychlosti. Stejný postup platí pro vysílání podvratného signálu. V tomto případě tedy není potřeba žádných přídavných ochran, systém by ale mohl benefitovat z autentikace Galilea.

Automatické vedení vlaku

V systému AVV využívající GNSS je detekce rušení žádoucí, aby mohl strojvůdce v případě zarušení bezpečně převzít řízení. Pokud by přijímač chybně vyhodnotil svou pozici pod vlivem nepravého signálu, mohlo by dojít např. k vykolejení soupravy díky vysoké rychlosti v oblouku. Z tohoto důvodu je záhodno více se zabývat v této aplikaci obranou proti spoofingu a jeho detekcí. Dále by bezpečnost systému zvýšila autentikace Galilea.

Zabezpečení regionálních tratí

V této zabezpečovací aplikaci je detekce rušení i spoofingu nezbytná. V případě rušení by nefungovala záloha lidského činitele a tím by byla bezpečnost celého systému notně oslabena. Vysíláním nepravých signálů by při nepozornosti strojvedoucího nebo neznalosti trati (relativně nízká pravděpodobnost, neboť radioblok má být nasazen na reginálních tratích s nízkou intenzitou provozu) mohlo dojít k srážce vlaků způsobené vyjetím železničního vozidla

z úseku, pro který mělo povolení. Bylo by vhodné použít multikonstelační přijímač pro vyšší bezpečnost a přidané komplexnosti pro provedení útoku podvratným signálem v případě použití systému Galileo (autentikace).

Tabulka 6 - Doporučení pro zvýšení bezpečnosti v aplikacích GNSS veřejné dopravy. Červeně jsou vyznačeny systémy které byly na základě předešlé analýzy určeny jako velmi vhodné pro implementaci. Vhodné doplňující systémy jsou vyznačeny zeleně (dražší varianta)

	Detekce		Autentikace	Ochrana
	Interference	Spoofing		
Informace cestujícím, návaznost linek	-	-	-	-
Preference MHD	X	-	X	-
Zpřesnění odometrie ETCS	X	-	X	-
Přiblížení k letišti	X	X	X	X*
Řízení letového provozu	X	X	X	X
Automatické vedení a sledování vlaku	X	X	X	X
Zabezpečení regionálních tratí	X	X	X	X

*letadla jsou již IMU vybavena, je však nutno propojit IMU se systémem na přiblížení pomocí GNSS

9 Závěr

Cílem práce bylo provést analýzu současných možností negativního ovlivnění příjmu signálu GNSS přijímače, způsobů detekce těchto útoků a nabízejících se způsobů ochran. Na základě těchto poznatků byla v poslední části práce vytvořena doporučení pro vybrané aplikace GNSS ve veřejné dopravě.

K dnešnímu dni jsou pouze dva civilní signály GNSS plně funkční – GPS L1 C/A a GLONASS L(G)1 C/A. Tyto signály, jelikož jsou vysílány ze satelitů ve výšce okolo 20 000 km nad povrchem Země, jsou na jejím povrchu velice slabé – dokonce pod hladinou okolníhošumu. Díky tomu není potřeba vysokého výkonu k úspěšnému zarušení signálu ve velké oblasti. Existují tři hlavní způsoby jak zarušit přijímač: přivedení příliš velkého výkonu na vstup přijímače, který ho může poškodit, „oslepení“ – přijímač není schopen nalézt signál vysílaný satelity a rušení takové, při kterém ještě přijímač poskytuje vypočtenou pozici, ovšem nesprávnou, pohybující se v okruhu desítek až stovek metrů od správné pozice. Byl proveden orientační výpočet, jakým výkonem by musel útočník vysílat ze vzdálenosti 10 metrů, aby byl na vstup přijímače přiveden maximální možný výkon, který by mohl přijímač poškodit. Bylo by nutno vysílat výkonem okolo 2 kW, což je hodnota velmi vysoká, a tak jsem se dále tímto způsobem rušení v práci dále nezabýval.

