ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Tomáš Vlček

GNSS RUŠENÍ

Bakalářská práce

2017

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

K621..... **Ústav letecké dopravy**

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

Jméno a příjmení studenta (včetně titulů):

Tomáš Vlček

Kód studijního programu a studijní obor studenta:

B 3710 – LED – Letecká doprava

Název tématu (česky): **GNSS rušení**

Název tématu (anglicky): GNSS interference

Zásady pro vypracování

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

- GNSS a jeho zranitelnost
- Možnosti rušení pro přijímače GNSS
- Kritické fáze letu a kritická místa při narušení signálu GNSS
- Zhodnocení závažnosti

Rozsah grafických prací: dle pokynů vedoucího bakalářské práce

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

Seznam odborné literatury: EGNOS SoL SDD v3.1
Letecký předpis L10
GPS Interface Specifications

Vedoucí bakalářské práce: **Ing. Jakub Kraus, Ph.D.**

Datum zadání bakalářské práce: **28. října 2016**
(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: **28. srpna 2017**
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. Stanislav Szabo, PhD. MBA
vedoucí
Ústavu letecké dopravy

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

Potvrzuji převzetí zadání bakalářské práce.

Tomáš Vlček
jméno a podpis studenta

V Praze dne ..... 28. října 2016

Poděkování

Na tomto místě bych velmi rád poděkoval svému vedoucímu bakalářské práce Ing. Jakubovi Krausovi, Ph.D. za cenné rady, odborné vedení a vstřícný přístup po celou dobu mého studia a dále všem, kteří mi poskytli důležité materiály nezbytné pro zpracování daného tématu.

Zvláštní poděkování pak patří mé rodině a blízkým za důvěru a podporu, kterou mi projevovali během celého studia na vysoké škole.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

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

V Praze dne 14. srpna 2017 .....

podpis

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

GNSS RUŠENÍ

bakalářská práce
srpen 2017
Tomáš Vlček

ABSTRAKT

Předmětem bakalářské práce „GNSS rušení“ je charakterizovat současné GNSS systémy, popsat metody rušení signálů těchto systémů a uvést několik příkladů rušení, ke kterým v minulosti došlo. Cílem je tyto problémy pochopit a zhodnotit jejich závažnost v souvislosti s leteckou dopravou.

ABSTRACT

The subject of the bachelor thesis „GNSS interference“ is to characterize current GNSS systems, to describe methods of signal interference of these systems and to give some examples of interference that have occured in the past. The aim is to understand these problems and assess their relevance in relation to air transport.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

GNSS RUŠENÍ

bakalářská práce
srpen 2017
Tomáš Vlček

KLÍČOVÁ SLOVA

GNSS systémy, GNSS rušení, jamming, spoofing, letiště, letoun, satelit, systémy pro odhalení rušení, GNSS zpřesnění, příklady rušení, závažnost rušení

KEYWORDS

GNSS systems, GNSS interference, jamming, spoofing, airport, airplane, satellite, systems for detecting interference, GNSS augmentation, examples of interference, relevance of interference

Obsah

Seznam použitých zkratek

LPV	Localizer Performance with Vertical guidance
	Přiblížení pomocí GNSS s vertikálním vedením
GNSS	Global Navigation Satellite System
	Globální družicový navigační systém
GPS	Global Positioning System
	Globální polohový systém
GBAS	Ground-Based Augmentation System
	Systém zpřesnění GNSS
SBAS	Satellite-Based Augmentation System
	Systém zpřesnění GNSS
ABAS	Aircraft-Based Augmentation System
	Systém zpřesnění GNSS
VHF	Very High Frequency
	Velmi krátké vlny
WAAS	Wide Area Augmentation System
	Systém zpřesnění GNSS
GAGAN	GPS Aided Geo Augmented Navigation
	Vylepšení SBAS v Indii
EGNOS	European Geostationary Navigation Overlay Service
	Vylepšení SBAS v Evropě
J/S	Jamming-to-Signal ratio
	Poměr rušícího signálu/originálního signálu
LAAS	Local Area Augmentation Systém
	Systém zpřesnění GNSS
C/No	Carrier-to-Noise ratio
	Poměr signálu/šumu
JLOC	Jamming Detection and Location System
	Systém pro odhalení rušení signálu GNSS
SENTINEL	Services Needing Trust In Navigation Electronics Location and timing
	Systém pro odhalení rušení signálu GNSS
eLoran	Enhanced Long range navigation
	Pozemní rádiový navigační systém
VOR	VHF Omnidirectional Radio Range
	Všesměrový radiomaják
DME	Distance Measuring Equipment
	Systém pro měření šikmé vzdálenosti

VFR	Visual Flight Rules
	Pravidla letu za viditelnosti země
IFR	Instrument Flight Rules
	Pravidla letu podle přístrojů

Úvod

Je to již přes čtyřicet let, kdy byl zahájen vývoj jednoho z nejvýznamnějších, globálních navigačních družicových systémů (GNSS, Global Navigation Satellite System) současné doby a to amerického NAVSTAR GPS (Navigation Signal Timing and Ranging Global Positioning System). Od té doby došlo k mohutnému rozvoji tohoto způsobu navigace a určování polohy kdekoliv na zemském povrchu. Vzniklo také několik nových systémů, mezi které můžeme zařadit ruský GLONASS (Globalnaja navigacionnaja sputnikovaja sistěma) nebo evropský systém Galileo. Využívání této možnosti navigace se stalo součástí našeho všedního života a je nezbytné pro mnohá odvětví. Jedním z těchto odvětví je také letectví, konkrétně navigace letadel.

Vzhledem k dobrým charakteristikám, kterou je zejména přesnost, začal tento typ navigace v letectví postupně nahrazovat navigaci pomocí radionavigačních zařízení a využívá se jak při traťových letech, tak při přiblíženích na přistání (například LPV,Localizer performance with vertical guaidance). I přesnost samotných systémů je však omezena a tak je zapotřebí poskytovat různé druhy zpřesnění. Nevýhodou GNSS systémů je fakt, že satelity obíhají zemi ve velké výšce a signály přicházející na zemský povrch jsou tudíž velmi slabé, a proto mohou být během své cesty ovlivňovány různými negativními vlivy a také mohou být rušeny. Jedním z hlavních důvodů zpracování této bakalářské práce je fakt, že letecká doprava je velmi rychle se rozvíjející způsob dopravy, kterou využívá mnoho lidí po celém světě, a v minulosti byly zaznamenány případy rušení signálu na palubách letadel. Bezpečnost je vždy na prvním místě a proto se nelze spokojit s tím, že letadlo ztratí v určitém okamžiku informaci o své aktuální poloze. Je proto nutné hledat metody, které by těmto situacím předcházely a zabraňovaly.

Cílem této práce je tudíž přiblížit čtenáři základní principy fungování GNSS systémů, vysvětlit jednotlivé typy možného rušení vysílaných signálů, navrhnout postup detekce rušení a zhodnotit závažnost vzhledem k jednotlivým vytvořeným příkladům.

1 GNSS a její zranitelnost

V této úvodní kapitole bakalářské práce si autor klade za povinnost seznámit čtenáře alespoň zjednodušeně se základními principy fungování současných GNSS systémů. Přiblížen bude jak princip samotného fungování a přenosu signálů mezi jednotlivými komponentami, tak popsáno strukturálního dělení těchto systémů. Nebudou vynechány ani požadavky, které na systémy klademe, ani jejich zranitelnost, která v problematice této práce hraje významnou roli. Tyto základní poznatky jsou považovány za stěžejní pro další pochopení zpracovávaného tématu, a proto jim je věnována samostatná kapitola.

1.1 Princip fungování

Pod pojmem GNSS se skrývá označení pro všechny systémy sloužící pro určení polohy přijímače kdekoliv na zemském povrchu.

Základním principem fungování těchto systémů je přenos radiových vln mezi jednotlivými družicemi (satelity) na oběžných drahách a přijímači těchto signálů na zemském povrchu, tedy uživatelskými zařízeními. Satelity obíhající zemi ve výškách přibližně 20 000 km nad zemským povrchem vysílají nepřetržité signály na určitých frekvencích. Tyto signály mimo jiné obsahují údaje o poloze daného satelitu a časové údaje. Přijímač na zemi dokáže na základě znalosti rychlosti šíření radiových vln a doby, která uplyne mezi odesláním signálu z družice a jeho přijmutím v tomto přijímači, určit vzdálenost k danému satelitu. Z předchozí věty plyne logický závěr, že pro přesné určení polohy na zemském povrchu nepostačuje pouze jeden satelit, ale v trojrozměrném prostoru potřebujeme tyto satelity alespoň čtyři, a to pro určení třech souřadnic XYZ a pro zajištění reálného času. Platí zde fakt, že čím více signálů z různých satelitů přijímač přijímá, tím přesněji je poloha určena.

1.2 Struktura GNSS

Pro správné a časově kontinuální fungování systémů GNSS je zapotřebí, aby byly tyto systémy kromě samotných satelitů a uživatelských přijímačů vybaveny také různými typy pozemních stanic, které monitorují a nastavují parametry jednotlivých satelitů. Globální družicové navigační systémy jsou tedy složeny z několika částí.

1.2.1 Kosmický segment

Kosmický segment je tvořen jednotlivými satelity obíhající zemi po oběžných drahách ve vzdálenosti přibližně 20 000 km nad zemským povrchem. Tyto satelity vysílají rádiové vlny, které jsou s určitým časovým zpožděním na zemském povrchu přijímány a zpracovány uživatelskými zařízeními. Kromě těchto vysílačů jsou satelity také vybaveny přijímačem,

přesnými atomovými hodinami, raketovými motory a solárními panely. Raketové motory jsou využívány v případě potřeby satelitu upravit svoji polohu a solární panely k výrobě elektrické energie.

1.2.2 Řídící segment

Řídící segment je pro fungování systému GNSS jako celku zcela nezbytný, a bez něho by nebyla zaručena úplná správnost přijímaných informací. Tento segment se skládá ze tří typů pozemních stanic. Jsou to stanice monitorovací, hlavní řídící a stanice pro komunikaci se satelity.

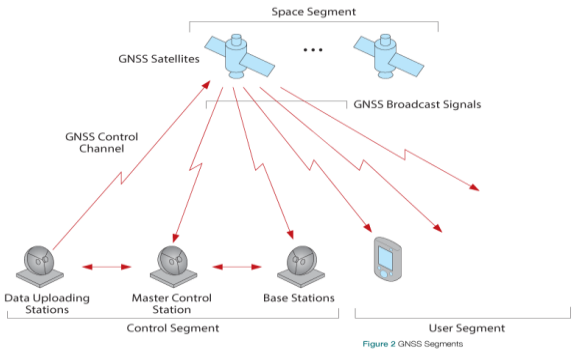
Monitorovací stanice jsou rozmístěny na velkých územních plochách. Monitorují signály, které satelity vysílají, a zároveň stav těchto satelitů. Tyto informace dále předávají do hlavní řídící stanice.

Hlavní řídící stanice přijímá informace o jednotlivých satelitech z monitorovacích stanic. Na základě velmi přesné známé polohy jednotlivých monitorovacích stanic určuje časové a polohové korekce pro jednotlivé satelity a tyto informace předává do stanic pro komunikaci s družicemi.

Stanice pro komunikaci s družicemi přijímají informace o časových a polohových korekcích z hlavních řídících stanic a dále je předávají jednotlivým satelitům, které poté vysílají do uživatelských zařízení již opravené signály.

1.2.3 Uživatelský segment

Uživatelský segment tvoří taková zařízení, která přijímají signály ze satelitů, vyhodnocují je a na základě vyhodnocení určují polohu zařízení. Můžeme do nich zařadit jak smartphony, kapesní navigace, tak složitější a pokročilejší přijímače využívané v mapovacích aplikacích. Jak již bylo uvedeno dříve, pro přesné určení polohy jsou zapotřebí alespoň čtyři viditelné satelity.

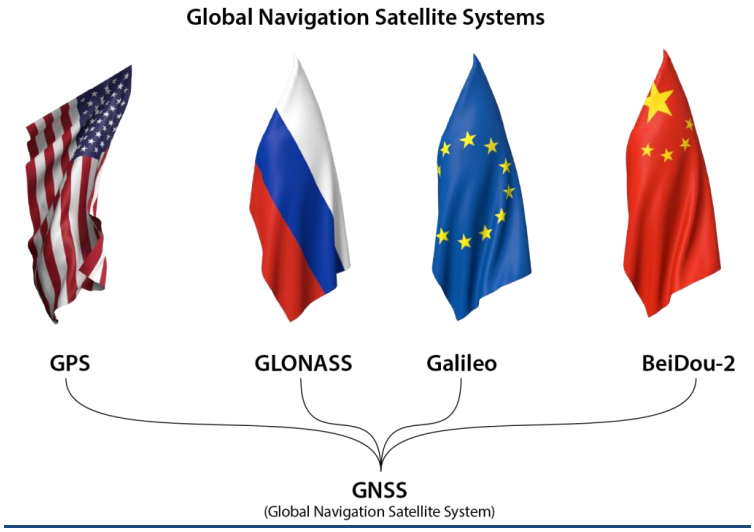


Obrázek 1 - Struktura GNSS [26]

1.3 Významné systémy

V současné době existuje několik systému GNSS. Tyto systémy se od sebe odlišují zejména počtem družic, počtem oběžných drah, výškou oběhu družic nad zemským povrchem, kódováním signálů a také státem, popřípadě organizací, která tento systém spravuje. Z hlediska celosvětového pokrytí můžeme mezi ty nejvýznamnější zařadit systémy GPS, GLONASS a GALILEO, který je od konce roku 2016 ve zkušebním provozu. Existují i systémy, které pokrývají pouze vymezenou oblast. Mezi ně patří systém BeiDou 1, poskytující službu nad územím Číny. Do roku 2020 by měl být postupně transformován na systém BeiDou 2, který bude poskytovat celosvětové pokrytí.

