FAKULTA
APLIKOVANÝCH VĚD
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

DIPLOMOVÁ PRÁCE

Techniky pro detekci podvržených signálů v satelitní navigaci

Student: Bc. Ondřej Dohnal
Vedoucí práce: doc. Ing. Jindřich Duník, Ph.D.

Plzeň, 2024

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta aplikovaných věd
Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Ondřej DOHNAL**
Osobní číslo:	**A22N0088P**
Studijní program:	**N0714A150011 Kybernetika a řídicí technika**
Specializace:	**Automatické řízení a robotika**
Téma práce:	**Techniky pro detekci podvržených signálů v satelitní navigaci**
Zadávající katedra:	**Katedra kybernetiky**

Zásady pro vypracování

1. Seznamte se s fungováním satelitní navigace a způsoby podvržení jejích signálů (tzv. spoofing).
2. Vypracujte přehled technik detekce podvržení pro stacionární přijímače.
3. Vybranou techniku (příp. techniky) ověřte simulačně.

Rozsah diplomové práce: **40-50 stránek A4**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

P. Y. Hwang and G. A. McGraw, "Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis," in Record – IEEE PLANS, Position Location and Navigation Symposium. Monterey, CA,USA: IEEE, 2014, pp. 270–281. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6851386

M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," in *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258-1270, June 2016, doi: 10.1109/JPROC.2016.2526658.
Paul Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, Second Edition* , Artech, 2013.

Vedoucí diplomové práce: **Doc. Ing. Jindřich Duník, Ph.D.**
Katedra kybernetiky

Datum zadání diplomové práce: **2. října 2023**
Termín odevzdání diplomové práce: **20. května 2024**

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
L.S.

Doc. Ing. Miloš Železný, Ph.D.
děkan

Doc. Dr. Ing. Vlasta Radová
vedoucí katedry

V Plzni dne 2. října 2023

Prohlášení

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

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a výhradně s použitím odborné literatury a pramenů, jejíž úplný seznam je její součástí.

V Plzni, 2024 .....

Poděkování

Rád bych vyjádřil svou upřímnou vděčnost všem, kteří mi pomohli při vypracování této diplomové práce. Nejprve bych chtěl poděkovat mému vedoucímu doc. Ing. Jindřichu Duníkovi, Ph.D., za jeho neocenitelné rady, trpělivost a podporu během celého procesu výzkumu a psaní diplomové práce. Jeho odborné znalosti a vedení mi byly velkým zdrojem inspirace.

Dále nemohu opomenout svou rodinu a přátele, kteří mě povzbuzovali a dodávali mi sílu v průběhu celého mého studia. Děkuji za vaši nekonečnou trpělivost a lásku.

Také bych chtěl vyjádřit uznání všem autorům relevantních knih, článků a studií, jejichž práce mi poskytla potřebný teoretický základ pro tuto diplomovou práci.

Nakonec bych rád poděkoval všem, kteří mi v různých situacích pomohli, ať už morálně, emocionálně nebo prakticky.

Tato diplomová práce by nebyla možná bez vaší podpory a přínosu, a za to jsem vám vděčný.

Abstrakt

V této diplomové práci se budeme věnovat otázce detekce napadení satelitních signálů poskytovaných systémem GPS. Toto napadení bude založené na bázi spoofingu, nebo-li falšování těchto signálů, které se bude zaměřovat na změnu časové informace přenášené signálem. Změna časové základny naruší proces synchronizace hodin napadeného přijímače s časovou osou konstelace GPS, což může vyústit v nejrůznější komplikace v oblastech spoléhajících na přesný čas. Mezi takové oblasti patří doprava, energetika či finanční sektor. V práci tak bude představena metoda detekce spoofingu, která vychází ze statistické analýzy měřených pseudo-vzdáleností poskytované systémem GPS pouze z měřené pseudo-vzdálenosti poskytované GPS signálem, bez nutnosti dodatečných senzorů či znalosti softwarového a hardwarového vybavení GPS přijímače. Tato metoda je založena na Allanově varianci. Jedná se o statistickou metodu, využívanou k analýze časových řad, která bude počítána z odhadů času GPS konstelace daného přijímače. Detekce bude zobrazena vizuálně, jako porovnání určených průběhů variancí s referenčními mezemi, vyjádřenými pro signál bez napadení. Funkčnost detekční metody bude simulačně ověřena a diskutována na několika případech podvrženého signálu. Nakonec se zaměříme na nastínění kroků, které by mohli vést k zpřesnění detekce.

Klíčová slova: GPS, satelitní signály, pseudo-vzdálenosti, napadení, generování podvržených signálu, jamming, spoofing, detekce napadení, časová oblast, synchronizace hodin, Allanova variance, metoda nejmenších čtverců, simulace GPS

Abstract

In this thesis we will address the issue of detection of attacks on satellite signals provided by GPS. This attack will be based on spoofing, or falsification of these signals, which will focus on altering the temporal information transmitted by the signal. The change in the time base will disrupt the process of synchronising the clock of the compromised receiver with the time axis of the GPS constellation, which may result in various complications in areas relying on accurate time. Such areas include the transport, energy and financial sectors. Thus, this paper will present a spoofing detection method that relies on statistical analysis of the measured pseudo-distances provided by the GPS system only from the measured pseudo-distance provided by the GPS signal, without the need for additional sensors or knowledge of the GPS receiver software and hardware. This method is based on Allan's variance. It is a statistical method used to analyse time series that will be calculated from the time estimates of the GPS constellation of a given receiver. The detection will be displayed visually, as a comparison of the determined variance traces with reference limits expressed for a signal without attack. The performance of the detection method will be verified by simulation and discussed on several cases of a spoofed signal. Finally, we will focus on outlining steps that could lead to more accurate detection.

Key words: GPS, satellite signals, pseudo-ranges, attacks, spoofed signal generation, jamming, spoofing, attack detection, time domain, clock synchronization, Allan variance, least squares method, GPS simulation

Obsah

1 Úvod

První kroky k uvedení globální satelitní navigace do provozu začaly v 2. polovině 20. století, kdy byly vypuštěny první americké testovací satelity systému GPS (z angl. Global Positioning System). Ke konci století se již jednalo o plně funkční satelitní systém. Z počátku byl přesný signál z těchto systémů využíván pouze k vojenským účelům a pro veřejnost byl degradován. To vedlo k horší kvalitě určované polohy, která měla neurčitost v řádu přibližně 100 metrů. Nicméně netrvalo dlouho a počátkem 21. století byl přesný systém k dispozici i veřejnosti. Hlavním oblastí využití byl letecký průmysl, kde tento druh navigace nahradil dosavadní rádiové systémy, jako například LORAN (z angl. Long Range Navigation). S rostoucí kvalitou určení polohy a klesající cenou nutného vybavení přineslo několik posledních let obrovské rozšíření satelitních systémů. Vznikli tak další navigační systémy jako ruský GLONASS (z rus. Globalnaja navigacionnaja sputnikovaja sistěma) nebo evropský Galileo a další. Tyto systémy se souhrnně začaly označovat jako globální navigační satelitní systémy, zkráceně GNSS. Cílem těchto systému pak je poskytnout globální pokrytí signály, které jsou nutné k nalezení obecného PVT řešení (z angl. position, velocity and time), tj. k učení pozice, rychlosti a časové korekce přijímače.