Velkým problémem, který by mohl v příštích letech, nastat je rozšíření osobních rušiček do automobilu/nákladního vozu (PPD). Takové přístroje (ač jsou v převážné většině zemí nelegální) se dají koupit na internetu za ceny v řádech desítek dolarů a jsou schopny zarušení signálu v řádu kilometrů. Tyto rušičky většinou vysílají nějaký druh lineárně frekvenčně modulovaného (chirp) signálu, který ani nemusí frekvenčně spadat do 2 MHz pásma C/A signálu, pokud vysílají dostatečným výkonem, a rušení tak projde přes pásmově propusti přijímače. K akvizici signálu je zapotřebí silnější signál než k úspěšnému sledování signálu, proto je přijímač zranitelnější bezprostředně po svém zapnutí. Jelikož většina civilně dostupných přijímačů nedisponuje žádnými ochranami proti rušení, stávají se nepoužitelnými již při hodnotě J/S přesahující 25 dB.

Celá řada aplikací GNSS ve veřejné dopravě nespoléhá na satelitní navigaci jako jediný systém a má zálohu v podobě systému jiného (INS, odometr, ILS apod.). Pro tyto by mohl dostačovat systém detekce rušení. K zjištění faktu, zda přijímač funguje správně, tedy není rušen, existuje celá řada přístupů. První možností je experimentálním měřením pro daný přijímač vytvořit křivku nominálních hodnot C/N_0 pro satelit v závislosti na jeho elevaci a následně statisticky vyhodnocovat odchylky v těchto hodnotách. Dalším způsobem je využití AGC, které je velmi citlivé na změnu širokopásmého šumu, proto je tento způsob vhodný na detekci širokopásmovou rušičkou, nikoli již tak pro detekci rušení kontinuální vlnou. Další

zvýšení bezpečnosti systému lze provést pomocí instalace přídavných ochran, které lze aplikovat dle potřeb dané aplikace. Je možné použít multikonstelační či v blízké budoucnosti multifrekvenční přijímač, spřáhnout satelitní navigaci s navigací inerciální, filtrovat interferenci v případě rušení kontinuální vlnou anebo nasadit pole antén s adaptivní příjmovou charakteristikou.

Mnohem komplexnějším a potenciálně nebezpečnějším útokem je vysílání nepravých signálů. Útočník v tomto scénáři vysílá signály se stejnými pozorovanými veličinami (zpoždění, fáze), přijímač zachytí tento signál a začne sledovat jej místo signálu pravého. V tuto chvíli může útočník měnit pozorované veličiny signálu a tím měnit přijímačem vypočtenou pozici dle jeho vůle. Takovýto scénář není zatím pravděpodobný, jelikož generátory GNSS signálů jsou velice drahé a rozměrné a postavit takový přístroj dokáže pouze hrstka lidí na světě. Oblasti dopravy, kde by takovýto útok napáchal velké škody (letecká, železniční doprava) se naštěstí nespoléhají pouze na GNSS, ale mají jiné záložní systémy. Pro bezpečný provoz tedy stačí vědět, že přijímač nepřijímá pravá data. Opět jsou vyvíjeny způsoby jak detekovat útok podvratným signálem – detekce pomocí vyššího výkonu přijímaného nepravého signálu, pomocí příliš velké skokové odchylky vnitřního oscilátoru, či pozice přijímače nebo detekce pomocí geometrie přijímaných signálů (potřeba rozměrnějšího pole antén). Zabezpečení proti spoofingu by se mělo v budoucnosti zvýšit společně se spuštěním konstelace Galileo, který bude poskytovat službu autentikace signálu – tedy potvrzení, že přijímač pracuje s pravým signálem.

V poslední části práce byla vytvořena doporučení na základě jednoduché analýzy pro vybrané oblasti veřejné dopravy využívající GNSS služby. Byla vytvořena tabulka odhadovaných dopadů pro rušení a spoofing. Na základě těchto dopadů byla dále uvedena doporučení ve variantě základní a dražší.

Práce je celkovým pohledem na zranitelnost služeb poskytovaných GNSS a ukazuje současné tendence vývoje různých způsobů detekce a ochrany vůči útokům proti signálu satelitní navigace.

10 Seznam použité literatury

[1] GNSS Market report [online]. GSA, 2015, (4) [cit. 2016-08-21]. ISSN 24435236. Dostupné z: http://www.gsa.europa.eu/system/files/reports/GNSS-Market-Report-2015-issue4_0.pdf

[2] MISRA, Pratap a PER ENGE. *Global positioning system: signals, measurements, and performance*. 2. ed. Lincoln, Mass: Ganga-Jamuna Pr, 2006. ISBN 09-709-5441-7.