Charakteristické rozdíly mezi jednotlivými systémy jsou zobrazeny níže. V tabulce jsou uvažovány pouze systémy s aktuálním celosvětovým pokrytím.



Obrázek 2 - GNSS systémy [27]

Tabulka 1 - Charakteristiky jednotlivých GNSS systémů

GNSS systém	Počet družic	Počet oběžných drah	Výška oběhu	Rozlišení družic	Signály
GPS	24	4	20200 km	kódové	L1,L2,L5
GLONNAS	24	3	19100 km	fázové	L1,L2,L3,L5
GALILEO	30 (2020)	3	23222 km	kódové	E1-L1-E2, E5,E6

Jak vyplývá z předchozí tabulky, jednotlivé systémy vysílají různě označené signály, které se odlišují nosnou frekvencí. Tyto frekvence se pohybují v řádech stovek MHz a jsou důležité z pohledu možného rušení a znemožnění správného příjmu v uživatelských zařízeních. Přehled signálu s nosnými frekvencemi je uveden v následující tabulce.

Tabulka 2 - Signály systémů a jejich frekvence

	GPS	GLONNAS	GALILEO
L1 (E1)	1575 MHz	1598-1605 MHz 1575 MHz (CDMA)	1575 MHz
L2	1228 MHz	1243-1249 MHz	-
L3	-	1198-1212 MHz	-
L5	1176 MHz	1176 MHz (CDMA)	-
E5	-	-	1176 MHz
E6	-	-	1279 MHz

Pro určení polohy přijímače je nutné vědět, z jaké konkrétní družice daný signál přichází. Z tohoto důvodu se využívá kódování. Existují dva základní druhy kódování, a to kódový multiplex, který využívají systémy GPS a GALILEO, a kmitočtový multiplex, který preferuje ruský GLONNAS.

Kódový multiplex je založen na tom, že všechny satelity vysílají signály na stejné frekvenci, ale každý z nich obsahuje jedinečný kód. Na tomto základě dokáže přijímač určit, z jaké družice signál pochází. Kmitočtový multiplex je naopak založen na principu stejných kódů, ale každá družice vysílá na své přidělené frekvenci, která se v případě signálu L1 ruského GLONNASU pohybuje v rozmezí přibližně 1598 MHz – 1605 MHz. Pro lepší spolupráci a kompatibilitu mezi jednotlivými systémy však i u ruského systému v případě signálu L1 existuje multiplex kódový, který vysílá na nosné frekvenci 1575 MHz.

1.4 Požadavky na GNSS

Jednotlivé systémy by měly splňovat čtyři základní požadavky, na jejichž základě systém hodnotíme. Těmito kritérii jsou přesnost, dostupnost, spojitost a integrita.

1.4.1 Přesnost

Přesnost je jedním ze základních ukazatelů každého GNSS systému. Pro běžné uživatele počítáme u současných systémů s přesností v řádech desítek metrů, ve vojenském využití může být poloha určována s přesností na několik centimetrů. Definujeme ji jako odchylku naměřené polohy od polohy skutečné, a tudíž ji můžeme zapsat pomocí vzorce

$$P(|Xi - Xy| \leq \varepsilon) \geq \gamma. \quad (1.1)$$

Tento vzorec nám říká, že rozdíl mezi skutečnou a naměřenou polohou nepřekročí hodnotu epsílon na hladině pravděpodobnosti gama. Přesnost může být zhoršována různými vlivy, o nichž je pojednáno v kapitole 1.6 zranitelnost systémů.

1.4.2 Spojitost

Spojitost je vyjádřena jako taková schopnost systému, která zajišťuje kontinuální chod systému bez neplánovaných výpadků nebo přerušení v poskytování služby.

1.4.3 Dostupnost

U této vlastnosti je zapotřebí zavést dva časy. Jeden čas označíme jako celkový čas T_1, na který byl systém navrhnut, že bude funkční a po jehož dobu bude k dispozici. Druhý čas označíme jako skutečný čas T_2, během kterého systém funguje. Procentuální vyjádření času T_2 k času T_1 označíme jako dostupnost systému.

1.4.4 Integrita

Integrita je velice důležitou vlastností, která vyjadřuje schopnost systému varovat do určitého časového limitu jeho uživatele v situacích, kdy je překročena přípustná hodnota určitého parametru, a systém je tudíž nevhodný k používání.

1.5 Vylepšení charakteristik GNSS

Jak již bylo uvedeno v předchozí podkapitole, na systémy GNSS jsou kladeny velké nároky. V některých odvětvích jsou však poskytované služby nedostatečné, a proto musí být systémy vhodně rozšířeny. Jedním z těchto odvětví je letectví. V letectví se využívají tři základní typy rozšíření, a to GBAS, SBAS a ABAS.

1.5.1 Ground based augmentation system

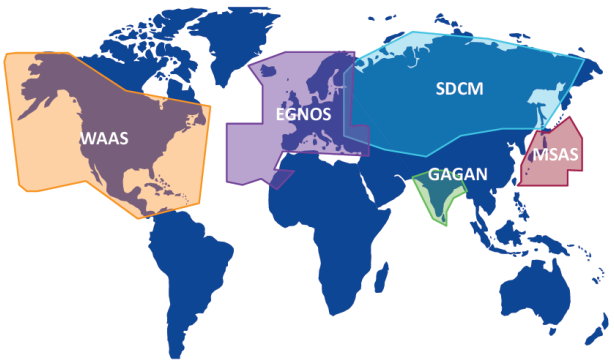
Tento typ rozšíření se využívá zejména blízko letišť při přiblížení letadel na přistání. Je složen z několika pozemních přijímačů, které zpracovávají signály ze všech viditelných satelitů. Na základě své přesně známé polohy určují korekce v přesnosti a kontrolují též integritu. Pomocí VHF vln vysílají tyto korekce do letadel, které se nacházejí ve fázi přiblížení na přistání. Piloti dostávají již opravené údaje a tím je zajištěna větší bezpečnost zejména při zhoršeném počasí. Přesnost je v horizontální i vertikální rovině do jednoho metru.

1.5.2 Satelite based augmentation system

Rozšíření označované jako SBAS má v různých částech světa různé označení. V Severní Americe se používá název WAAS, v Indii GAGAN a v Evropě je to EGNOS. I přes rozdílné názvy je však princip stejný a cílem je opět zlepšovat charakteristiky GNSS.

Systém je tvořen pozemními stanicemi a geostacionárními satelity. V pozemních stanicích se vyhodnocují přijaté signály ze satelitů GNSS a určují se korekční data. Tato data se dále

spolu se zprávami o integritě systému vysílají na geostacionární satelity a z těch dále do uživatelských zařízení.



Obrázek 3 – SBAS [28]

1.5.3 Aircraft based augmentation system

Je to systém sloužící zejména ke kontrole integrity během letu. Funguje na principu porovnávání dat z přijatých signálu GNSS družic s informacemi z dalších palubních přístrojů. Jako příklad můžeme uvést barometr.

1.6 Zranitelnost systémů

Jednou z nevýhod GNSS při poskytování služeb je zranitelnost jejich signálů. Tyto signály jsou při příchodu na zem velmi slabé, a proto jsou snadno zranitelné. Mohou být rušeny, přičemž rozlišujeme tři typy rušení signálů. Jsou to jamming, spoofing a meaconing. Podrobněji si je rozebereme později.

Mimo zmiňované rušení mohou být vlastnosti signálů zhoršovány. Takových vlivů, které ovlivňují kvalitu signálů a negativně působí na základní ukazatele GNSS, zejména na přesnost, rozlišujeme celou řadu. Tyto chyby se s časem mohou měnit a zmínit můžeme ionosférickou chybu, troposférickou chybu nebo nepřesnou polohu družic (efemeridická chyba). Přehled nejvýznamnějších vlivů a jejich chyby jsou zobrazeny v následující tabulce.

Tabulka 3 - Chyby GNSS

Zdroj chyby	Chyba
Ionosferický efekt	± 5 m
Troposferický efekt	± 0,5 m
Efemeridická chyba	± 2,5 m
Chyba hodin satelitů	± 2 m
Vícecestné šíření	± 1 m

2 Možnosti rušení přijímačů GNSS

V této kapitole se zaměříme na možnosti, jak lze signály, které vysílají družice, narušit a uvedeme několik příkladů, kdy se v minulosti nějaký typ rušení vyskytoval a jaký to mělo dopad na uživatele. Obecně lze říci, že pro běžného uživatele není chvilková ztráta signálu GNSS problém. To už ovšem neplatí v určitých odvětvích jako je letectví popřípadě záchranná služba. V těchto odvětvích by mohla mít ztráta signálu fatální následky, a proto se snažíme rušení předcházet.

2.1 Kategorie rušení

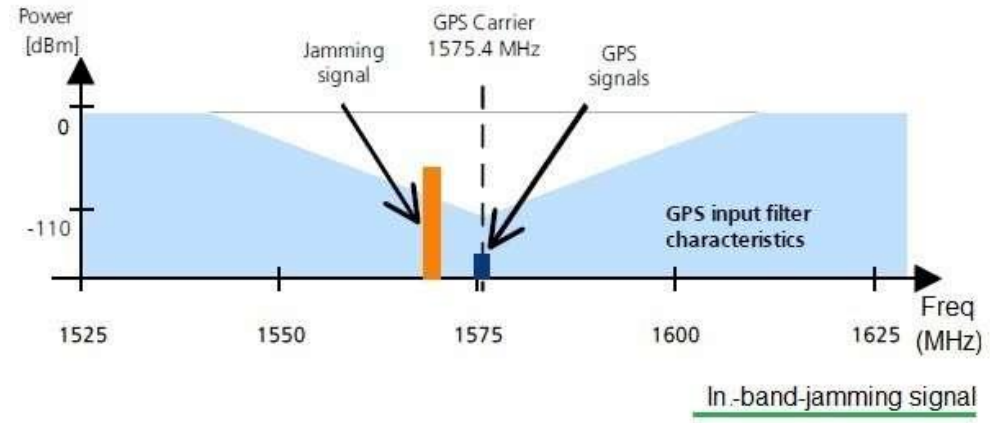
Rušení signálů můžeme rozdělit na tři základní kategorie vzhledem k důvodu a cíli, proč je rušení způsobováno.

První kategorií je rušení náhodné, které ve většině případů není způsobováno z iniciativy člověka. Toto rušení označujeme jako nezáměrně vysílané a většinou se jedná o poruchy vysílačů, které náhodně pronikají svým vysíláním do pásem frekvencí, které jsou vyhrazeny pro systémy GNSS. Toto rušení je nepředvídatelné, a proto může být nebezpečné. Téměř se ale nevyskytuje.

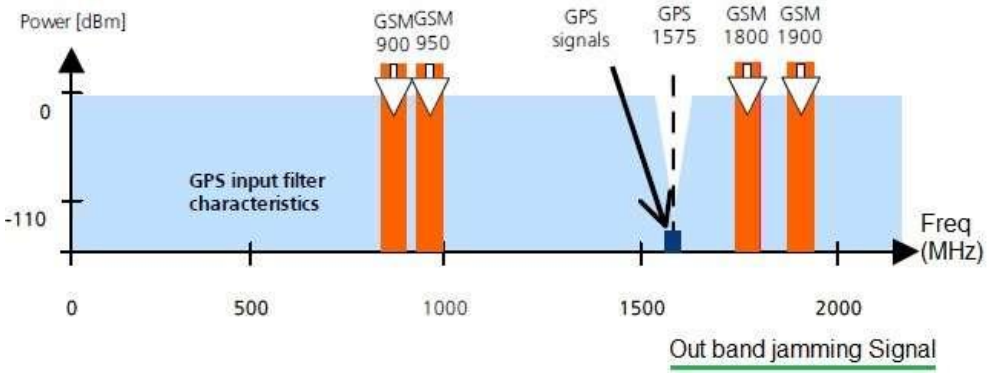
Druhou kategorii označujeme jak rušení neinformované. Tento druh rušení je způsoben záměrným vysíláním na daných frekvencích, nicméně cílem není poškodit uživatele systémů a způsobit velké škody, ale vlastní užitek. Příkladem může být používání rušících zařízení, které využívá mnoho řidičů zejména nákladních vozidel, aby nemohli být sledováni svými zaměstnavateli.

Poslední kategorií je rušení škodlivé. V tomto případě se jedná o záměrně vysílané rušení s cílem poškodit co nejvíce uživatelů, které může postihovat rozsáhlé plochy. V těchto situacích je vhodné používat záložní systémy, které nejsou založeny na příjmu signálů z GNSS satelitů.

Další dělení můžeme provést na základě pásem a frekvencí, na kterých rušící zařízení vysílají. Je to tzv. In-band rušení a Out-band rušení. První z nich, In-band rušení, je takové rušení, u kterého je frekvence rušícího signálu totožná nebo velice blízká originální frekvenci GNSS satelitů. Druhým typem je Out-band rušení, kde je frekvence naprosto odlišná od GNSS frekvencí. Pomocí skládání vln však dochází ke vzniku vyšších harmonických vln s frekvencemi, které dokáží rušit originální GNSS signály. Rozdíl mezi oběma typy je zřejmý z přiložených obrázků, kde na obrázku 4 vidíme na vodorovné ose nepatrný rozdíl mezi frekvencí originálního signálu GPS a frekvencí rušícího signálu, zatímco v případě obrázku 5 se tento rozdíl pohybuje v řádech stovek MHz.