Kromě určování polohy se také začaly tyto systémy využívat k synchronizaci času na základě atomových hodin družic, například v bankovnictví, energetice, telekomunikacích a plánování dopravy. V současné době se tak lze setkat s zařízeními využívající signály GNSS na denní bázi, kdy jde především o telefony a dopravní prostředky.

Nicméně s rozšířením využití satelitní navigace přichází i nové výzvy. Jelikož je signál GNSS velice snadné, za pomoci běžně dostupných prostředků rušit nebo zachytit a napodobit, stává se jednou z hlavních výzev včasná detekce napadení satelitních signálů. Takové napadení může mít vážné důsledky pro fungování řady aplikací. Útok může způsobit nedůvěryhodnost signálu, či jeho úplné ztracení. Například v roce 2011 se Íránu podařilo úspěšně zachytit americký bezpilotní dron, který údajně monitoroval jejich jaderné zařízení. Toho bylo docíleno za pomoci falšování GNSS signálů, které dron oklamali a bez většího poškození nechali přistát na Íránském území [1]. Následně v roce 2017 došlo k incidentu, kdy byla chybně určena poloha 20 lodí. To bylo způsobeno podobným problémem. Ten vedl k tomu, že navigační zařízení lodí lokalizovalo jejich polohu několik kilometrů od místa, kde se právě plavily [1]. Uvedené příklady ilustrují napadení GNSS signálů formou tzv. spoofingu, nebo-li falšování navigačních signálů. To je napadení, kdy na základě autentického signálu poskytovaného GNSS útočník generuje falešný signál, který následně poskytuje napadeným zařízením. Ty následně ztrácejí schopnost správně určit polohu či synchronizovat čas.

1.1 Cíl diplomové práce

V dnešní době, kdy se satelitní navigace stává nezbytnou součástí našeho každodenního života, je důležité pochopit a řešit takové potenciální hrozby, které mohou ohrozit integritu a spolehlivost těchto systémů. Tato diplomové práce se tak bude zabývat problémem napadení GNSS signálů a jeho detekcí.

Soustředit se budeme převážně na detekci falšovaného (spoofovaného) GPS signálů poskytovaného stacionárním přijímačům. Jelikož máme stacionární přijímače, které ve většině situací mají svou polohu přesně zaměřenou, bude se jednat hlavně o útoky zaměřené na změnění časové osy přenášené těmito signály. To bude prováděno útočníkem s cílem oklamat přijímač napadeného uživatele a docílit tak jeho chybné synchronizace času, či výjimečně i určení polohy.

Z existujících studií se pouze několik z nich zaměřuje na útoku působících změny v časové oblasti a ještě méně na jejich detekci. Jiang a další prokázali pouze s využitím simulací proveditelnost útoku GPS časového spoofingu [2]. Mattei a spol pak představili detekci podvržených signálů v časové oblasti prostřednictvím porovnání více fázových měřících jednotek [3]. Jedná se o metodu založenou na ochranných relé, které fungující jako fázová měřící jednotka. Vychází tak z předpokladu specifického hardwarového zařízení, které nemusí být součástí běžně užívaných přijímačů.

My se zaměříme na metodu, která k potencionální detekci napadení nepotřebuje dodatečný hardware, ani software a vystačí si pouze s daty získanými ze satelitních signálů GNSS. Jednat

se bude o detekční metodu založenou na Allanově varianci (AVAR), s pomocí které se pokusíme detekovat napadení v časové oblasti. Tuto metodu jsme zvolili, jelikož předchozí studie zabývající se detekcí v poziční oblasti měly slibné výsledky, viz [4], a nás zajímá, zda bude možné tuto metodu využít i v časové oblasti. AVAR je statistická metoda používaná k analýze časových řad, která je zvlášť účinná pro detekci anomálii v takových datech. Pro ověření funkčnosti a spolehlivosti této metody budeme v našem výzkumu simulovat různé situace ovlivňující kvalitu falšovaného signálu. Jednat se bude především o věrnost modelování působících šumů na autentické GNSS signály útočníkem, přesnost jeho zaměření uživatelského přijímače či počátek působení napadení. Výsledky pro různé situace nám pak poskytnou lepší vhled o funkčnosti metody.

Cílem této diplomové práce je tak nejen uvést čtenáře do problematiky satelitní navigace a jejího napadení, ale především poskytnout podrobný přehled o zkoumané detekční metodě Allanovy variance. Ta by měla přinést možnost další doplňkové softwarové detekce k současným metodám. Zároveň však představíme a budeme diskutovat výsledky našeho výzkumu. Věříme, že naše práce přispěje k lepšímu pochopení tohoto důležitého problému a poskytne cenné informace pro další výzkum a vývoj v oblasti detekce napadení falšujícího časové základny přenášené navigačními signály.

V budoucnu by tak mohl další výzkum problému detekce falšování GNSS signálů přinést zvýšení jejich bezpečnosti a spolehlivosti, což by mohlo vést k většímu využití GNSS ve kritických oblastech či vývoji nových technologií spoléhajících na data z těchto systémů.

1.2 Struktura práce

Tato práce je strukturována tak, aby poskytla čtenářům jasný a srozumitelný přehled o našem výzkumu. Každá kapitola je pečlivě navržena tak, aby poskytla podrobné informace o konkrétním aspektu našeho výzkumu.

V první části si nejprve představíme základy fungování satelitní navigace. Budeme se zde zabývat strukturou GNSS, společně se souřadnými systémy a metodami nezbytnými k určování polohy. Neopomeneme zde ani neúmyslné vlivy působící na kvalitu přenášeného signálu. Závěrem první části si představíme metody využívané k odhadu polohy a času z měřených dat přenášených signálem.

Druhá část následně bude věnována motivaci zkoumání tohoto problému, kde si uvedeme simulační příklad a možné cíle této práce.