[3] HOFMANN-WELLENHOF, B, Herbert LICHTENEGGER a Elmar WASLE. *GNSS--global navigation satellite systems: GPS, GLONASS, Galileo, and more*. New York: Springer, 2008, xxix, 516 p. ISBN 978-321-1730-126.

[4] MAZÁNEK, Miloš, Pavel PECHAČ a Jan VRBA. *Základy antén, šíření vln a mikrovlnné techniky*. Vyd. 1. Praha: Česká technika - nakladatelství ČVUT, 2008. ISBN 978-80-01-03997-7.

[5] POOLE, Ian. Signal to noise ratio. Radio-Electronics [online]. [cit. 2016-04-09]. Dostupné z: http://www.radio-electronics.com/info/rf-technology-design/rf-noise-sensitivity/receiver-signal-to-noise-ratio.php

[6] DAMM, Wolfgang. Signal-to-Noise, Carrier-to-Noise, EbNo: on Signal Quality Ratios [online].2010 [cit. 2016-04-14]. Dostupné z: http://www.noisecom.com/~/media/Noisecom/Webinars/SN%20CN%20EbNo.ashx

[7] OLEYNIK, Ekaterina. Glonass status and modernization [online]. Central Research Institute of Roscosmos Federal Space Agency, 2012 [cit. 2016-07-04]. Dostupné z: http://www.unoosa.org/documents/pdf/psa/activities/2012/un-latvia/ppt/1-2.pdf

[8] RAPANT, Petr. *Družicové polohové systémy*. Vyd. 1. Ostrava: Vysoká škola báňská - Technická univerzita, 2002, 197 s. ISBN 80-248-0124-8.

[9] GLOBAL POSITIONING SYSTEMS DIRECTORATE. INTERFACE SPECIFICATION: IS-GPS-200 [online]. 2013 [cit. 2016-03-27]. Dostupné z: www.gps.gov/technical/icwg/IS-GPS-200H.pdf

[10] DOBERSTEIN, Dan. *Fundamentals of GPS receivers a hardware approach*. New York, NY: Springer, 2012. ISBN 978-146-1404-095.

[11] DOBEŠ, Josef a Václav ŽALUD. *Moderní radiotechnika*. 1. vyd. Praha: BEN - technická literatura, 2006, 767 s. ISBN 80-730-0132-2.

[12] SUBIRANA, J., JM. ZORNOZA a M. HERNANDEZ-PAJARES *GNSS signal* [online]. 2011 [cit. 2016-03-27]. Dostupné z: http://www.navipedia.net/index.php/GNSS_signal

[13] New civil signals. *GPS.gov: Official U.S. Government information about the Global Positioning System (GPS) and related topics* [online]. b.r. [cit. 2016-07-04]. Dostupné z: http://www.gps.gov/systems/gps/modernization/civilsignals/

[14] RODRÍGUEZ, José. *On Generalized Signal Waveforms for Satellite Navigation*. Německo, 2008. UNIVERSITY FAF MUNICH.

[15] RODRÍGUEZ, J.A. Galileo Signal Plan. *Esa Navipedia* [online]. University FAF Munich, Germany, 2011 [cit. 2016-03-27]. Dostupné z: http://www.navipedia.net/index.php/Galileo_Signal_Plan

[16] An introduction to GNSS. *Novatel* [online]. b.r. [cit. 2016-07-06]. Dostupné z: http://www.novatel.com/an-introduction-to-gnss/chapter-5-resolving-errors/multi-constellation-and-multi-frequency/

[17] Receiver types. In: *ESA Navipedia* [online]. 2011 [cit. 2016-07-06]. Dostupné z: http://www.navipedia.net/index.php/Receiver_Types

[18] *GPS Antennas: RF Design Considerations for u-blox GPS Receivers [online]. uBlox, 2009 [cit. 2016-05-07]. Dostupné z: https://www.u-blox.com/sites/default/files/products/documents/GPS-Antenna_AppNote_%28GPS-X-08014%29.pdf?utm_source=en%2Fimages%2Fdownloads%2FProduct_Docs%2FGPS_Antennas_ApplicationNote%28GPS-X-08014%29.pdf*

[19] GROVES, Paul. *Principles of GNSS, Inertial, and Multi-sensor Integrated Navigation Systems*. 2008. ISBN 1580532551.