Obrázek 4 - In-band jamming [29]



Obrázek 5 Out-band jamming [29]

2.2 Typy rušení

Jak již bylo popsáno v kapitole 1.6, kvalita signálů může být zhoršována různými vlivy, které nemůžeme ovlivnit. Jedná se zejména o ionosférické a troposférické chyby. Mimo to však existují situace, ve kterých může dojít k naprosté ztrátě signálů. Tato ztráta může trvat od několika sekund až po desítky minut v závislosti na tom, zda je přijímač v pohybu a dokáže se od zdroje rušení vzdálit, popřípadě obráceně.

Signál, který přichází do uživatelských zařízení ze satelitů, je při příchodu na zem velice slabý. Proto dokáže být pomocí jednoduchých rušících zařízení rušen, čímž dojde k znemožnění využívání systému. Rozlišujeme již zmíněné tři typy rušení. Jsou to jamming, spoofing a meaconing.

2.2.1 Jamming

Nejčastější formou rušení signálu GNSS je právě jamming. Tento druh rušení funguje na principu toho, že rušící zařízení vysílá signál na stejné nebo velmi blízké frekvenci, jako jsou

frekvence vyhrazené pro GNSS systémy. Do původního signálu zavádí šum nebo svým výkonem přetíží obvod původního přijímače, a ten není schopný přijímat původní signál. Cílem jammingu je tudíž rušit, nebo úplně znemožnit přenos signálu ze satelitů GNSS do přijímačů na zemi. Tyto přijímače poté nejsou schopny udávat správnou polohu.

Využívají se jak jednoduché osobní rušící zařízení, tak složitější a sofistikovanější zařízení s větším výkonem a schopností rušit širší pásmo frekvencí. Osobní rušičky využívají zejména řidiči dopravních prostředků. Tím docilují toho, že nebudou sledováni a monitorováni svým zaměstnavatelem. Složitější zařízení se využívají v armádě, kde je v nějaké situaci zapotřebí vyřadit z provozu všechny přijímače GNSS na větším území.

2.2.2 Spoofing

Spoofing se v porovnání s jammingem téměř nevyskytuje, ale o to delší doba může nastat pro jeho odhalení a tudíž je také nebezpečnější. Je to záměrné vysílání falešných GNSS signálů, jejichž cílem je vypadat jako původní GNSS signál. Přijímač poté sleduje tento falešný signál místo původního signálu z družic. Tím dochází ke špatnému určování polohy, rychlosti a času.

Zde již podstatnou roli hraje samotný přijímač. Některé přijímače nejsou schopny rušení rozpoznat či filtrovat, a tak přijímají vše, co jako GNSS signál vypadá. Ty nejsou proti rušení téměř vůbec odolné a může docházet k situacím, kde místo originálního signálu sledují signál falešný. Některé sofistikovanější jsou vybaveny filtry, které dokáží spoofing rozpoznat a stále udávat spolehlivá data. Proto je nutné odlišit kvalitní přijímače s větší odolností od těch jednoduchých.

2.2.3 Meaconing

Tento druh rušení je založen na principu nahrávání GNSS signálů a jejich opětovném vysílání. Tím se docílí toho, že znovu vysílaný signál je silnější než původní, a pokud přijímač začne sledovat tento signál, nebude schopen udávat správnou polohu.

2.3 Zdroje rušení

Mezi zdroje, které způsobují rušení signálu GNSS, můžeme kromě zmiňovaných rušiček a sofistikovanějších zařízení zařadit také sluneční erupce nebo různé odrazy signálu.

2.3.1 Rušičky

Jednotlivé rušičky se mohou odlišovat jak velikostí a výkonem, tak také cenou. Na internetu se běžně dají sehnat od 30 eur. Ty lepší poté stojí několik stovek eur. Existuje celá řada různých designů rušiček, z nichž některé jsou zobrazeny dále. Alarmující je však již jen fakt,

že se většinou nelegální rušičky na internetu vůbec objevují a při zadání spojení „signal jammer“ webový prohlížeč google vyhledá 725 000 výsledků.

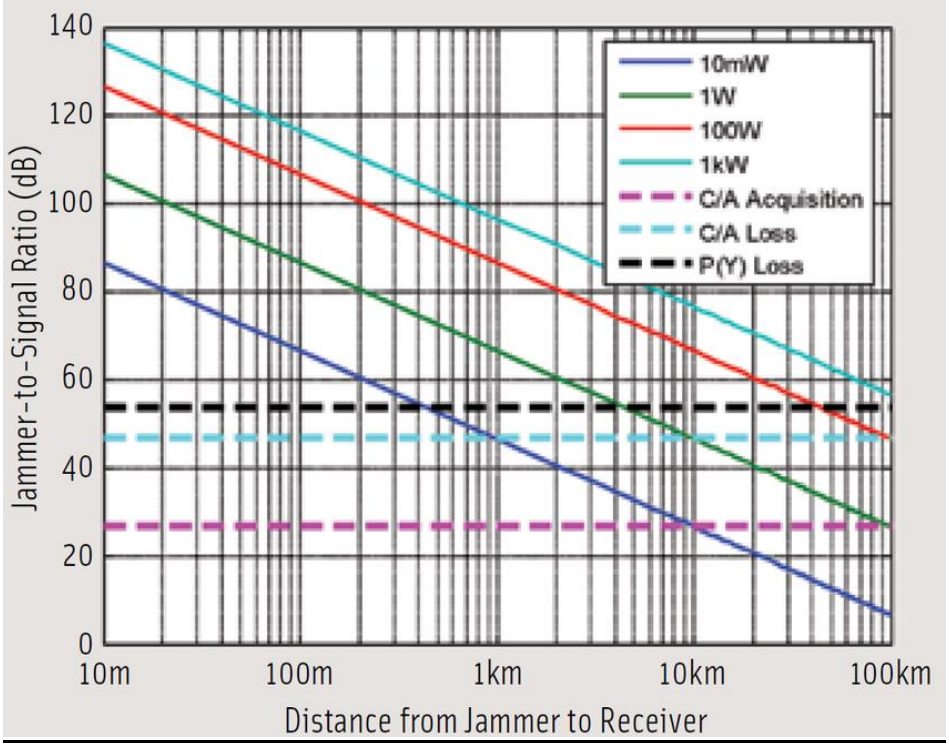
Obrázek 6 - rušička 1 [36]

Obrázek 7 - rušička 2 [35]

Z hlediska výkonu se v případě nejjednodušších rušiček pohybujeme v řádech miliwattů. U výkonnějších, s větším dosahem, může výkon dosahovat hodnot v řádech jednotek až desítek wattů.

Na přiloženém obrázku vidíme dosah rušení a poměr J/S vzhledem k výkonu rušičky. Tento poměr, jehož jednotkou je dB, udává poměr mezi silou rušícího signálu a signálu originálního. Čím větší je tento poměr, tím je kvalita přijímaného signálu horší. Úhlopříčné čáry zobrazují, jak se mění J/S poměr a vzdálenost rušení v závislosti na daném výkonu rušičky, a vodorovné zobrazují meze, kdy dochází ke ztrátám signálu. V případě první rušičky o výkonu 10 mW dojde ke ztrátě signálu na vzdálenost 1 km. Pokud je však výkon

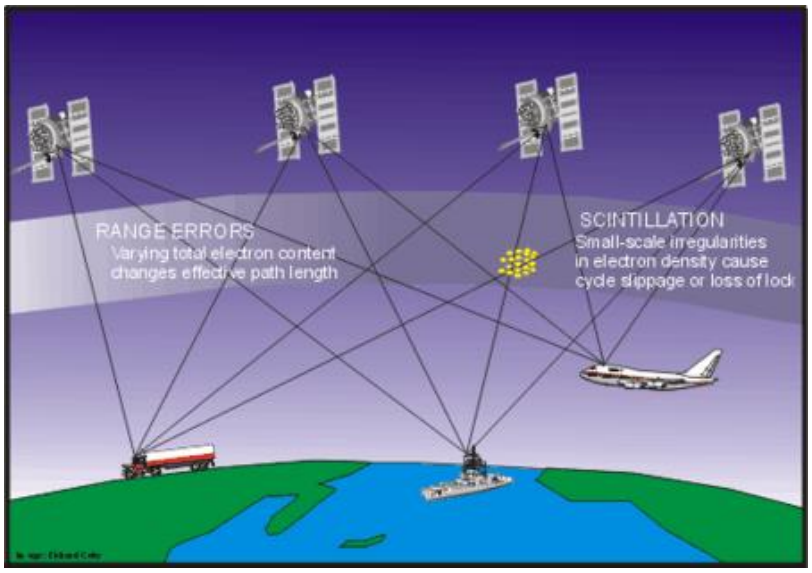
rušičky větší a má hodnotu například 1 W, dojde ke ztrátě signálu v okolí 10 km.



Obrázek 8 - Výkony rušiček [1]

2.3.2 Kosmické počasí

Dalším ze zdrojů, které mohou ovlivnit signály GNSS systémů je kosmické počasí. Na slunci probíhají ve více či méně periodických intervalech sluneční erupce. Některé z nich mohou být až tak rozsáhlé, že nabité částice, usazující se v ionosféře, způsobují snížení rychlosti radiových vln vysílaných satelity. To se poté promítá do přesnosti systémů a v některých případech může vlivem velmi hustého prostředí v ionosféře docházet ke ztrátě signálu. Pro bližší představu je přiložen obrázek s popsanou situací, kdy nabité částice dokáží měnit rychlost vln postupujících na zem a v druhém případě úplně vyřadit systém z provozu.



Obrázek 9 - Ionosféra [34]

2.4 Příklady

Pro účely této práce je zásadní uvést několik případů, kdy došlo nebo opakovaně docházelo k rušení signálu GNSS ať už omylem nebo záměrně. Podrobněji se podíváme na rušení signálu v okolí letiště Newark a dále na příčiny ztráty signálu v okolí pozemní stanice zařízení WAAS v americkém Leesburgu. Mimo to se jamming může vyskytovat i ve výzkumných laboratořích pro pochopení a objasnění účinků rušení jednotlivých typů rušiček. Jeden takovýto test si také přiblížíme a bude uvedeno i několik dalších příkladů.

2.4.1 Rušení v Newarku

V prvním příkladě si popíšeme jeden z nejvýznamnějších případů rušení signálu GNSS. Toto rušení se začalo odehrávat v blízkosti amerického letiště Newark téměř ihned po zavedení systému pro zpřesnění vlastností družicové navigace, a to LAAS (Local area augmentation system) v letech 2008-2009. Princip tohoto zpřesnění je totožný jako u systému GBAS, liší se pouze v pojmenování. V Evropě se používá název GBAS, zatímco v americkém letectví je zaveden pojem LAAS.

Letiště v Newarku je i přes svou vysokou vytíženost a velký počet přepravených cestujících soustředěno na relativně malé ploše. Jen pro ilustraci, v roce 2015 bylo na tomto letišti odbaveno přibližně 37 milionů cestujících. Nedaleko od letiště, paralelně s dráhami 04L/22R a 04R/22L, vede rušná dálnice s téměř 100 000 projíždějícími vozidly denně. Tento fakt se při výstavbě LAAS na tomto letišti nezdál býti rizikový, nicméně ihned po spuštění systému se začaly vyskytovat problémy.

Pozemní vybavení LAAS se na tomto letišti skládá ze 4 antén, které jsou ve vzájemné vzdálenosti 100 m. Tyto antény jsou umístěny paralelně vedle dráhy a od rušné silnice je dělí vzdálenost průměrně 150 m. Rozmístění těchto antén můžeme vidět na přiloženém obrázku.

Obrázek 10 - Rozmístění antén Newark [13]

Princip funkce systému GBAS (popřípadě LAAS) je popsán v kapitole 1.5.1. V případě Newarku docházelo během dne k několika případům, kdy jednotlivé antény zaznámenávaly pokles poměru C/No. Tento poměr, carrier to noise, vyjadřuje vztah mezi úrovní intenzity signálu nosné vlny a šumu. Jednotkou je decibel a platí, že čím větší tento poměr je, tím je kvalita příjmu signálu větší.

Po určitých měřeních a výzkumech se dospělo k závěru, že za chvilkovým snižováním poměru C/No stojí osobní rušičky řidičů projíždějících na nedaleké dálnici. Vzhledem k velkému počtu osobních aut se tak dělo několikrát denně. V původním návrhu systému LAAS docházelo při ztrátě signálu na jedné ze čtyř antén k výpadku systému a byl nutný restart. Vzhledem k malé vzdálenosti mezi jednotlivými anténami mohlo při silném rušení docházet k výpadku dvou i více antén najednou. To bylo naprosto nevyhovující, neboť během této doby nebyl systém schopný vysílat přesné informace do pilotních kabin a tak bylo zvýšeno nebezpečí zejména při špatném počasí. Proto byla přijata opatření k modifikace LAAS na letišti v Newarku, která budou popsána dále.