V další části práce se podrobněji seznámíme s úmyslnými způsoby napadení satelitních signálů jako je jamming (rušení signálů) a spoofing (falšování signálů). Podrobněji si zde poté rozvedeme spoofing, kde si představíme i způsob generování podvrženého signálu útočníkem, který následně využijeme v simulační části této práce.

Ve čtvrté části se zaměříme na detekční metody využívané k napadení formou spoofingu. Zde si uvedeme základní hardwarové metody využívané k detekci a představíme si Allanovu varianci se způsobem, jakým se dá využít k detekci napadení z časové oblasti.

Pátou, předposlední částí si představíme náš simulační model. Uvedeme zde podrobný postup generování polohy satelitů jejich pseudo-vzdálenosti od daného přijímače a jeho offsetu hodin od atomových hodin konstelace GPS. Dále zde bude využita metoda odhadu vycházející z nejmenších čtverců k znázornění kvality odhadu offsetu hodin.

Šestá a poslední část bude věnována výsledkům simulace a jejich popisu. Představíme několik simulovaných situací. Začneme nejsložitějším případem, kdy je útočník schopen přesně modelovat vlastnosti působícího šumu na autentické GPS signály. Postupně se skrze tento případ dostaneme k realističtější situaci, kde si uvedeme jak se rozšíří detekční možnosti, pokud nebude modelování přesné. Závěrem této části diskutujeme a zhodnotíme všechny námi dosažená výsledky.

2 Základy satelitní navigace

Předtím než-li se začneme podrobněji věnovat tématu této práce, je třeba si představit základy, ze kterých vycházíme. V této kapitole si tak nejprve představíme jakým způsobem se určuje poloha, kdy si uvedeme hlavní metody a jejich porovnání. Pokračovat budeme souřadnicovými rámci, definujícími prostor či plochu, ve které se nacházíme a jejich vzájemné závislosti. A nakonec si tyto pojmy zasadíme do globálního navigačního satelitního systém systému, u kterého si také uvedeme jeho strukturu, princip fungování a jak díky němu získáváme potřebná měření.

2.1 Úvod do satelitní navigace

Problémem lokalizace, pohybu a orientace v geografickém prostoru se již od nepaměti zabývá obor navigace. Navigaci je podle [5] možné definovat jako proces, spočívající převážně v přesném určení polohy a jejím následném využití. Metody a technologie využívané k těmto účelům se v průběhu času vyvíjely. Od pouhého pozorování nebeských těles nebo orientačních bodů, přes využití astrolábů či sextantů, až po moderní éru satelitní navigace založené na rádiových signálech.

V současnosti představuje revoluční technologii, nejen v oblasti navigace, globální navigační satelitní systém, nebo-li GNSS. Jedná se o souhrnný pojem označující systémy satelitní navigace, které poskytují globální pokrytí a umožňují určení polohy, rychlosti a času pro uživatele na celém světě. Oproti většině pozemním technologiím, které kvůli své signálové geometrii určují polohu pouze ve dvourozměrném prostoru, je GNSS schopno tuto polohu určit tří-dimenzionální.

Kromě určení polohy, systém také poskytuje možnost časové synchronizace. Tento proces slouží k harmonizaci hodin všech zařízení a zavedení společného časového referenčního bodu. Během tohoto procesu se na základě stabilních a přesných referenčních hodin, například atomových, umístěných na satelitu a korigovaných pozemními stanicemi, periodicky aktualizují hodiny v každém zařízení.

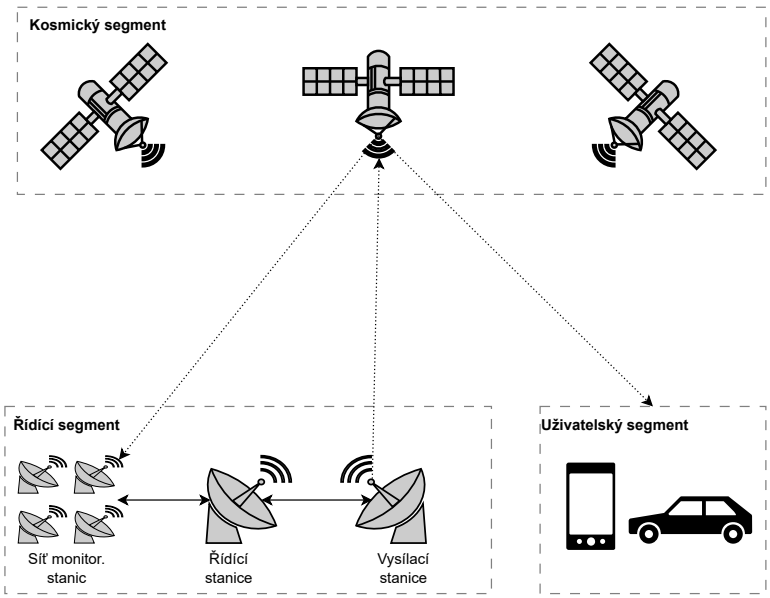
Satelity obíhající kolem Země po daných orbitách vysílají rádiové signály k povrchu planety, které tvoří nezbytný základ k fungování GNSS. Tyto signály jsou následně za pomocí přijímačů zachyceny a zpracovány. Hlavním cílem GNSS je pak synchronizovat čas těchto uživatelských přijímačů a poskytovat jejich co nejpřesnější polohu v reálném čase.

Poloha uživatele získaná prostřednictvím GNSS poskytuje přesnost v jednotkách metrů (v závislosti na počtu a vlastnostech přijímaných signálů), což je vyšší přesnost než-li jsme schopni dosáhnout za pomoci pozemních systémů. Mezi tyto systémy patří například DME (z angl. Distance Measuring Equipment), kde se jedná o zařízení užívané v oblasti letectví k určení vzdálenosti mezi letadlem a pozemním radarem či LORAN (z angl. Long Range Navigaion) což byl rádiový navigační systém, jehož principiální funkci převzali GNSS. Signály získané ze satelitů jsou však slabé, a tudíž náchylné na náhodné i úmyslné rušení, společně s útlumem způsobeným překážkami, jako jsou budovy a hory. Tyto útlumy a rušení budou podrobněji probrány v dalších kapitolách této práce.

Nejznámějšími součástmi GNSS jsou systémy jako GPS (Global Positioning Systems) provozovaná Spojenými státy, GLONASS vyvinutého Ruskem. Dále pak Galileo vedené Evropskou unií a Čínské BeiDou. Dodatečně jsou k dispozici i regionální systémy, např. Indický IRNSS a Japonský QZSS, pracující jen na určitém území. Tyto systémy kolektivně známé jako GNSS pracují na stejných principech a jsou vzájemně kompatibilní a interoperabilní. To umožňuje uživatelským přijímačům využívat současně signály ze všech dostupných satelitů od různých systémů, [6]–[8].