[20] PETOVELLO, Mark a Lawrence R. WEILL. Differences between signal acquisition and tracking. *Inside GNSS* [online]. 2011 [cit. 2016-04-04]. Dostupné z: http://www.insidegnss.com/auto/IGM_janfeb11-Solutions.pdf

[21] PETOVELLO, Mark. Quantifying the performance of navigation systems and standars for assisted-GNSS. *Inside GNSS* [online]. 2008 [cit. 2016-03-30]. Dostupné z: http://www.insidegnss.com/auto/sepoct08-gnsssolutions.pdf

[22] FORSSELL, Börje. The danger of GPS/GNSS. *MyCoordinates*. 2009, (5), 6-8.

[23] KAPLAN, Elliott *Understanding GPS: principles and applications*. Boston: Artech House, 1996. ISBN 08-900-6793-7.

[24] No jam tommorow. *The Economist* [online]. 2011 [cit. 2016-04-14]. Dostupné z: http://www.economist.com/node/18304246

[25] DE BAKKER, Peter *Effects of Radio Frequency Interference on GNSS Receiver Output* [online]. [cit. 2016-04-14]. Dostupné z: http://www.tudelft.nl/fileadmin/Faculteit/CiTG/Over_de_faculteit/Afdelingen/Afdeling_Geoscience_and_Remote_Sensing/MSc_theses/de_bakker07_msc.pdf. Master Thesis. Delft University of Technology Faculty of Aerospace Engineering.

[26] PACE, Scott a Sergio CAMACHO. *GNSS spectrum protection* [online]. 2015 [cit. 2016-04-14]. Dostupné z: http://www.gps.gov/governance/advisory/meetings/2015-10/pace-camacho.pdf

[27] *Coalition to save our GPS* [online]. [cit. 2016-04-14]. Dostupné z: http://www.saveourgps.org

[28] MAXIM INTEGRATED, . *MAX2769B: Universal GPS Receiver*. 2012. Dostupné také z: http://datasheets.maximintegrated.com/en/ds/MAX2769B.pdf

[29] UBLOX, . *MAX-M8: u-blox M8 Concurrent GNSS modules Data Sheet*. 2015. Dostupné také z: https://www.u-blox.com/sites/default/files/MAX-M8_DataSheet_(UBX-13004644).pdf

[30] *Jammer from china* [online]. [cit. 2016-05-07]. Dostupné z: http://www.jammerfromchina.com

[31] KATULSKI, Ryszard, Jaroslaw MAGIERA, Jacek STEFANSKI a Agnieszka STUDANSKA. Research study on reception of GNSS signals in presence of intentional interference. In: 2011 34th International Conference on Telecommunications and Signal Processing (TSP). Gdansk University of Technology: IEEE, 2011, s. 452-456. DOI: 10.1109/TSP.2011.6043691. ISBN 978-1-4577-1410-8. Dostupné také z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6043691

[32] BAUERNFEIND, R., T. KRAUS, A. AYAZ, D. DÖTTERBÖCK a B. EISSFELLER *ANALYSIS, DETECTION AND MITIGATION OF INCAR GNSS JAMMER INTERFERENCE IN INTELLIGENT TRANSPORT SYSTEMS*. University FAF Munich, Germany. Deutscher Luft- und Raumfahrtkongress, 2012.

[33] MITCH, Ryan, Ryan DOUGHERTY, Mark PSIASKI, Steven POWELL, Brady O'HANLON, Jahshan BHATTI a Todd HUMPHREYS Know your enemy: Signal charasteristics of civil GPS jammers. *GPS World* [online]. 2012 [cit. 2016-04-13]. Dostupné z: https://radionavlab.ae.utexas.edu/images/stories/files/papers/jammerCharacterizationGPSWorld_Mitch.pdf

[34] JONES, Michael. The civilian battlefield: Protecting GNSS receivers from interference and jamming. *Inside GNSS* [online]. 2011 [cit. 2016-05-11]. Dostupné z: http://www.insidegnss.com/auto/marapr11-Jones.pdf

[35] NOVATEL, . *ProPak-II RT-2: Specifications*.