2.4.2 Rušení Leesburg

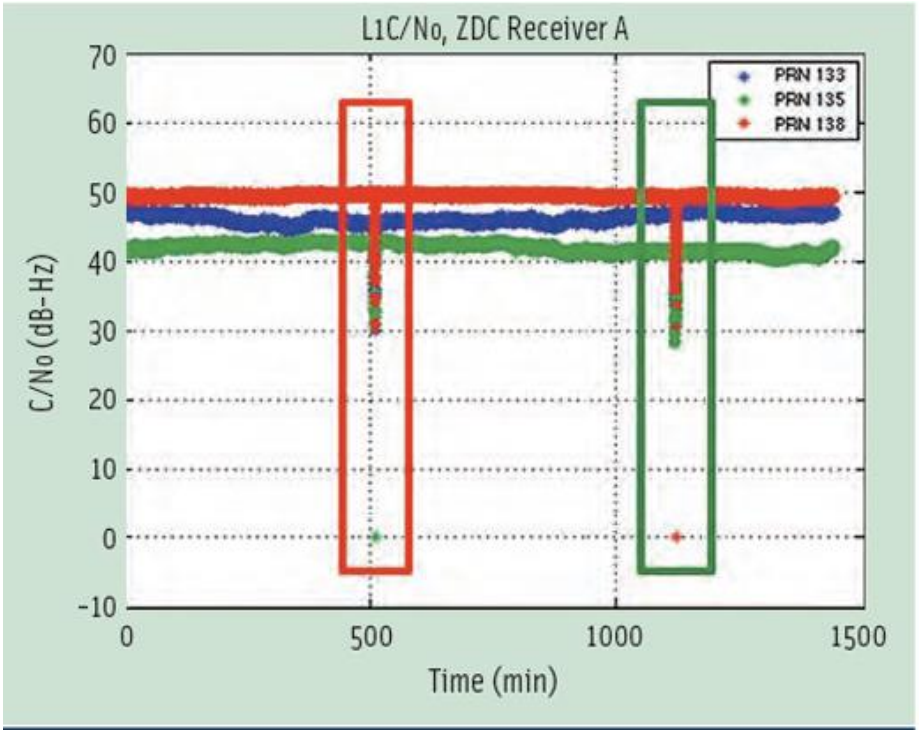
Podobný případ jako na letišti v Newarku se kolem roku 2011 odehrával také ve městě Leesburg ve Virginii. Tentokrát však nešlo o rušení systému GBAS, ale systému SBAS, označovaný ve Spojených státech amerických jako WAAS (Wide area augmentation system). Princip systému je popsán v kapitole 1.5.2.

Systém WAAS tvoří několik pozemních stanic rozmístěných na velkých plochách a tři geostacionární satelity. Každá pozemní stanice je tvořena třemi přijímači, které jsou opět rozmístěny nedaleko od sebe. Tato stanice se nachází nedaleko rušných silnic a její pozice je zobrazena na obrázku níže.

Obrázek 11 - WAAS Leesburg [30]

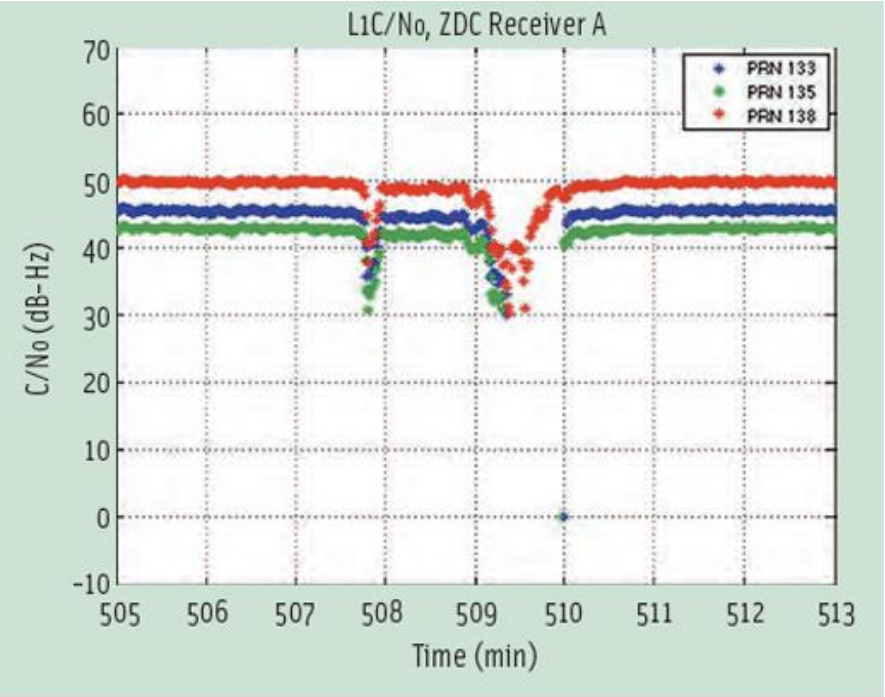
Systém zaznamenával chvilkové poklesy C/No na všech geostacionárních satelitech, z čehož vyplývá, že tyto satelity nebyly schopny přijímat informace o korekcích z pozemní stanice. Vzhledem k pouze chvilkovému rušení je zřejmé, že se rušící zařízení nevyskytovalo na jednom fixním místě, ale bylo v pohybu. To nás opět vede k myšlence, že rušení pocházelo z vozidel z nedalekých silnic. Tato domněnka se také potvrdila a na základě pravidelně se opakujích časů, kdy bylo rušení zaznamenáno, byl sestaven časový plán daného vozidla a v konečném výsledku byl řidič dopaden a osobní rušící zařízení mu bylo odebráno.

Na obrázku 12 jsou zobrazeny poklesy poměru C/No v průběhu celého dne. Je z něho patrné, že docházelo k poklesům na všech třech geostacionárních satelitech a to dvakrát denně. To poukazuje na fakt, že řidič se večer vracel stejnou cestou, ale druhým směrem, do místa, odkud ráno vyjel.



Obrázek 12 - WAAS Leesburg denní [13]

Zajímavé je také zaměření se na jednotlivá rušení v průběhu minut. Na obrázku 13 vidíme, že rušení při průjezdu vozidla v okolí pozemní stanice probíhalo ve dvou časech. Mezi těmito dvěma událostmi v rozmezí minut 508-509 však příjem signálu nebyl narušen. Tato situace je vysvětlována tak, že vozidlo se na konci 507. minuty dostalo do takové blízkosti pozemní stanice, že rušící zařízení ve vozidle dokázalo znemožnit příjem signálu. Pokračováním v cestě se však ve zmiňovaním rozmezí 508-509 dostalo do vzdálenosti větší a výkon rušičky už nebyl dostatečně velký na to, aby mohl příjem signálu ovlivňovat. Po krátké době se však do těsné blízkosti opět dostal, z čeho plynulo snížení poměru C/No v čase 509.



Obrázek 13 - WAAS Leesburg zoom [13]

Vzhledem k tomu, že těchto stanic je po území Spojených států amerických rozmístěno několik, je systém odolnější vůči rušení než GBAS. Ten je navrhován pro jednotlivá letiště a v případě jeho rušení je nemožné poskytovat korekční data.

2.4.3 Test ve finském institutu

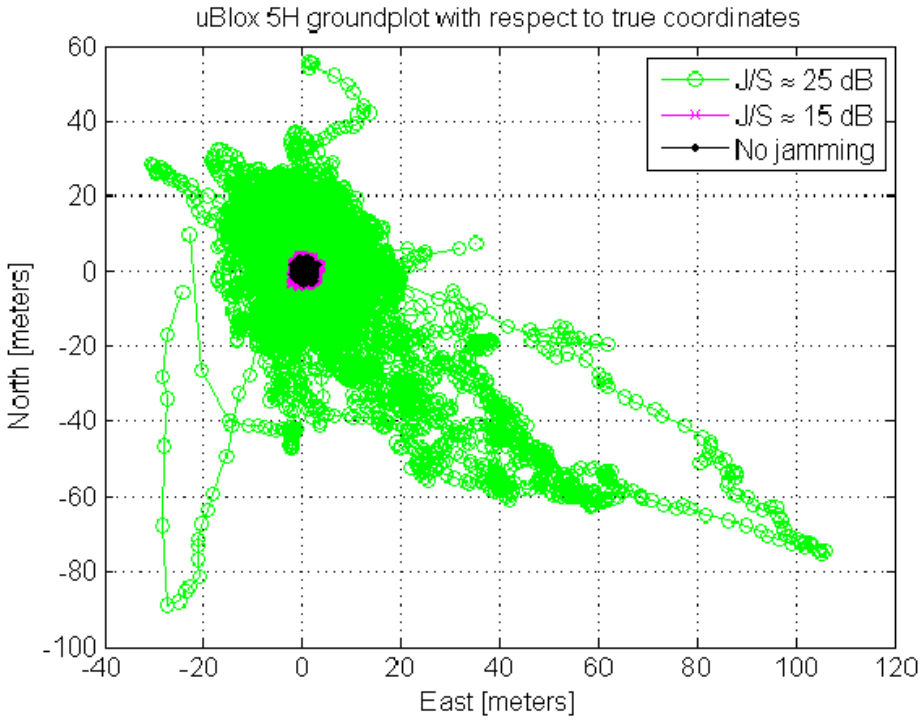
Během roku 2012 byly ve finském geodetickém institutu, konkrétně v navigační laboratoři, provedeny testy na posouzení efektu jammingu na různé typy přijímačů. Nutno podotknout, že testy byly provedeny s povolením používat rušičky v uzavřeném prostoru s maximálním výkonem 0,001 mW (-30 dBm).

První test zahrnoval jamming signálu L1 jednoduchou rušičkou a postupně byl prováděn na 6 různých příjímačích. Jedním z nich byl mj. smartphone Nokia N-8. Test byl prováděn po celých 24 hodin a příjímače byly testovány na tři různé situace. První z nich byla bez přítomnosti rušícího signálu. Během druhé situace, kdy již k rušení docházelo, dosahoval poměr J/S maximální hodnoty 15 dB a v posledním případě byl maximální přípustný poměr J/S 25 dB. Jak je vidět z tabulky níže, se zvyšujícím se poměrem J/S se také zvyšovala jak průměrná, tak maximální horizontální výchylka. Byl také zaznamenán výrazný pokles v procentuálním vyjádření dostupnosti systému. Do tabulky byly uvedeny pouze 3 ze 6 daných přijímačů, přičemž výsledky byly u všech zbývajících velice podobné.

Tabulka 4 - Působení jammingu na jednotlivé přijímače

		Prům.odchylka (m)	Max.odchylka (m)	Dostupnost (%)
uBlox 5H	No jam	1,0	3,8	100
	J/S 15 dB	1,4	4,6	100
	J/S 25 dB	9,2	129,3	16
Fastrax IT500	No jam	2,2	5,3	100
	J/S 15 dB	2,3	6,5	100
	J/S 25 dB	3,7	85,4	16
NovAtel	No jam	1,0	4,8	100
	J/S 15 dB	2,4	90,5	30
	J/S 25 dB	5,4	92,1	8

Na obrázku 14 jsou znázorněny jednotlivé polohy určené přijímačem uBlox 5H v jednotlivých případech rušení. Z obrázku i z tabulky výše vyplývá, že do doby, než poměr J/S dosáhne hodnoty 15 dB nejsou zaznamenány výrazné odchylky. V případě poměru vyššího již nastáva rychlý nárust této horizontální odchylky od teoreticky správné polohy.



Obrázek 14 - Odchylky přijímače uBlox 5H [6]

Druhý test posuzoval účinek jammingu na přijímač NovAtel OEM4, který dokáže zároveň přijímat na dvou různých frekvencích. Rušení probíhalo na frekvencích signálů L1 a L2, a proto byla k tomuto testu, kromě již zmiňované rušičky, která byla použita k prvnímu testu a rušila L1 signál, využita i druhá rušička, která dokázala rušit signály L2-L5. Opět se zkoumaly výsledky v případech, kdy rušení neprobíhá, kdy je poměr J/S maximálně 15 dB a kdy tento poměr dosahuje maximální hodnoty 25 dB. Test probíhal v hodinových krocích a výsledek je vidět z přiložené tabulky.

Tabulka 5 - Dvoufrekvenční jamming

		Prům. odchylka (m)	Max. odchylka (m)	Dostupnost (%)
NovAtel	No jam	0,8	2,8	100
	J/S 15 dB	3,4	78,9	100
	J/S 25 dB	3,5	26,6	11

Z tabulky vidíme, že ochylky dosahují podobných hodnot, jako při prvním testu, kdy byla rušena pouze jedna frekvence. Zajímavé by bylo sledovat účinky rušení jednoho signálu (například L1) z podledu přijímače, který by byl schopen přijímat více frekvencí současně (například L1 a L2).

2.4.4 Další případy

Za povšimnutí stojí také případ, který se odehrál v sousedním Německu. V hangáru zkoušeli pomocí GNSS opakovače funkčnost GPS vybavení na letadlech, která se v tomto hangáru nacházela. Výkon tohoho opakovače byl však moc velký a kromě samotného hangáru pronikal signál i do okolí. Poté bylo od několika letadel, využívající dané letiště, hlášeno rušení signálu GPS z družic.

To, že jamming může mít i politický podtext je jasné z dalšího příkladu, který si uvedeme. Vše začalo kolem roku 2010, kdy bylo v Jižní Koreji zaznamenáno rušení signálu GNSS, které pocházelo ze Severní Koreje. Tento problém hlásilo přibližně 1000 letadel a 250 lodí. V případě letadel to taková hrozba nebyla, neboť využívají inerční navigační systémy. V roce 2012 se odehrál velice podobný případ, kdy rušení signálu, pocházející opět ze Severní Koreji, ovlivnilo GPS navigace v autech ve městě Soul. V této době už měla sofistikovanější zařízení dosah blížící se 60 statutarním mílím.

Existují i další případy, kdy k rušení signálu docházelo. Můžeme uvést kompletní ztrátu signálu na téměř 20 minut v obchodním domě v Londýně, nebo jamming v blízkosti dálnic

u Mnichova, kde se v rámci jamming kampaně zkoumal výskyt tohoto rušení (zaznamenáno 6 výskytů za týden).