2.2 Struktura GNSS

Kosmický segment, řídící segment a uživatelský segment, tyto tři části dávají dohromady strukturu satelitních navigačních systémů, viz Obr. 1. Uživatelé mohou využívat jednoho nebo více signálů z nezávislých vesmírných segmentů jednotlivých GNSS. Struktura je pak dále podrobněji popsána v pracích [6], [9], [10]

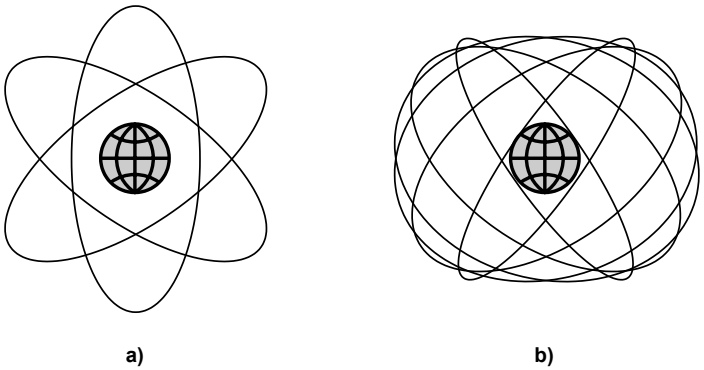


Obrázek 1: Struktura GNSS.

2.2.1 Kosmický segment

Nejprve si uvedeme složení kosmického segmentu. Ten je tvořen satelity, které obíhají zemi po oběžných drahách ve vzdálenosti přibližně 20 000 km od zemského povrchu rychlostí kolem 3800 m/s. Tyto satelity vysílají rádiové signály, o několika frekvencích, k oběma zbývajícím segmentům na povrchu země, kde jsou s jistým zpožděním zpracovány. Podle sytému, GPS, GLONASS, Galileo, BeiDou atd., tvoří satelity konstelace, kde většina v plném provozu obsahuje minimálně 24 satelitů.

Aby konstelace zajistily spolehlivý signál pro polohování, musí být jejich satelity rozmístěny na několika nerovnoběžných orbitách. Toho je docíleno nakloněním orbitálních rovin oproti rovníku o určitý úhel, viz Obr. 2. Satelity pak obíhají tyto orbity s určitou periodou. Perioda udává čas, ve kterém se satelity dostanou do stejného pozice nad povrchem Země. To, společně s počtem satelitů v konstelaci, zajišťuje, že kdekoliv na světě bude k dispozici signál nejméně ze čtyř satelitů. Všechny hodnoty jsou pro nejznámější satelitní systémy uvedeny v Tab. 1, vycházející z [6].



Obrázek 2: GPS orbity pozorované z a) pólu, b) rovníku.

U GPS se tak dostaneme k tomu, že každá orbita obsahuje minimálně 4 satelity. Ty, na rozdíl od ostatních zmíněných GNSS v Tab. 1, nejsou rozloženy rovnoměrné. To umožňuje minimalizovat

Konstelace	Úhel sklonu	Perioda	Výška nad povrchem	Orbit. roviny
GPS	55°	11h58min	20 180 km	6
GLONASS	64.8°	11h15min	19 100 km	3
Galileo	56°	14h5min	23 220 km	3
Beidou	55°	12h52min	21 440 km	3

Tabulka 1: Parametry GNSS konstelací

dopad při výpadku jednoho ze satelitů.

2.2.2 Řídící segment

Jako další je tu řídící segment, také nazývaný pozemní. Přítomnost pozemního segmentu je nezbytná k zajištění správného fungování GNSS jako celku. Ten se skládá, jak můžeme vidět na Obr. 1, ze sítě monitorovacích, jedné nebo více řídících stanic a několika stanic pro komunikaci se satelity. Ku příkladu GPS obsahuje 12 stanic pro vysílaní signálu k satelitům, 16 monitorovacích stanic a dvě řídící stanice.

Monitorovací stanice se rozprostírají po povrchu celé Země a jejich pozice je přesně známa. Celá síť má také vzájemně synchronizované hodiny, což společně s přesně známou polohou umožňuje použít měřené signály k určení dráhy družic a korekci jejich hodin. Měření vzdálenosti, získané ze satelitů jsou pak monitorovacími stanicemi odeslány do řídících k dalšímu zpracování.

Po přijetí měřených informací od monitorovacích stanic, řídící stanice vypočte nutné korekce navigačních dat pro všechny satelity. Dále rozhodne, zda je nutné uskutečnit jistý pohyb upravující rozložení satelitů na základě dané korekce. Informace o korekcích jsou pak prostřednictvím vysílacích stanic odeslány satelitům do kosmickém segmentu. Korekční, malé, pohyby satelitů slouží k zachování správné orbity satelitů. Pokud je však detekováno selhání satelitu, může dojít i k velkým pohybovým změnám. Ty zajistí orbitální výměnu nefunkčního satelitu za nový.

2.2.3 Uživatelský segment

Poslední máme uživatelský segment skládající se ze zařízení schopných přijímat signály z jednoho či více satelitních systémů. Přijímače GNSS signálů jsou součástí mnoha zařízení, jakými jsou auta, smartphony a další. Přijímače se obecně skládají z několika částí potřebných k určení polohy. Nejprve tu máme anténu, sloužící k přijetí radiového signálu od GNSS a jeho převedení na signál elektrický. Elektrické signály jsou dále demodulovány, aby poskytovaly časové reference. K demodulování se využívá hodin přijímače, což je další z částí zařízení v uživatelském segmentu. Na základě výstupu přijímače se pak určuje vzdálenost mezi anténou a dostupnými satelity pomocí procesoru vzdáleností, který k tomu využívá jistých algoritmů přijímaných pseudo náhodných sekvencí. Procesor, který také řídí funkce přijímače, zároveň dekóduje navigační data. Nakonec z měřených vzdáleností obdržíme z navigačního procesoru PVT řešení (PVT z angl. position, velocity, time) [6], [8].

2.3 Souřadné systémy

Během procesu navigace se snažíme určit polohu, orientaci a pohyb přijímačů a jim příslušných objektů. Abychom mohli stanovit polohu a pohyb daného objektu, je nutné zavést jeho specifický bod, tzv. počátek. Počátek může být libovolný vhodně zvolený bod, jednat se může o roh, těžiště nebo geometrický střed objektu. Pokud chceme popsat i úhlový pohyb a orientaci je dále nutné zavést sadu tří os, které musí být vzájemně kolmé a nesmí ležet ve stejné rovině, tj. musí být nekoplanární.