[36] KUUSNIEMI, Heidi, Esa AIROS, Mohammad ZAHIDUL H. BHUIYAN a Tuomo KRÖGER. GNSS Jammers: how vulnerable are Consumer grade Satellite Navigation Receivers?. *European Journal of Navigation*. 2012, **10**(2).

[37] *Fastrax IT600 GPS Module* [online]. [cit. 2016-04-19]. Dostupné z: http://www.glynstore.com/fastrax-it600-gps-module/

[38] Fastrax IT600: OEM GPS Receiver Module. 2011. Dostupné také z: http://www.anglia.com/fastrax/datasheets/IT600%20brochure%20rev.0.7.pdf

[39] PSIAKI, M.L. a T.E. HUMPHREYS GNSS Spoofing and Detection. *Proceedings of the IEEE*. 2016.

[40] UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea. UTNews: The University of Texas at Austin. Dostupné také z: http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea

[41] HUMPHREYS, T., B. LEDVINA, M. PSIAKI, B. O'HANLON a P. KINTNER *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer*. The Institute of Navigation, Savanna, Georgia, 2008.

[42] CALCAGNO, R., S. FAZIO, S. SAVASTA a F. DOVIS *An Interference Detection Algorithm for COTS GNSS Receivers* [online]. Turin, Italy [cit. 2016-05-08].

[43] BASTIDE, Frederic, Dennis AKOS, Christophe MACABIAU a Benoit ROTURIER. Automatic Gain Control (AGC) as an Interference Assessment Tool. In: *ION GPS* [online]. Portland, 2003 [cit. 2016-05-09].

[44] YANG, Jeong, Chang KANG, Sun KIM a Chan PARK. Intentional GNSS Interference Detection and Characterization Algorithm Using AGC and Adaptive IIR Notch Filter. *International Journal of Aeronautical and Space Sciences* [online]. 2012, **13**(4), 491-498 [cit. 2016-05-09]. DOI: 10.5139/IJASS.2012.13.4.491. ISSN 2093-274x. Dostupné z: http://koreascience.or.kr/journal/view.jsp?kj=HGJHC0

[45] An introduction to GNSS: Chapter 6: GNSS+INS. In: *NovAtel* [online]. b.r. [cit. 2016-07-07]. Dostupné z: http://www.novatel.com/an-introduction-to-gnss/chapter-6-gnss-ins/gnss-ins-systems/

[46] GEBRE-EGZIABHER, Demoz a Scott GLEASON. *GNSS applications and methods*. Boston, Mass.: Artech House, 2009. GNSS technology and applications series. ISBN 978-1-59693-329-3.

[47] Systems: New civil signals. *GPS.gov: Official U.S. Government information about the Global Positioning System (GPS) and related topics* [online]. b.r. [cit. 2016-05-11]. Dostupné z: http://www.gps.gov/systems/gps/modernization/civilsignals/

[48] *ESA Navipedia* [online]. [cit. 2016-05-11]. Dostupné z: http://www.navipedia.net

[49] Galileo. *ESA* [online]. b.r. [cit. 2016-05-11]. Dostupné z: http://www.esa.int/Our_Activities/Navigation/The_future_-_Galileo/What_is_Galileo

[50] DANESHMAND, Saeed, Ali JAFARNIA-JAHROMI, Ali BROUMANDAN a Gérard LACHAPELLE. Low-Complexity Spoofing Mitigation. GPS World [online]. 2011 [cit. 2016-05-13]. Dostupné z: http://gpsworld.com/gnss-systemsignal-processinglow-complexity-spoofing-mitigation-12366/

[51] HUMPHREYS, Todd E., Jahshan A. BHATTI a Brent M. LEDVINA. The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness, and Resistance to Spoofing [online]. 2010 [cit. 2016-05-13]. Dostupné z: https://repositories.lib.utexas.edu/bitstream/handle/2152/17602/assimilator_for_distribution.pdf?sequence=2

[52] HERNÁNDEZ, Ignacio. *Galileo's commercial service: Testing GNSS high accuracy and authentication* [online]. 2015 [cit. 2016-06-28]. ISSN Inside GNSS. Dostupné z: http://www.insidegnss.com/auto/janfeb15-FERNANDEZ.pdf

[53] FERNÁNDEZ-HERNÁNDEZ, I. The Galileo Commercial Service: Current Status and Prospects. *Coordinates* [online]. 2014 [cit. 2016-06-28]. Dostupné z: http://mycoordinates.org/the-galileo-commercial-service-current-status-and-prospects/