3 Kritické fáze letu a kritická místa při narušení signálu GNSS

Letectví patří mezi nejrychleji se rozvíjející a také nejbezpečnější způsoby dopravy. Podle aktuálních prognóz by mělo být v roce 2030 přepraveno 7 miliard osob po celém světě, což je dvojnásobný počet oproti současnému stavu. S ohledem na tento fakt je nutné zajistit požadovanou úroveň bezpečnosti v tomto odvětví a tu stále zvyšovat. Proto si v následující kapitole rozebereme, jaká jsou kritická místa a kritické fáze letu, při kterých je téma této bakalářské práce, rušení signálu GNSS, nejzávažnější. Zaměříme se také na metody odhalení těchto nežádoucích jevů a reakce, které mohou snižovat nebo úplně vyloučit pravděpodobnost jejich výskytu.

3.1 Kritické fáze letu

V dnešní době globální družicové navigace, kdy již i malá sportovní letadla disponují systémy, které využívají tento typ navigace, jsou na tyto systémy kladeny velké nároky. Vysoká přesnost, dostupnost, integrita, to jsou jen některé vlastnosti, které musí splňovat. Je tedy důležité, aby GNSS fungovala správně a to zejména během kritických fází letu.

Letadlo během letu prochází jednotlivými fázemi. Od vzletu, po nastoupání určité letové hladiny, letu po trati, až po zahájení klesání a přiblízení na přistání na cílové letiště a samotné přistání. Během tohoto letu, jak vyplývá z předchozí věty, letadlo mění svou výšku. I z tohoto důvodu je námi popisované rušení jinak závažné ve výšce 10 000 metrů nad zemí nebo při finálním přiblížení na přistání pomocí přesného přístrojového přiblížení využívající GNSS. Tyto rozdíly mezi jednotlivými výškami mohou být umocněny počasím. Špatná dohlednost, nízka základna oblačnosti, žádný vizuální kontakt se zemí, to vše může hrát při ztrátě signálu svoji roli. Proto za kritické fáze letu označujeme zejména přiblížení na přistání a vzlet. Souhrnně tedy okamžiky, kdy se letadlo nachází v malé výšce a na správná rozhodnutí není takové množství času, jako kdyby se letadlo pohybovalo v letové hladině během traťového letu.

3.2 Kritická místa

Pokud se zaměříme na místa a infrastrukturu, nikoho asi nepřekvapí, pokud za nejvíce kritická místa z pohledu rušení označíme letiště. V okolí velkého počtu letišť se nachází pozemní systém GBAS pro zpřesnění vlastností družicové navigace, jejíž rušení bylo popsáno v kapitole 2.4.1. Dalším podkladem pro toto tvrzení jsou také husté dopravní sítě s velmi frekventovanými dálnicemi v okolí letišť, kde řidiči vozidel mohou ať už záměrně nebo omylem ovlivnit kvalitu signálu z družic.

Dalšími místy, kde je rušení nežádoucí, jsou pozemní stanice systému SBAS. Tento typ zpřesnění GNSS má však po velké ploše rozmístěno velké množství stanic a tak je chvilkovému rušení jedné z nich mnohem více odolný, než v případě GBAS.

3.3 Systémy a metody pro odhalení rušení

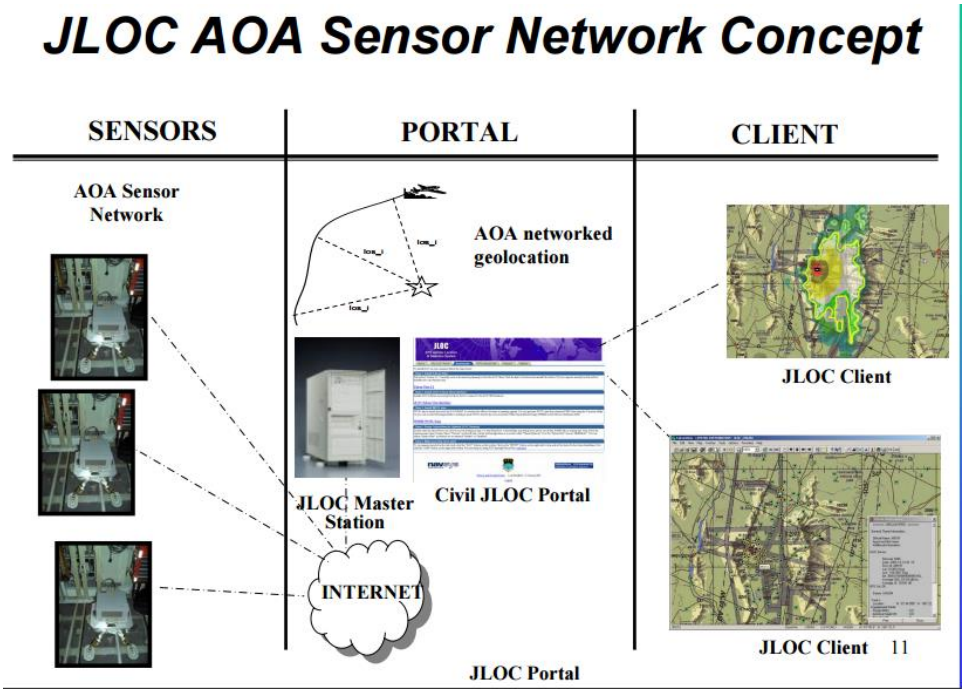
S nástupem velkého množství rušících zařízení se ve 21. století začaly formovat projekty a systémy pro detekci rušení a nasledné zmírňování následků. Můžeme mezi ně zařadit evropský Protector, americký JLOC nebo britský Gaardian. Jednotlivé projekty si zkráceně popíšeme v dalších kapitolách, avšak můžeme konstatovat, že všechny pracují na podobném principu a se stejným cílem-umisťovat senzory do kritických míst infrastruktury, detekovat rušení GNSS s jeho následnou charakterizací a včasné varování uživatelů o možných hrozbách.

3.3.1 JLOC - Jammer detection and location system

Jedním z prvních systému pro detekci rušení se stal americký JLOC. První návrhy na způsob fungování proběhly již na konci 20. století. Během dalších let probíhalo testování a v roce 2007 byl již systém provozně způsobilý pro své fungování. Mezi hlavní cíle tohoto systému patří monitorovat hrozby, které by mohly ovlivnit fungování GPS. Dále to jsou automatické výstrahy uživatelům, pokud je nějaká hrozba detekována a také předpovídat, kdy by mohlo rušení signálu nastat. Mimo to se také podílet na vytváření způsobu obrany proti potenciálním hrozbám.

Systém funguje na principu několika různých typů senzorů a hlavní stanice. Mezi senzory můžeme zařadit senzory pro měření poměru C/No, kterými se rušení detekuje a dále senzory pro charakterizaci a zjištění polohy daného zdroje rušení. Některé z nich měří úhel, pod jakým rušící signál přichází, dalšími se určuje časové zpoždění příchodu signálu. Všechny údaje z těchto senzorů se odesílají do řídící stanice, ve které se tyto jednotlivé informace vyhodnocují. Na základě vyhodnocení se poté informace o přitomnosti rušení dostávají k uživatelům.

Na obrázku 15 pro ilustraci vidíme princip fungování senzorů pro zjištění úhlu, pod jakým k nim rušící signál přichází.



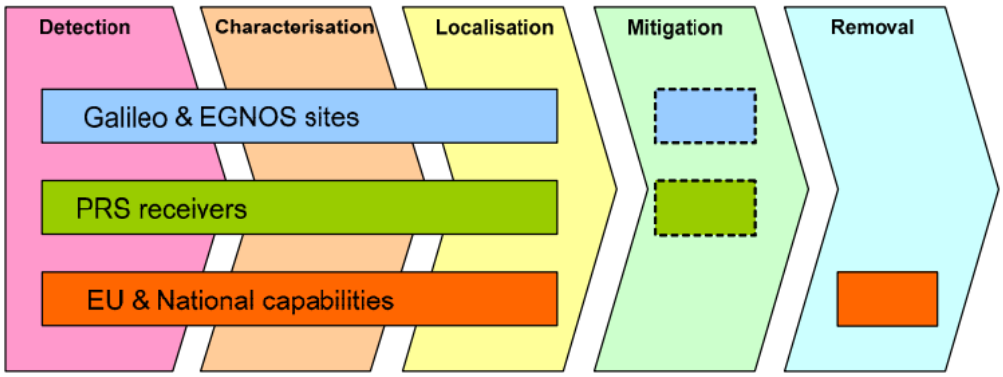
Obrázek 15 - JLOC senzory [5]

3.3.2 PROTECTOR

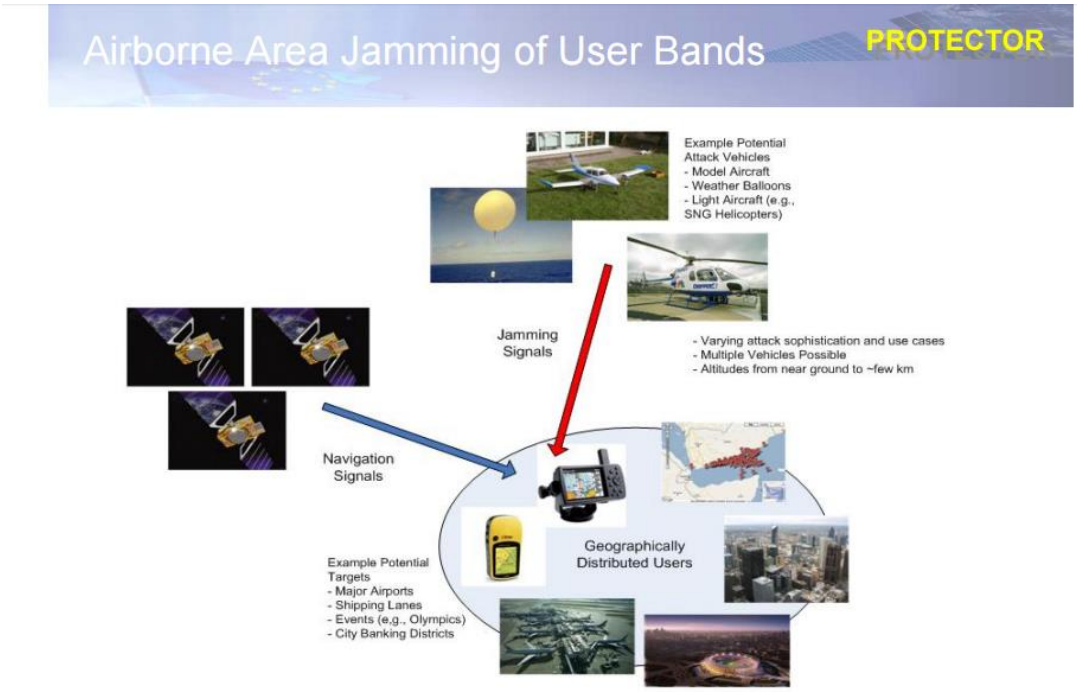
V roce 2010 byl v Evropě spuštěn 18-ti měsíční program PROTECTOR, jehož cílem opět bylo studovat, jak nejlépe chránit infrastrukturu a uživatele GNSS před nežádoucím rušením rádiových signálů. Byly kladeny otázky, z jakých zařízení a míst může rušení přicházet a uvažováno bylo kromě rušení pozemního také rušení ze vzduchu s využitím létajících modelů letadel nebo meteorologických balónů. Tyto případy jsou zobrazeny na obrázku číslo 17. Součástí projektu bylo také vytvoření konceptu systému JIMS (jamming and interference mitigations system) a jeho využívání v Evropě. Studie byla dokončena ke konci roku 2011.

Cílem konceptu systému JIMS bylo chránit kritickou infrastrukturu jakou jsou letiště nebo přístavy. Do těchto míst měly být umisťovány senzory, podobně jako u systému JLOC. Jednalo se o senzory na měření C/No poměru, na měření směru odkud rušící signál vychází, časové senzory a jiné. Údaje by poté podléhaly analýze, docházelo by k včasnému varování uživatelů o anomáliích a incidenty by podléhaly právnímu zkoumání.

Byly rovněž navrženy různé postupy, jak rušení signálu zmírnit. K tomu se mělo využívat adaptivní filtrování šumu, speciální antény určené pro snížení intenzity rušení a jiné. Na obrázku 16 vidíme cyklus systému JIMS.