Pohyb, poloha a orientace objektu je však sama o sobě zcela bezcenná. Je zapotřebí jistého druhu reference, vzhledem ke kterému můžeme daný objekt popsat. Taková reference je opět definována pomocí počátku a os souřadného systému. Do možných počátků pak spadají střed

Země, střed solárního systému či vhodné lokální body. Jako osy následně můžeme uvažovat severní, východní a vertikální směr, osy rotace Země s vektory v rovině rovníku a další.

Počátek a osy objektu a vztažné soustavy dohromady tvoří souřadnicové rámce. Aby bylo možné jednotlivé rámce definovat, je nutná možnost vyjádření jednotlivých rámců vzhledem k rámcům jiným nebo mezi sebou. Tento jev se také nazývá jako princip relativity, kdy se fyzikální zákony zdají být stejné pro veškeré pozorovatele, tzn. že například popis polohy silnice vzhledem k vozidlu poskytuje stejnou informaci jako poloha vozidla vzhledem k silnici. Můžeme tedy říct, že pro libovolný navigační problém je k jeho popisu potřeba nejméně dvou souřadnicových rámců. A to rámec objektu jehož polohu a orientaci požadujeme a vztažný rámec, popisující známé těleso, jako je Země, vzhledem ke kterému tyto parametry určujeme [6], [7].

Nyní si zde uvedeme tři základní souřadnicové systémy, využívané při určování polohy v satelitní navigaci. Jedná se o ECI (z angl. Earth-Centered Inertial), ECEF (z angl. Earth-Centered, Earth-Fixed) a lokální souřadný systém.

2.3.1 ECI

Jedná se o souřadnicový rámec poskytující referenční systém pro sledování pohybu objektů v kosmickém prostoru vzhledem k Zemi. Toho je využíváno při měření orbitální polohy družic. V tomto rámci jsou osy pevně ukotveny v počátku umístěném ve středu Země, přičemž nereagují na její rotaci, tzn. jejich směr je fixní vzhledem k hvězdám. V běžných souřadnicových systémech ECI se rovina xy shoduje s rovinou zemského rovníku, osa x je pak trvale fixována k tzv. jarnímu bodu. Jde o bod, kde Slunce vstupuje na oblohu vzhledem k Zemi ve specifickém okamžiku v roce, kterým je jarní rovnodennost. Osa y je posunuta o 90° před osu x ve směru rotace země. A osa z je považována za normálu k rovině xy ve směru skutečného severního pólu.

Definice souřadného rámce ECI je však ovlivněna drobnou nepřesností, a to tím, že se nejedná o striktně inerciální rámec. Země totiž vlivem gravitačního působení Slunce, na své oběžné dráze podléhá změně rychlosti rotace. Tento vliv je nicméně menší než-li šum měření způsobený navigačními senzory, tudíž můžeme s rámcem ECI ve všech praktických případech zacházet jako s inerciálním rámcem [6], [7].

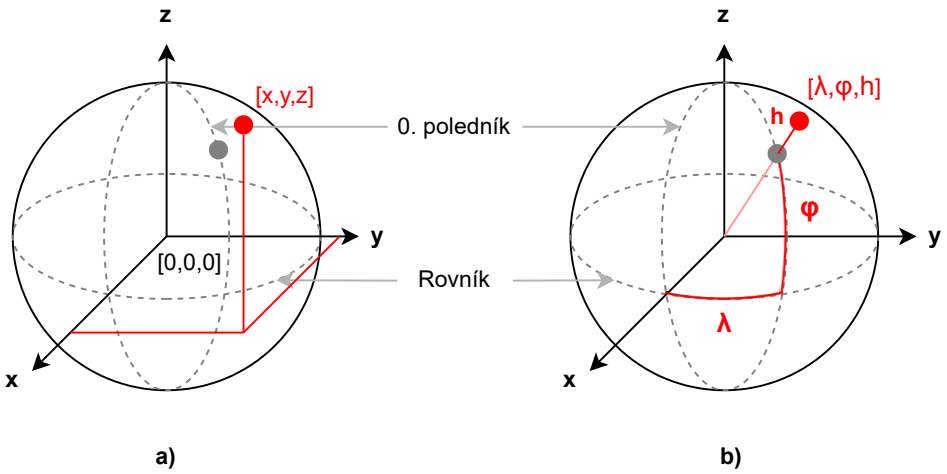
2.3.2 ECEF

Jde o rámec podobný ECI s tím rozdílem, že všechny jeho osy zůstávají pevné vůči Zemi. U obou souřadných systémů je také stejný počátek, a to ve středu Země. Osa z pak opět splývá s osou rotace Země a míří od jejího středu ke skutečnému severnímu pólu. Osa x dále prochází průsečíkem rovníku a nultého poledníku a osa y je nakonce opět kolmá k ose x, tzn. prochází průsečíkem rovníků a devadesátého poledníku na východní polokouli [6]. To můžeme vidět na Obr. 3. Rámec ECEF je univerzální standard využívaný k popisu polohy, jelikož usnadňuje matematické operace a umožňuje efektivní zpracování a analýzu dat.

Tvar Země je obecně popsán jako geoid, což je tvar, který by povrch Země měl, kdyby byl ovlivněn pouze gravitačními silami a rotací. Geoid je tedy referenční povrch pro definování nadmořské výšky a je považován za nejlepší aproximaci skutečného tvaru Země. Pro jednoduchost však v této práci uvažujeme model Země jako elipsoid, který je svázán se střední hladinou světových oceánů (MSL z angl. mean sea level).

Polohu na povrchu je pak v tomto souřadném systému možné uvést v kartézských ($x[m]$, $y[m]$, $z[m]$) či geodetických neboli sférických souřadnicích ($\lambda[rad]$, $\varphi[rad]$, $h[m]$), viz Obr. 3. Je dobré uvést, že sférické souřadnice jsou založeny na kouli, kdy tento popis polohy využívají lidé. GNSS na druhou stranu využívají ke své práci geodetické souřadnice, které vycházejí z elipsoidu. V geodetických resp. sférických souřadnicích λ označuje zeměpisnou délku, φ zeměpisnou šířku a h udávající nadmořskou výšku vzhledem k MSL.