[54] Assuring authentication for all. In: *European global navigation satellite systems agency* [online]. 2016 [cit. 2016-06-28]. Dostupné z: http://www.gsa.europa.eu/news/assuring-authentication-all

[55] WULLEMS, Chris, Oscar POZZOBON a Kurt KUBIK. *Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems* [online]. 2005 [cit. 2016-04-13]. Dostupné z: http://eprints.qut.edu.au/38275/1/wullems_SignalAuth.pdf

[56] POZZOBON, Oscar, Giovanni GAMBA, Mateo CANNALE, Samuele FANTINATO a Günther HEIN. GNSS authentication for modernized signals: From data schemes to supersonic codes. *Inside GNSS* [online]. 2015 [cit. 2016-04-12]. Dostupné z: http://www.insidegnss.com/auto/janfeb15-WP.pdf

[57] *CENTRÁLNÍ DISPEČINK IDS JMK* [online]. b.r. [cit. 2016-04-28]. Dostupné z: http://www.idsjmk.cz/ced.aspx

[58] DIBLÍK, Lukáš. *VYUŽITÍ STÁVAJÍCÍCH SYSTÉMŮ GNSS PRO URČOVÁNÍ POLOHY V MĚSTSKÉ ZÁSTAVBĚ*. Praha, 2014. ČVUT, Fakulta dopravní. Vedoucí práce Ing. Milan Sliacky.

[59] BAMBUŠEK, Martin. *Metodika pro zavádění systému preference ve VD s využitím technologie TYFLOSET* [online]. In: . 2013 [cit. 2016-04-07]. Dostupné z: https://www.cdv.cz/file/teipt-metodika-pro-zavadeni-systemu-preference-ve-vd-s-vyuzitim-technologie-tyfloset/

[60] GONZÁLEZA, Emilio, Celso PRADOSA, Virginia ANTÓNA a Boris KENNESB. *GRAIL-2: Enhanced Odometry based on GNSS* [online]. In: . Transport Research Arena, 2012 [cit. 2016-04-28]. Dostupné z: http://www.gsa.europa.eu/sites/default/files/virtual_library/2012-04_-_GRAIL-2_Project_-_Enhanced_Odometry_based_on_GNSS.pdf

[61] Approach. In: *Navipedia* [online]. ESA, 2011 [cit. 2016-04-28]. Dostupné z: http://www.navipedia.net/index.php/Approach

[62] HUMPHREYS, Todd. *Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing*. 2012. The University of Texas at Austin.

[63] COSTIN, Andrei a Aurelien FRANCILLON. *Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices*. Network and Security Department EURECOM Sophia-Antipolis, France, 2012.

[64] LUNDBERG, Devin. *Security of ADS-B Receivers*. SAN DIEGO, 2014. Master thesis. UNIVERSITY OF CALIFORNIA.

[65] GPS.gov: GPS applications. *Official U.S. Government information about the Global Positioning System (GPS) and related topics* [online]. 2014 [cit. 2016-08-14]. Dostupné z: http://www.gps.gov/applications/

[66] Rail Applications. ESA Navipedia [online]. 2011 [cit. 2016-08-21]. Dostupné z: http://www.navipedia.net/index.php/Rail_Applications

[67] BINKO, Marek. Automatické vedení vlaku na síti SŽDC [online]. In: . 2012 [cit. 2016-06-29]. Dostupné z: http://binko.wz.cz/2012-2b.pdf

[68] FIKEJZ, Jan. Možnosti lokalizace kolejových vozidel v železniční síti. *Elektro-revue*. 2012, **14**(4).

[69] INTENS CORPORATION S.R.O., *Zavádění aplikací a služeb využívajících družicové navigační systémy Galileo a EGNOS v ČR.: Podkladové materiály pro odborný seminář*. 2015.

[70] *RADIOBLOK PRO VEDLEJŠÍ TRATĚ RBA-10*. AŽD Praha, b.r.. Dostupné také z: https://www.azd.cz/admin/files/Dokumenty/pdf/Produkty/Kolejove/11-RBA-100.pdf

11 Seznam příloh

1. Uživatelský manuál a specifikace GPS rušičky GP 5000