Obrázek 16 - Cyklus systému JIMS zdroj [1]



Obrázek 17 - PROTECTOR rušení vzduch zdroj [1]

3.3.3 GAARDIAN a SENTINEL

Posledním projektem, který si popíšeme je projekt GAARDIAN a na něj navazující SENTINEL. GAARDIAN je britské konsorcium, které vzniko jako reakce na zvyšující se počet případů rušení signálu. Vedoucí pozici zastávala společnost Chronos Technology. Toto uskupení vymyslelo takový systém, který sleduje vlastnosti GNSS (zejména v kritických oblastech jakou jsou letiště) po celý rok a je schopen poskytovat informace o spolehlivosti systému v reálném čase. Je také vytvořena poplachová síť a při jakékoliv anomálii jsou uživatelé ihned informováni. Principem fungování je síť sond, které dokáží přijímat jak signál z globálních družicových systémů, tak z pozemního systému eLoran. Tyto sondy mimojiné obsahují malé atomové hodiny a na základě porovnávání časů z těchto dvou systému lze

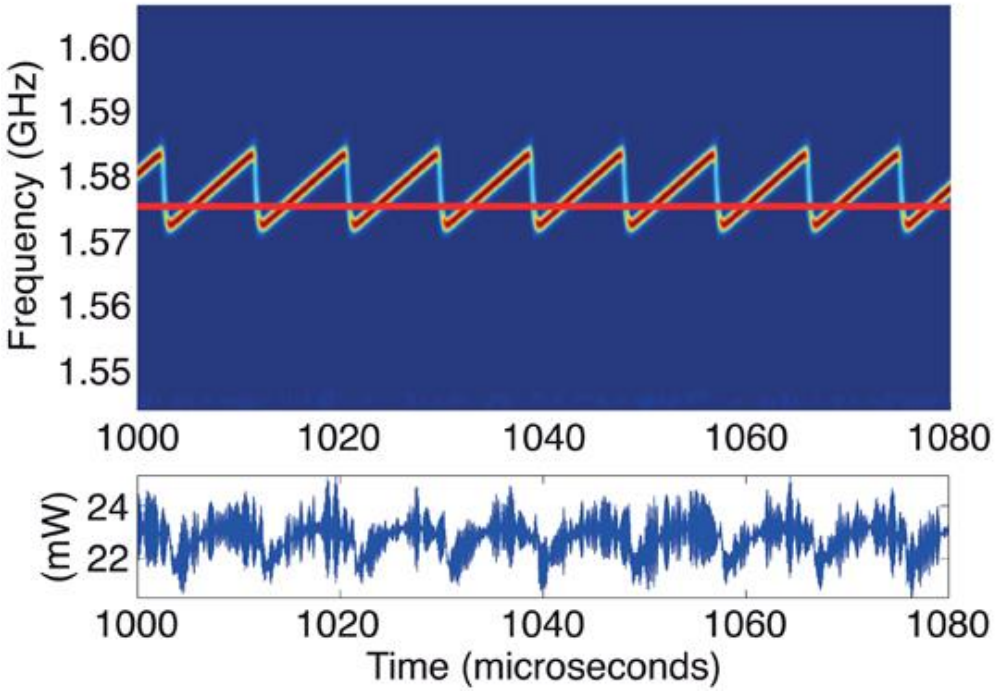
určit, zda je rušení na dané sondě přítomno a pokud ano, zda se jedná o člověkem záměrně vytvářené nebo přírodní.

Na GAARDIAN plynule navazuje SENTINEL, představený opět firmou Chronos Technology. Tento systém využívá podobné sondy jako předchozí GAARDIAN, nicméně sondy jsou vzájemně propojeny. To dává možnost určit polohu zdroje rušení pomocí triangulace.

3.3.4 Další metody odhalení rušení

Mimo již zmíněné systémy pro odhalení rušení existuje celá řada dalších způsobů, jak zjistit přítomnost rušení.

Jednou z nich je metoda v rámci projektu DETECTOR. Rušičky většinou nevysílají stále na jedné nosné frekvenci, ale kolem této hlavní frekvenci oscilují s různou amplitudou jak je vidět na obrázku 18. Každá rušička má tudíž nějaké charakteristické spektrum vysílání. Principem projektu bylo vytvoření databáze spekter všech známých rušících zařízení. Poté, když je detektorem spektrum přijmuto, dochází k porovnání tohoto spektra se spektry z vytvořené databáze. Na základě shod či neshod můžeme říci, zda rušení probíhá a jaký typ rušičky je použit.



Obrázek 18 - Spektrum rušičky [38]

Další možností, která byla představena na konferenci v Portlandu v roce 2010, bylo vytvoření aplikace pro chytré telefony s operčacním systémem Android, která by přeměnila telefony v JLOC senzory. Členové pohotovostních služeb a také veřejnost by byli vyzváni, aby si danou aplikaci stáhli a nechali zapnutou na svém chytrém telefonu. Tato metoda by poskytovala hustou síť pro detekci malých rušících zařízení.

Na internetu jsou v současné době dostupná také kapesní zařízení od společnosti Chronos. Tato zařížení dokáží detekovat a určit azimut, odkud rušení pochází a proto se využívají v přístavech, letištních parkovištích nebo skládkách vozového parku . Díky své velké přesnosti dokáží na rozlehlém parkovišti určit, v jakém autě je rušička ukryta. Zmínit můžeme například výrobek CTL3520 (obrázek 19), který je prozatím na nejvyšší úrovni v nabízeném sortimentu této společnosti.

Obrázek 19 - CTL3520 [31]

3.4 Reakce na rušení

V souvislosti s rostoucím počtem výskytů rušení signálů GNSS je nutné na ně vhodně reagovat. Některé reakce a úpravy budou popsány v následující kapitole.

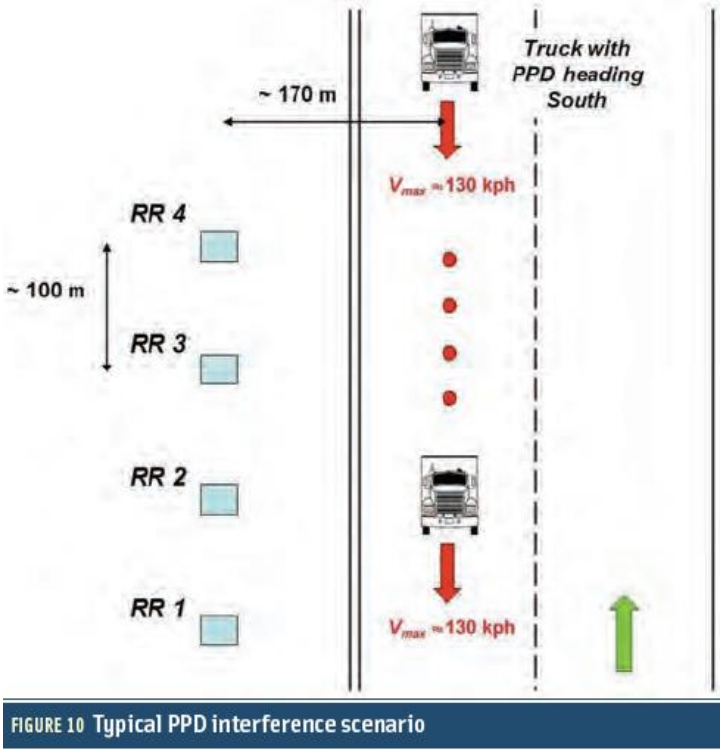
3.4.1 Upravení stanice GBAS Newark

V kapitole 2.4.1 je popsána situace z letiště v Newarku, kde docházelo k rušení signálu GNSS a pozemní stanice LAAS nebyla schopna správně fungovat. V souvislosti s vyskytujícím se rušením byla zavedena opatření, která vedla k omezení tohoto jevu.

V původní struktuře systému, nazvaného Block 0, docházelo k rušení několikrát během dne. Systém byl navrhnut tak, že jakmile došlo ke snížení poměru C/No na více než jednom přijímači pod přijatelnou úroveň, systém automaticky vyžadoval restart a po určitou dobu nebyl schopný poskytovat korekční data. Během měření bylo zjištěno, že nejménně odolný proti tomuto rušení je přijímač číslo 2. Vyzkoušeno bylo zvednutí jeho antény do větší výšky, s cílem odstranit vícecestné šíření a odrazy od země. Po tomto zavedení však byly pozorovány ještě větší anomálie než doposud, neboť byl snížen stínící efekt okolních překážek. Logickým krokem proto bylo anténu snížit. Tento pokus byl již úspěšnější a míra rušení poté dosahovala podobných hodnot, jako ostatní tři přijíače.

Hlavním zmírněním následků rušení však bylo zavedení vylepšeného software Block 1. Jednalo se o vylepšení původního algoritmu a novinkou bylo to, že mohlo docházet k chvilkové ztrátě signálu GNSS na dvou přijímačích zároveň. To je velkou výhodou, neboť z pozorování je zjištěno, že pokud nemá rušící zařízení extra silný výkon, dokáže rušit dva přijímače najednou a při přechodu na další je již příjem na prvním obnoven. Typický scénař je vidět na obrázku číslo 20, kdy nákladní vozidlo směřuje na jih a postupuje od přijímače 4 až po přijímač 1. V místech, kdy se nachází mezi přijímači 3 a 2 je však příjem na RR4 většinou obnoven a systém je plně funkční.

K rušení bohužel dochází i po této úpravě, avšak byl zaznamenán výrazný pokrok v tomto směru.



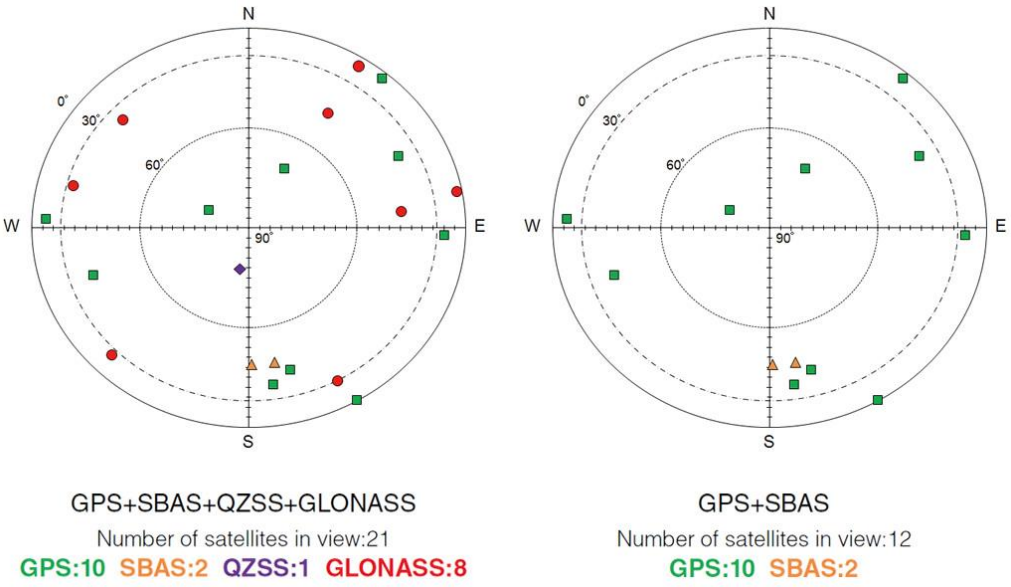
Obrázek 20 - Scenář rušení Newark [13]

3.4.2 Další reakce

V letectví se pro navigaci používají zejména GNSS služby a inerční navigační sytémy. Inerční systém tvoří kromě centrální jednotky velmi citlivé gyroskopy a akcelerometry. Při zadání počátečních podmínek (např. zrychlení -> časová integrace = rychlost -> druhá časová integrace = dráha) lze zobrazit polohu letadla v každém okamžiku letu a není zde nutné používat GNSS systémy. Nevýhodou této metody navigace je narůstající chyba v čase od poslední korekce. Z tohoto důvodu jsou v moderních letadlech tyto systémy ztrojeny, což umožňuje přesnější určování polohy. Během delších letů dochází k automatickým korekcím za pomoci údajů ze zařízení VOR a DME.

Dalšími způsoby, které mohou zvyšovat odolnost vůči rušení je poskytování záložních non GNSS služeb, které nejsou závislé na příjmu signálu ze satelitů. Mezi ně můžeme zařadit pozemní navigační systém eLoran.

Dalším typem ochrany proti nežádoucímu rušení signálů GNSS je poskytovaní multi GNSS služeb. To má 2 důležité výhody. První z nich je mnohem větší konstelace satelitů v dohledu a tím zvyšující se přesnost. To může být výhodné zejména v nehostinných oblastech a členitých terénech. Druhou výhodou, v souvislosti s tématem této práce mnohem zajímavější, větší odolnost vůči rušení využíváním a přijímáním více frekvencí současně (např. L1, L2). Pro ilustraci na přiloženém obrázku vidíme konstelaci satelitů při multi GNSS a při samotném GPS s vylepšením SBAS.



Obrázek 21 - Multi GNSS [37]

Svou roli v kvalitě přijmu signálů hraje také samotný přijímač a anténa. Některé antény jsou schopny adaptivního filtrování šumu a tím jsou méně náchylné k rušení.

Záměrné vysílání rušících signálů je nezákonné a protiprávní, a proto by mělo být trestáno přísněji se snahou snížit jeho výskyt.

4 Zhodnocení závažnosti

V závěrečné kapitole této bakalářské práce je zhodnocena závažnost rušení signálu GNSS. Uvedeme také módy navigace, které se při ztrátě signálu využívají a porovnáme vytvořené příklady vzhledem k bezpečnosti provedení letu.

4.1 Módy navigace při ztrátě signálu GNSS

Jak již plyne z předchozích kapitol, ztráta signálu ze systémů GNSS je pro letadla během letu vždy nežádoucí. Závažnost rušení je však rozdílná s ohledem na aktuální situaci. Pod pojmem aktuální situace si můžeme představit meteorologické podmínky nebo daný režim letu. Při dobré dohlednosti a viditelnosti země může pilot reagovat mnohem pružněji a efektivněji, než v případech, kdy mu meteorologická situace nedovolí problém řešit vizuálně, ale musí se spolehnout na jiné módy navigace nebo na informace z ostatních letadel a od řidících letového provozu. Jiné důsledky může mít také rušení v závislosti na režimu letu. Během traťového letu v hladině má posádka mnohem více času na řešení situace, než kdyby se nacházela v těsné blízkosti země. Z těchto poznatků plyne fakt, že nejzávažnější důsledky může mít rušení v situacích, kdy se letoun nachází ve špatných meteorologických podmínkách v blízkosti země.