Uvedené souřadnicové popisy jsme schopni mezi sebou převádět pomocí vztahů uvedených v práci [6]. Jelikož lidé k popisu polohy na Zemi převážně využívá sférických souřadnic, uvedeme si



Obrázek 3: Souřadný systém ECEF popsaný a) kartézskými, b) sférickými souřadnicemi.

jen jejich převod do kartézských souřadnic

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} (R_E + h)\cos\varphi\cos\lambda \\ (R_E + h)\cos\varphi\sin\lambda \\ (R_E(1-e^2) + h)\sin\varphi \end{bmatrix}, \tag{1}$$

kde R_E je poloměr zakřivení, který můžeme popsat vztahem

$$R_E = \frac{R_0}{\sqrt{1 - e^2\sin^2\varphi}}, \tag{2}$$

R_0 pak udává poloměr Země a e její excentricitu. Tyto hodnoty jsou dle modelu elipsoidu WGS84 definovány jako $R_0 = 6378137\ [m]$ a $e = 0.0818191908425$.

Převod z kartézských do geodetických souřadnic je pak obvykle prováděn pomocí procesu, který se nazývá geodetická inversní transformace. Tento proces využívá geometrických a trigonometrických vztahů a může být složitější než převod z geodetických souřadnic do kartézských souřadnic [6], [7], [10].

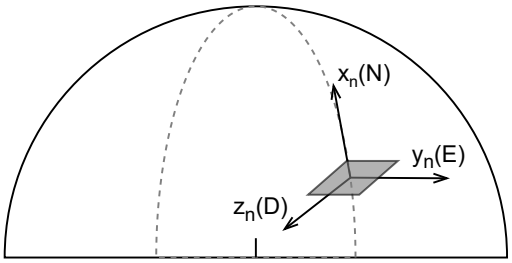
2.3.3 Lokální navigační rámec

Je takový souřadnicový systém, jehož počátek leží v těžišti objektu, jehož polohu určujeme. Osy jsou pak spjaty s topografickými směry sever, východ a vertikála. U lokálních rámců se nejčastěji uvažuje uspořádání NED (z angl. North, East, Down), tzn. osu z nebo-li vertikálu také označujeme jako osu dolů. Lze ji definovat jako normálu k povrchu referenčního elipsoidu směřující k Zemi. Dále zde pak máme osu y také známo jako východní a x jako severní. Můžeme názorně vidět na Obr. 4.

Lokální navigační rámec je důležitý v navigaci pro popis polohy uživatele vzhledem k směru na sever, východ a dolů. Využívá k tomu vhodnou sadu rozlišovacích os, ale nevyužívá se jako referenční rámec. Hlavní nevýhoda tohoto rámce spočívá v singularitě vyskytující se na každém z pólu, jelikož zde jsou severní a východní osa neurčité. Proto je použití tohoto rámce nevhodné v blízkosti pólů. Tento problém lze vyřešit využitím alternativního rámce převádějícího navigační řešení do lokálního až na konci zpracovávaného řetězce [6], [10].

2.3.4 Převodní vztahy mezi rámci

Pro převod mezi jednotlivými rámci můžeme využít tzv. transformačních (rotačních) matic $\mathbf{C}^{\alpha}_{\beta}$, kdy požadovaný parametr (poloha, rychlost, atd.) v jednom rámci $\mathbf{x}^{\beta}$ získáme násobením



Obrázek 4: Lokální navigační rámec s uspořádáním NED.

transformační matice odpovídajícím parametrem druhého rámce $\mathbf{x}^\alpha$

$$\mathbf{x}^\beta = \mathbf{C}^\alpha_\beta \mathbf{x}^\alpha, \tag{3}$$

kde α, β definují jednotlivé souřadné systémy. Při převodu mezi ECI a ECEF jsou jejich počátky a osy z těchto rámců shodné. Osy x a y se pak shodují v čase t_0 a rotují kolem osy z úhlovou rychlostí $\omega = 7.292115 \cdot 10^{-5}[rad/s]$. Na základě toho lze psát převodní matice jako [6]

$$\mathbf{C}^i_e(t) = \begin{bmatrix} \cos\omega(t-t_0) & \sin\omega(t-t_0) & 0 \\ -\sin\omega(t-t_0) & \cos\omega(t-t_0) & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \mathbf{C}^e_i(t) = \begin{bmatrix} \cos\omega(t-t_0) & -\sin\omega(t-t_0) & 0 \\ \sin\omega(t-t_0) & \cos\omega(t-t_0) & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{4}$$

Pro převod mezi ECEF a lokálním navigačním rámcem jsou pak transformační matice popsány pomocí geodetických souřadnic daného objektu následovně

$$\mathbf{C}^e_n = \begin{bmatrix} -\sin\varphi\cos\lambda & -\sin\varphi\sin\lambda & \cos\varphi \\ -\sin\lambda & \cos\lambda & 0 \\ -\cos\varphi\cos\lambda & -\cos\varphi\sin\lambda & -\sin\varphi \end{bmatrix}, \quad \mathbf{C}^n_e = \begin{bmatrix} -\sin\varphi\cos\lambda & -\sin\lambda & -\cos\varphi\cos\lambda \\ -\sin\varphi\sin\lambda & \cos\lambda & -\cos\varphi\sin\lambda \\ \cos\varphi & 0 & -\sin\varphi \end{bmatrix}. \tag{5}$$

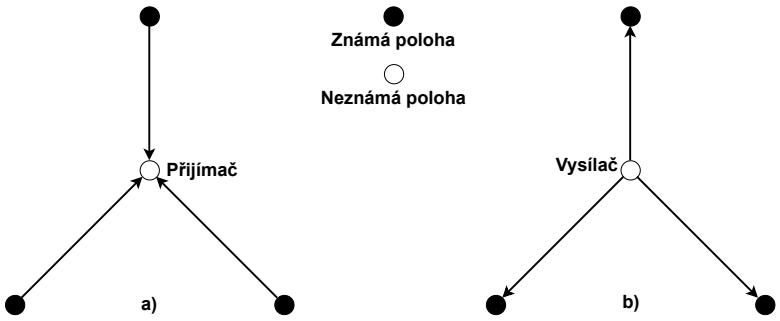
2.4 Určování polohy a času

Polohování nebo-li určování polohy je jeden z klíčových úkolů satelitní navigace, který umožňuje stanovení polohy objektu či subjektu v geografickém prostoru. Prostor je typicky určen souřadným systémem ECEF ze získaných měřených dat. Z těchto měření můžeme různými polohovacími metodami určit polohu požadovaného objektu. Tyto metody jsou uvedeny v dalších částech této kapitoly.