Při ztrátě signálu GNSS během traťového letu existují dvě základní metody navigace. První z nich je metoda výpočtu (dead reckoning), kdy dochází k určení polohy letounu na základě poslední známé polohy za využití gyroskopů a akcelerometrů. Tento mód nelze využít během přiblížení a využívá se v případech, kdy je letoun vzdálen od letiště nejméně 30 námořních mil. Druhá metoda nese název „loss of integrity mode“, který se využívá v případech, kdy je letoun od letiště vzdálen méně než 30 námořních mil. V těchto případech se na navigačím displeji zobrazí nápis „NO GPS POSITION“ a všechny přijaté údaje z GNSS satelitů nejsou brány v úvahu. V těchto případech je nutná již zmíněna komunikace s řízením letového provozu a snaha letět do podmínek viditelnosti země.

Během přiblížení je rušení mnohem nebezpečnější a při využití typu přiblížení závislém na GNSS systémech se při detekci rušení objeví varovné hlášení „abort the approach“. Je nutné provést go around a přistání opakovat s možností přejít na nouzovou frekvenci.

4.2 Příklady posuzování závažnosti při rušení

Nyní si uvedeme několik typových příkladů, na kterých budeme posuzovat závažnost rušení signálu GNSS v dané situaci. Příklady se budou odlišovat typem letadla, letištěm přistání, za jakých pravidel je let prováděn a typem rušení. Závažnost budeme posuzovat vzhledem

ke třem kritériím, kterými jsou:

a) může letadlo kvůli rušení spadnout?

b) musí posádka zvyšovat pozornost?

c) dochází k narušení letového provozu v okolí letiště?

Na závěr sestavíme tabulku, ve které budou příklady seřazeny podle závažnosti.

4.2.1 Příklad 1

V příkladě číslo 1 uvažujeme takovou situaci, kdy máme k dispozici malý letoun Cessna 172 (zobrazený na obrázku 22) a letíme za pravidel VFR (Visual flight rules), tedy za podmínek viditelnosti země. Za těchto podmínek je GNSS navigace až druhořadým a doplňkovým typem navigace a piloti by měli létat za stálé dohlednosti země jen v určitých meteorologických podmínkách. Letiště přistání uvažujeme menší letiště v Jihlavě, které se využívá zejména pro rekreační létání a slouží také aeroklubovým účelům. Není tudíž vybaveno žádnými sofistikovanými systémy pro přesné přiblížení. Přítomným typem rušení bude jamming. Shrnutí vstupních informací udává tabulka dále.

Obrázek 22 - Cessna 172 [32]

Tabulka 6 - Parametry příkladu 1

Typ rušení	Letoun	Letiště	Pravidla letu
Jamming	Cessna 172	Jihlava	VFR

Z těchto vstupních parametrů a myšlenek, které jsou obsahem této podkapitoly, můžeme odpovědět na tři zásadní otázky, uvedené v kapitole 4.2. Letadlo nemůže spadnout a posádka nemusí zvyšovat svou pozornost, protože let probíhá za pravidel VFR a piloti tudíž provádí srovnávací navigaci s terénem a GNSS systémy pro svůj let tudíž nepotřebují. K narušení letového provozu v okolí letiště také nechodází, neboť není vybaveno systémy, které jsou na funkci GNSS závislé.

Tabulka 7 - Zodpovězení otázek příkladu 1

Může letadlo spadnout?	Musí posádka zvyšovat pozornost?	Dochází k narušení letového provozu?
NE	NE	NE

4.2.2 Příklad 2

V tomto příkladě budou vstupní parametry téměř totožné, jako jsou v předchozím příkladu. Jediným rozdílem bude letiště přistání, kterým nyní bude letiště Brno-Tuřany. U tohoto letiště již předpokládáme větší provoz a to jak menších sportovních tak i dopravních letounů, které mohou využívat GNSS systémy. Naše vstupní parametry jsou tudíž následující.

Tabulka 8 - Parametry příkladu 2

Typ rušení	Letoun	Letiště	Pravidla letu
Jamming	Cessna 172	Brno-Tuřany	VFR

Pro náš letoun se v tomto příkladě nic nemění. Posádka není nucena zvyšovat pozornost ani zde není hrozba, že by letadlo mohlo vlivem jammingu spadnout, protože pořád letíme za podmínek VFR a GNSS systémy nepotřebujeme. Horší dopad to však již může mít na ostatní provoz v okolí tohoto mezinárodního letiště. Jiná letadla již GNSS služby mohou na rozdíl od nás využívat a jejich rušení může způsobit narušení letového provozu a zvýšení zátěže jak na posádku těchto letadel, tak také na řídící letového provozu. Z tohoto pohledu je proto tento příklad závažnější, než byl ten předchozí. Odpovědi na otázky jsou uvedeny v následující tabulce.

Tabulka 9 - Zodpovězení otázek příkladu 2

Může letadlo spadnout?	Musí posádka zvyšovat pozornost?	Dochází k narušení letového provozu?
NE	NE	ANO

4.2.3 Příklad 3

V následujícím příkladě budeme uvažovat situaci, která je obdobná s příkladem číslo 1, tzn. typem rušení bude jamming a letištěm přistání bude jihlavské letiště. Budeme však uvažovat, že náš letoun, Cessna 172, je vybaven IFR (instrument flight rules) avionikou a tudíž poletíme alespoň zpočátku za těchto podmínek.

Tabulka 10 - Parametry příkladu 3

Typ rušení	Letoun	Letiště	Pravidla letu
Jamming	Cessna 172	Jihlava	IFR->VFR

Pro tento konkrétní příklad musíme však předpokládat, že letiště Jihlava není vybaveno takovými systémy, za kterých by bylo možné přistát pomocí GNSS systémů a tak musí letadlo v koncové fázi letu přejít na podmínky VFR. K tomuto kroku by mělo být přihlédnuto již při plánování letu. Letoun by se tedy neměl dostat do situace, která by hrozila pádem, protože pravidla VFR již opět vyžadují viditelnost země a přijatelné meteorologické podmínky. Nebude docházet ani k narušení provozu v okolí letiště, nicméně posádka bude nucena zvyšovat svoji pozornost v situacích, kdy by k jammingu docházelo ještě v době, kdy letí za IFR podmínek. Zhodnocení závažnosti v následující tabulce.

Tabulka 11 - Zodpovězení otázek příkladu 3

Může letadlo spadnout?	Musí posádka zvyšovat pozornost?	Dochází k narušení letového provozu?
NE	ANO	NE

4.2.4 Příklad 4

V dalším příkladě uvažujeme úplně stejnou situaci jako v tom předchozím, avšak cílovým letištěm bude opět letiště Brno-Tuřany. Naším letounem je opět Cessna 172 vybavena pro IFR lety a předpokládáme začátek letu za těchto podmínek s přechodem na VFR v koncové fázi letu.

Tabulka 12 - Parametry příkladu 4

Typ rušení	Letoun	Letiště	Pravidla letu
Jamming	Cessna 172	Brno-Tuřany	IFR->VFR

Tento případ je oproti tomu minulému opět o něco závažnější, protože v okolí letiště se mohou pohybovat letadla, zejména ta dopravní, která svůj celý let provádí za podmínek IFR

a využívají GNSS služby. Jejich rušení by proto mohlo ohrozit a narušit letový provoz v okolí tohoto letiště. Pro náš letoun se však nic nemění a nemůže dojít k pádu, protože koncová fáze probíhá za VFR podmínek a zde je opět nutná srovnávací navigace za dohlednosti země.

Tabulka 13 - Zodpovězení otázek příkladu 4

Může letadlo spadnout?	Musí posádka zvyšovat pozornost?	Dochází k narušení letového provozu?
NE	ANO	ANO

4.2.5 Příklad 5

V příkladě číslo 5 opustíme Cessnu a budeme uvažovat dopravní letoun Boeing 737-800, který můžeme vidět na obrázku níže.

Obrázek 23 - Boeing 737-800 [33]

Předpokládejme let podle přístrojů po celou dobu letu a cílovým místem přistání bude letiště Brno-Tuřany.

Tabulka 14 - Parametry příkladu 5

Typ rušení	Letoun	Letiště	Pravidla letu
Jamming	Boeing 737-800	Brno-Tuřany	IFR

Jelikož se letoun pohybuje celou dobu za IFR podmínek, existovala by reálně hrozba, že by mohlo dojít vlivem jammingu k pádu letadla. Tato letadla však mají i jiné záložní systémy pro poskytování navigace a tudíž je tento scénář vyloučen. To však nemění nic na tom, že posádka je nucena zvýšit svoji pozornost a je narušen letový provoz v okolí letiště.

Tabulka 15 - Zodpovězení otázek příkladu 5

Může letadlo spadnout?	Musí posádka zvyšovat pozornost?	Dochází k narušení letového provozu?
NE	ANO	ANO

4.2.6 Příklad 6

Následující příklad se bude odlišovat od těch předchozích v typu rušení. Nyní nebudeme předpokládat jamming jako tomu bylo doposud, ale spoofing, který je obecně mnohem více nebezpečnější. Letounem bude Cessna 172 a předpokládáme letiště Jihlava. Let bude proveden za podmínek IFR s přechodem na VFR v koncové fázi letu.

Tabulka 16 - Parametry příkladu 6

Typ rušení	Letoun	Letiště	Pravidla letu
Spoofing	Cessna 172	Jihlava	IFR->VFR

Za určitých okolností by mohlo v tomto případě dojít k pádu letadla a to zejména za špatných meteoroogických podmínek a ještě během letu podle přístrojů. Při spoofingu sleduje přijímač falešný signál a zobrazuje nesprávnou polohu letadla. Při žádném vizuálním kontaktu se zemí by proto letadlo mohlo být navedeno do míst, kde by došlo k nárazu do země. Malá letadla, jako je naše Cessna 172, nemají tak sofistikované systémy na rozpoznání rušení a založní poskytování navigace, a proto by mohlo dojít za určitých okolností k pádu.

Tabulka 17 - Zodpovězení otázek příkladu 6

Může letadlo spadnout?	Musí posádka zvyšovat pozornost?	Dochází k narušení letového provozu?
ANO	ANO	NE

4.2.7 Příklad 7

Tento příklad uvažuje situaci, která je totožná s příkladem předchozím, avšak letištěm je Brno-Tuřany.

Tabulka 18 - Parametry příkladu 7

Typ rušení	Letoun	Letiště	Pravidla letu
Spoofing	Cessna 172	Brno-Tuřany	IFR->VFR

Situace téměř totožná jako v příkladu 6, avšak pohybujeme se v okolí většího letiště s větším provozem a s poskytováním služeb řízení letového provozu. Z toho důvodu by přítomný spoofing mohl ovlivnit ostatní letadla a narušil by tak letový provoz. Tento příklad proto označíme jako nejzávažnější ze všech, které jsou v této kapitole uvedeny.

Tabulka 19 - Zodpovězení otázek příkladu 7

Může letadlo spadnout?	Musí posádka zvyšovat pozornost?	Dochází k narušení letového provozu?
ANO	ANO	ANO

4.2.8 Příklad 8

V závěrečném příkladu uvažujme Boeing 737-800 a letiště Brno-Tuřany. Let probíhá po celou dobu podle přístrojů a přítomným typem rušení je spoofing.

Tabuka 20 - Parametry příkladu 8

Typ rušení	Letoun	Letiště	Pravidla letu
Spoofing	Boeing 737-800	Brno-Tuřany	IFR

Scénář by mohl být úplně stejný jako v případě menší Cessny v předchozím případě, avšak jak již bylo zmíněno, dopravní letouny jsou vybaveny záložními službami poskytování navigace a tudíž nedojde k pádu letounu vlivem spoofingu.

Tabulka 21 - Zodpovězení otázek příkladu 8

Může letadlo spadnout?	Musí posádka zvyšovat pozornost?	Dochází k narušení letového provozu?
NE	ANO	ANO

4.2.9 Srovnání příkladů

Pro přehledné srovnání závažnosti rušení GNSS systémů výše zmíněných příkladů poslouží následující tabulka.

Tabulka 22 - Seřazení příkladů podle závažnosti

Pořadí	příklad	Kritérium 1	Kritérium 2	Kritérium 3
1	Př. 7	ANO	ANO	ANO
2	Př. 6	ANO	ANO	NE
3	Př. 8	NE	ANO	ANO
4	Př. 5	NE	ANO	ANO
5	Př. 4	NE	ANO	ANO
6	Př. 3	NE	ANO	NE
7	Př. 2	NE	NE	ANO
8	Př. 1	NE	NE	NE

Z tabulky plyne, že nejhorší dopad může mít rušení v případech, kdy se jedná o spoofing, a malé letadlo se pohybuje v okolí větších letišť s hustějším provozem. V tabulce je několik případů, kdy jsou jednotlivá kritéria totožná. Za závažnější se považuje ten z příkladů, kdy se jedná o letoun Boeing 737-800 s větším počtem cestujících a přítomným typem rušení je spoofing.

4.3 Shrnutí závažnosti, opatření

V současné době jsou GNSS systémy hojně využívány i v letectví. Proto je nutné provádět taková opatření, která by zamezila nežádoucímu rušení systémů, které jsou na signálech GNSS závislé. V letectví jsou to zejména letiště, kde jsou často instalovány pozemní systémy GBAS pro zpřesnění navigace. Uvést můžeme také další systém pro zpřesnění určování polohy a to SBAS. Ten je však chvilkovému rušení mnohem více odolný, než zmiňovaný GBAS. V těchto kritických místech infrastruktury by měly být umisťovány senzory (senzory na měření poměru C/No, senzory pro měření směru odkud signál přichází, atd.),

které by informace dále předávaly do řídícího střediska. Tam by docházelo k vyhodnocování a určení, zda se jedná o originální GNSS signál nebo o signál rušící. V případě rušícího signálu by mělo být vydáno varovné hlašení všem uživatelům, že systém není bezpečný k užívání.