2.4.1 Klasifikace technik pro zpracování dat

Nyní si zde představíme způsoby, které nám udávají, jak je možné zpracovávat data měřená GNSS přijímačem. První z nich se týká časového zpracování, tzn. kdy jsou získaná měření vyhodnocena. Zpracování dat může být provedeno postprocesně (tj. off-line) nebo v reálném čase (tj. on-line). Off-line přístup běžně provádí určení polohy až po obdržení měření získaných v rozsahu několika hodin či dnů. Tento přístup však není vhodný pro navigaci, kde se vyžaduje znalost polohy v co nejkratším čase po příchodu měření, tzn. využíváme on-line vyhodnocení.

Druhý způsob se zabývá tím, kde se uskutečňuje vyhodnocení polohy, viz Obr. 5. U navigace se převážně využívá tzv. vlastního polohování, při kterém se měření zpracovávají u objektu, jehož polohu chceme určit (oblast určování polohy objektu senzory mimo objekt se nazývá sledováním/trackingem). Princip spočívá v tom, že vysílače o známe poloze předají měřené informace přijímači, který na jejich základě určí svou vlastní polohu. Na druhou stranu, zde máme vzdálené polohování, kdy se poloha neznámého objektu určuje mimo tento objekt. Zde princip spočívá ve vyslání informace neznámým objektem přijímačům, jejichž polohu známe, které pomocí hlavní



Obrázek 5: Schéma jednosměrného přenosu dat a) vlastního, b) vzdáleného polohování.

stanice vypočtou z přijatých informací polohu neznámého objektu. U vzdáleného polohování není nutně vyžadována spolupráce neznámého objektu, což je užitečné pro skryté sledování.

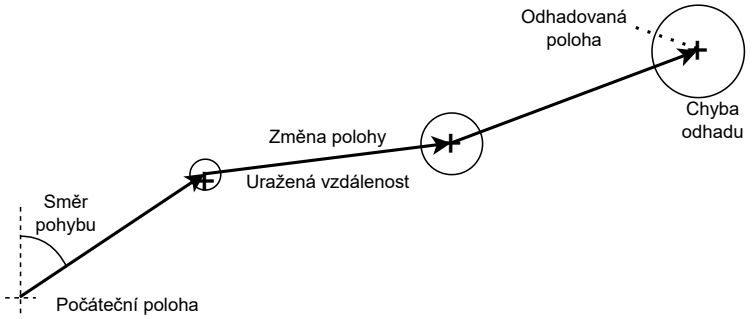
Třetí a poslední způsob závisí na pohyblivosti objektu, u nějž zjišťujeme polohu. Objekt může být jak fixní, také známé jako statické polohování, tak pohyblivý, nebo-li dynamické polohování. U pohyblivého objektu můžeme určovat krom polohy i jeho rychlost, představující další užitečnou informaci jeho chování.

Polohu je možné určovat pomocí různorodých metod. Každá z těchto metod nabízí jedinečný přístup a výhody přispívající k zdokonalování navigačních systémů. Kombinace různých metod nám umožňuje dosáhnout optimálních výsledků při navigaci v různých prostředí a podmínkách. Nyní si zde uvedeme několik vybraných metod.

2.4.2 Přehled alternativních navigačních metod

Inerciální navigace

Nejprve si uvedeme metodu, která k určení polohy využívá pouze informace měřené na daném objektu, resp. subjektu pomocí inerciální měřící jednotky IMU (z angl. Inertial Measurement Unit). To je elektronické zařízení, které měří zrychlení, úhlovou rychlost a orientaci tělesa pomocí kombinace akcelerometrů, gyroskopů a magnetometrů. Tato metoda se nazývá mrtvý odhad (angl. dead reckoning) a využívá k odhadu polohy měřený směr a vzdálenost, kterou daný objekt, resp. subjekt, urazil z předchozí polohy. Z toho vyplývá, že je zde nutná znalost počáteční polohy, rychlosti a orientace, od kterých se dále odvíjí následný odhad, viz Obr. 6. Hlavní nevýhodou



Obrázek 6: Principiální metody mrtvého odhadu.

metody mrtvého odhadu je postupná kumulace chyby v čase, jelikož se chyby v jednotlivých krocích sčítají. Na druhou stranu, inerciální navigace nespoléhá na externě vysílané signály.

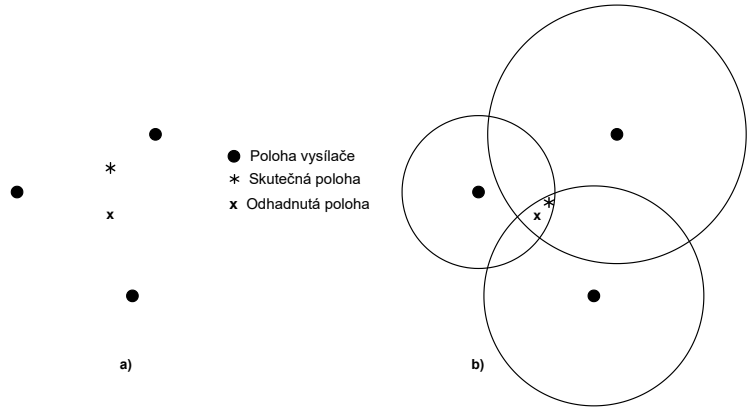
Dále si představíme metody, které k určení polohy využívají rádiový signál, které nám poskytují klíčovou informaci k exaktnímu určení geografické polohy uživatele.

Rádiová navigace

Jednou z nejjednodušších metod rádiové navigace je metoda založená na blízkosti k známým objektům/vysílačům. V její základní formě je po přijetí signálu poloha přijímače uvažována jako poloha vysílače, kdy oblast, kterou vysílaný signál pokrývá, udává nejistotu určené polohy. Není-li vysílač ve středu oblasti pokrývané signálem, například z důvodů překážek, je možné polohu uživatele uvažovat jako střed této oblasti, pokud je známý.

Pro určení polohy metoda využívá lokální signály. Jednat se muže o signály z nejrůznějších zdrojů, ať už se jedná o ty poskytovaná televizním, mobilním či WiFi vysíláním. Na základě využití těchto signálů je tato metoda schopna poskytnout přesnost v řádu jednotek až stovek metrů v závislosti na typu sítě.

Pro zvýšení přesnosti této metody je možné použít více vysílačů, kdy řešením polohy bude střed průniku jednotlivých oblastí pokrývaných vysílaným signálem, který bereme jako polohu přijímače. Toto můžeme vidět na Obr. 7. Pro jednoduchost jsme na obrázku uvedli symetrické oblasti pokrývané signálem. Ve skutečnosti tomu však tak není z důvodu výškových rozdílů, průběhů zesílení a překážek, měnící poloměr pokrytí v závislosti na směru. Je tedy zřejmé že u této metody je důležitá geometrie a síla signálu.