Mimo závadění systémů pro detekci rušení je nutné poskytovat také záložní metody navigace a zajišťovat větší robustnost a odolnost GNSS systémů . Mezi tyto metody můžeme zahrnout využívání pozemních navigačních systémů (eLoran) nebo inerční metody výpočtu založené na principu akcelerometrů a gyroskopů. Pro větší odolnost GNSS systémů je výhodné poskytovat Multi GNSS.

Závěr

Hlavním cílem této bakalářské práce bylo přiblížit čtenáři základní principy fungování GNSS systémů, charakterizovat možné typy rušení signálů GNSS, navrhnout postup detekce tohoto rušení a zhodnotit jeho závažnost na příkladech týkajících se letecké dopravy. Pro bližší pochopení bylo nutné uvést několik příkladů z minulosti, kdy k rušení skutečně docházelo, a znát alespoň základní principy jak dopravního, tak malého sportovního létání. Z poznatků načerpaných během studia a zpracovávání této práce autor dospěl k závěru, že rušení signálu GNSS je v letecké dopravě vždy nežádoucí. Je jasné, že jiný dopad může mít rušení na malé letadlo určené k rekreačnímu létání a na moderní dopravní letadlo, které je vybaveno dalšími systémy poskytování navigace nezávislých na družicové navigaci. Nejhorší dopad by z pohledu autora mělo rušení na malé letadlo pohybující se v blízkosti většího letiště při přítomném rušení typu spoofing. Nutno však poznamenat, že se autor nesetkal s jediným případem, kdy by kvůli jakémukoliv typu rušení mohla být ohrožena bezpečnost letu do takové míry, že by mohl skončit katastrofou. I přes tento poznatek je nutné provádět taková opatření, která by zabraňovala a omezovala možný výskyt rušení ať už v letecké dopravě nebo dalších odvětvích, které jsou na GNSS systémech závislé.

Z výše uvedeného mohou být cíle této bakalářské práce označeny jako splněné.

Seznam použité literatury

1. DAVIES, Nigel, Christof SCHÄFER, Benoit VAUVY a Michael SCHOENHUBER. *PROTECTOR: Protecting European GNSS Services.* GNSS Interference, Detection and Mitigation, 2011 [online]. National Physical Laboratory: 2011 [cit. 2017-08-12]. Dostupné z: https://connect.innovateuk.org/documents/3347783/3709541/PROTECTOR+-+Protecting+European+GNSS+Services+from+Interference.pdf/c307d544-27d8-4599-9d87-726f05189261
2. LÁSKA, Zdeněk, Martin TEŠNAR, Jaroslav SLABÝ a Jan SUKUP. *Globální navigační satelitní systémy a jejich využití v praxi:* [online]. 2010 [cit. 2017-08-12]. Dostupné z: http://www.crr.vutbr.cz/system/files/brozura_08_1009.pdf
3. RÜGAMER, Alexander a Dirk KOWALEWKSI. *Jamming and spoofing of GNSS Signals-An Underestimated Risk?!:* [online]. Sofia, Bulgaria: 2015 [cit. 2017-08-12]. Dostupné z: https://www.fig.net/resources/proceedings/fig_proceedings/fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf
4. KNIGHT, Jerry, Charles CAHN a Sidharth NAIR. *A New Anti-Jamming Method for GNSS Receivers:* [online]. 2007 [cit. 2017-08-12]. Dostupné z: https://www.navcomtech.com/navcom_en_US/docs/download_center/white_papers/current/sapphire_jamming_test_report_8_jan_2007v3.pdf
5. BROWN, Alison a Rick EDWARDS. *Civil Applications of the GPS Jamming Detection and Location (JLOC) System: GPS Jamming & Interference-A Clear and Present Danger.* [online]. Colorado Springs, CO 80921 USA: NAVSYS Corporation, February 2010 [cit. 2017-08-12]. Dostupné z: https://connect.innovateuk.org/documents/3120492/3713273/Civil+Applications+of+the+GPS+Jamming+Detection+%26+Location+(JLOC)%20System.pdf/5d5fe60c-dbf5-43f0-850b-d19d451c3589;jsessionid=B2FA2EED4225B16409AB1E9FA13E407E.2
6. KUUSNIEMI, Heidi. *Effects of GNSS jammers and potential mitigation approaches:* [online]. Riga, Latvia: Finnish Geodetic Institute, May 2012 [cit. 2017-08-12]. Dostupné z: http://www.unoosa.org/documents/pdf/psa/activities/2012/un-latvia/ppt/3-14.pdf
7. CURRY, Charles. *GPS Jamming-Quantifying the Threat:* [online]. San Jose, USA: Chronos Technology Ltd, April 2013 [cit. 2017-08-12]. Dostupné z: http://tf.nist.gov/seminars/WSTS/PDFs/7-2_CTL_Curry_GPS_Jamming%20ver%202.pdf
8. BROWN, Alison, Dale REYNOLDS, Darren ROBERTS a Steve SERIE. *JAMMER AND INTERFERENCE LOCATION SYSTEM-DESIGN AND INITIAL TEST RESULTS:* [online]. Nashville, USA: September 1999 [cit. 2017-08-12]. Dostupné z: https://pdfs.semanticscholar.org/62c9/1e3c8133c4d5f7b917005b92aea66f5bf335.pdf
9. FONTANELLA, Diana, Roland BAUERNFEIND a Bernd EISSFELLER. *In-Car GNSS Jammer Localization Using Vehicular Ad-Hoc Networks:* [online]. University Faf Munich,

Germany: May/June 2013 [cit. 2017-08-12]. Dostupné z: http://www.insidegnss.com/auto/mayjune13-WP.pdf

10. BHUIYAN, H.Mohammad Zahidul, Heidi KUUSNIEMI, Stefan SÖDERHOLM a Esa AIROS. *The Impact of Interference on GNSS Receiver Observables-A Running Digital Sum Based Simple Jammer Detector:* [online]. Kirkkonummi a Riihimäki, Finland: 2014 [cit. 2017-08-12]. Dostupné z: https://www.radioeng.cz/fulltexts/2014/14_03_0898_0906.pdf
11. RUOTSALAINEN, Laura, Heidi KUUSNIEMI, Mohammad Zahidul H.BHUIYAN, Stefan SÖDERHOLM, Martti KIRKKO-JAAKKOLA, Sarang THOMBRE, Salomon HONKALA. *DETERJAM: Detection, analysis, and risk management of satellite navigation jamming.* [online]. Finland: 2014 [cit. 2017-08-12]. Dostupné z: http://www.defmin.fi/files/3031/2500M-0006.pdf
12. BOYNTON, Franck, Peter F. MACDORAN, Michael B. MATHEWS, Michael O. DAVIES. *GNSS Interference Detection and Mitigation for UAV Navigation:* [online]. 2014 [cit. 2017-08-12]. Dostupné z: http://gpsworld.com/wp-content/uploads/2014/05/Loctronix-2014-GNSS-Webinar-140521-final.pdf
13. PULLEN, Sam a Grace GAO. *GNSS Jamming in the Name of Privacy: Potential Threat to GPS Aviation.* [online]. Stanford University: March/April 2012 [cit. 2017-08-12]. Dostupné z: http://www.insidegnss.com/auto/marapr12-Pullen.pdf
14. SCOTT, Logan. *Spoofing: Upping the Anti.* [online]. July/August 2013 [cit. 2017-08-12]. Dostupné z: http://www.insidegnss.com/auto/IGM_TLS07_13.pdf
15. JONES, Michael. *The Civilian Battlefield:* [online]. March/April 2011 [cit. 2017-08-12]. Dostupné z: http://www.insidegnss.com/auto/marapr11-Jones.pdf
16. MINISTERSTVO DOPRAVY. *Český kosmický portál: Informační stránky Koordinační rady ministra dopravy pro kosmické aktivity.* [online]. 2011 [cit. 2017-08-12]. Dostupné z: http://www.czechspaceportal.cz/
17. Globální družicový polohový systém. In: *Wikipedia:* [online]. Wikimedia Foundation, 2001-, 26.7.2017 [cit. 2017-08-12]. Dostupné z: https://cs.wikipedia.org/wiki/Glob%C3%A1ln%C3%AD_dru%C5%BEicov%C3%BD_polohov%C3%BD_syst%C3%A9m
18. No Jam Tomorrow. *The Economist:* [online]. March 2011 [cit. 2017-08-12]. Dostupné z: http://www.economist.com/node/18304246
19. GNSS MONITORING:JAMMING THE JAMMERS. *Thales:* [online]. October 2014 [cit. 2017-08-12]. Dostupné z: https://www.thalesgroup.com/en/worldwide/aerospace/news/gnss-monitoring-jamming-jammers

20. *Thales: The New Thales*. [online]. 2007 [cit. 2017-08-12]. Dostupné z: https://www.thalesgroup.com/en
21. *NovAtel:* [online]. [cit. 2017-08-12]. Dostupné z: https://www.novatel.com
22. PROCTOR, Andy G., Charles W.T. CURRY, Jenna TONG, Robert WATSON, Mark GREAVES a Paul CRUDDACE. GAARDIAN: A system to detect GNSS jamming and Interference: In: *Coordinates:* [online]. August 2012 [cit. 2017-08-12]. Dostupné z: http://mycoordinates.org/gaardian-a-system-to-detect-gnss-jamming-and-interference/
23. National Coordination Office for Space-Based Positioning , Navigation, and Timing. *GPS.GOV: Official U.S. government information about the Global Positioning Systém (GPS) and related topics.* [online]. 1.8.2017 [cit. 2017-8-13]. Dostupné z: http://www.gps.gov/
24. POZZOBON, Oscar. The Future of GNSS Security: Threat Development Parallels Information/Communication Technology. In: *GPS World:* [online]. December 2012 [cit. 2017-08-13]. Dostupné z: http://gpsworld.com/directions-2013-the-future-of-gnss-security/
25. BAUERNFEIND, Roland, Thomas KRAUS, Dominic DÖTTERBÖCK, Bernd EISSFELLER, Erwin LOEHNERT a Elmar WITTMANN. Car Jammers: Interference Analysis: In: *GPS World:* [online]. October 2011 [cit. 2017-08-13]. Dostupné z: http://gpsworld.com/transportationroadcar-jammers-interference-analysis-12128/
26. An Introduction to GNSS. *Novatel:* [online]. [cit 2017-08-13]. Dostupné z: https://www.novatel.com/an-introduction-to-gnss/chapter-1-gnss-overview/section-1/
27. What is GNSS?. *OXTS: Inertial + GNSS.* [online]. [cit. 2017-08-13]. Dostupné z: http://www.oxts.com/what-is-inertial-navigation-guide/what-is-gnss/
28. What is SBAS?. *European Global Navigation Satellite Systems Agency:* [online]. July 2016 [2017-08-13]. Dostupné z: https://www.gsa.europa.eu/european-gnss/what-gnss/what-sbas
29. Difference between In-band jamming and Out-band jamming. *RF Wireless World:* [online]. [cit. 2017-08-13]. Dostupné z: http://www.rfwireless-world.com/Terminology/In-band-jamming-vs-Out-band-jamming.html
30. GRABOWSKI, Joseph C. Personal Privacy Jammers: Locating Jersey PPDs: Jamming GBAS Safety-of-Life Signals. In: *GPS World:* [online]. April 2012 [cit. 2017-08-13]. Dostupné z: http://gpsworld.com/personal-privacy-jammers-12837/
31. CTL3520 Handheld GPS Jammer Detector and Locator. *GPS World:* [online]. [cit. 2017-08-13]. Dostupné z: http://www.gps-world.biz/index.php/products/gps-jamming-detection/products-solutions/ctl-3520
32. Cessna 172 SP. *Aeroweb:* [online]. [cit. 2017-08-13]. Dostupné z: http://www.aeroweb.cz/katalog/letadlo.aspx?mkat=0&item=274

33. ČERNÝ, Zdeněk. B737-8K5: In: *Planes:* [online]. 2016 [cit. 2017-08-13]. Dostupné z: https://www.planes.cz/cs/photo/1219044/b737-8k5-ok-tvp-smartwings-tvs-qs-ostrava-osr-lkmt
34. Government of Canada. Space Weather Effects on GPS. *Space Weather Canada:* [online]. October 2016 [cit. 2017-08-13]. Dostupné z: http://www.spaceweather.gc.ca/tech/se-gps-en.php
35. Portable wireless bug camera jammer. *Jammer4U.CO.UK:* [online]. January 2011 [cit. 2017-08-13]. Dostupné z: http://www.jammer4uk.com/portable-wireless-bug-camera-jammer-p-25.html
36. In Car Use GPS Signal Jammer Blocker. *PhoneJammer:* [online]. [cit. 2017-08-13]. Dostupné z: http://www.phonejammer.com.au/in-car-use-gps-signal-jammer-blocker-p-136.html
37. Multi GNSS (Multi-Frequency GNSS). *Furuno:* [online]. [cit. 2017-08-13]. Dostupné z: http://www.furuno.com/en/gnss/technical/tec_multi
38. MITCH, H. Ryan, Ryan C. DOUGHERTY, Mark L. PSIAKI, Steven P. POWELL, Brady W. O'HANLON, Jahshan A. BHATTI a Todd E. HUMPHREYS. Signal Characteristics of Civil GPS Jammers: In: *GPS World:* [online]. January 2012 [cit. 2017-08-13]. Dostupné z: http://gpsworld.com/gnss-systeminnovation-know-your-enemy-12475/

Seznam obrázků

Seznam tabulek