Obrázek 7: Určování polohy metodou blízkosti s více vysílači a) základní, b) pokročilý přístup.

Jako další si představíme úhlovou metodu, kterou lze využít k určení polohy ze rádiového signálu. Patří mezi jednu z nejstarších metod využívané v satelitní navigaci. Polohování provádí na základě měření elevačního úhlu družice nebo vysílače signálu. Elevace je úhel nad obzorem, pod kterým se satelit nachází na obloze z pozice pozorovatele na Zemi. Tento úhel měří, jak vysoko nad horizontem se satelit nachází. Místem, kde se body nacházejí s konstantní elevací k družici, je kužel s vrcholem umístěným v pozici satelitu. Provedeme-li takové měření znovu, buď po určité době ze stejného satelitu, nebo z dalšího dostupného satelitu, získáme tak další kužel. Výslednou polohu pak získáme jako průsečík jednotlivých kuželů s povrchem Země. Jedná se o méně přesnou metodu určení polohy.

Porovnávání vzorů

Poslední zmíněnou metodou je metoda porovnávání vzorů. Ta je založena na databázi vzorů, které se v závislosti na poloze mění. Mezi tyto vzory nejčastěji patři výška terénu, síla přijatého signálu z okolních lokálních vysílacích stanic, magnetické nebo gravitační pole v dané oblasti a určení signálů ovlivněných okolními budovami. Následně pak uživatel s neznámou polohou měří hodnoty těchto vzorů a porovnává je s hodnotami uloženými v databázi. V databázi jsou hodnoty vzorů uloženy v několika kandidátních mřížkách, odpovídající daným pozicím. Na základě toho

jaká kandidátní mřížka poskytuje nejlepší shodu s naměřenými hodnotami se udává výsledná poloha uživatele. Je-li výsledek několika sousedících kandidátů podobný, lze polohu určit na základě interpolace. Omezení řešení polohy spočívá ve velikosti databáze a značné nelinearitě.

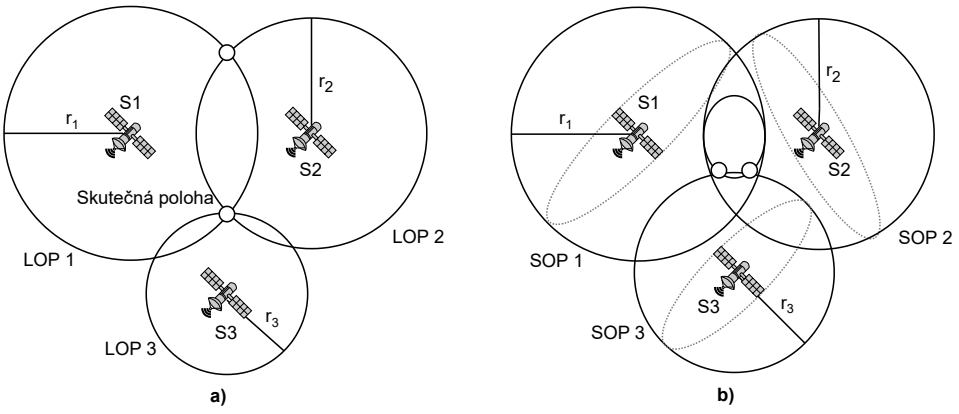
2.4.3 Vzdálenostní metoda

Jedná se o hlavní metodu určování polohy využívané v této práci. Metoda určuje polohu na základě vzdálenosti naměřené z několika rádiových signálů vysílaných satelity. V oblasti satelitní navigace se jedná o nejpoužívanější metodu určování polohy. Vzdálenosti se měří mezi přijímačem o neznámé poloze a satelitem (vysílač), jehož pozici známe. Běžně se vzdálenost neměří přímo, ale pasivně skrze dobu letu signálu (TOF z angl. Time of Flight). K přesnému měření TOF je však zapotřebí časová synchronizace hodin vysílače a přijímače. Jsou-li přijímače s neznámou polohou schopny pouze přijímat signály od satelitů se známou polohou jedná se o jednosměrné měření vzdálenosti. V takovém případě jsou synchronizovány pouze hodiny satelitů mezi sebou a offset hodin přijímače je uvažován jako další neznáma při řešení polohy. Tento postup se nazývá jako pasivní měření vzdálenosti a je podrobněji probrán dále.

Pokud bychom k určení pozice využili měření pouze od jednoho satelitu, pak přijímač může být umístěn kdekoliv na kruhu, resp. kouli (při 2D, resp. 3D polohování) se středem v anténě satelitu, viz Obr. 8. Tyto obrazce označujeme jako linii (LOP), resp. plochu (SOP) polohy, kdy zkratky vycházejí z anglického line/surface of position. Poloměr kruhu, resp. koule pak lze uvažovat jako vzdálenost mezi jednotlivými anténami.

Přidáme-li měření od dalšího satelitu, tak při 2D polohování obdržíme ještě jeden kruh. Průnikem dvojice kruhů získáme pozice, ve kterých se může uživatel vyskytovat. Jedná se však stále o nejednoznačné řešení. Jednoznačnosti můžeme dosáhnout využitím dalšího, třetího, měření nebo pomocí jisté apriorní informace, jako je například očekávaná pozice na povrchu Země či využití předchozí polohy a maximální možné uražené vzdálenosti.

Pro tří-dimenzionální přesné určení polohy je zapotřebí vždy o jedno měření vzdálenosti více než-li u 2D polohování. Jelikož při průniku dvou kulových prostorů, obdržíme celou linii polohy, na které se může uživatel vyskytovat. Oba případy jsou znázorněny na následujícím Obr. 8.



Obrázek 8: Znázornění a) 2D, b) 3D polohování pomocí vzdáleností antén.

Vzdálenost r_{su} od polohy antény satelitu, tj. $\mathbf{p}_s^e = [x_s^e, y_s^e, z_s^e]^T$, k anténě přijímače uživatele $\mathbf{p}_u^e = [x_u^e, y_u^e, z_u^e]^T$, které jsou vyjádřeny v rámci ECEF, může být popsána ve 3D vztahem

$$r_{su} = ||\mathbf{p}_s^e - \mathbf{p}_u^e|| = \sqrt{(x_s^e - x_u^e)^2 + (y_s^e - y_u^e)^2 + (z_s^e - z_u^e)^2}, \tag{6}$$

Odhad polohy uživatele pak obdržíme řešením soustavy rovnic, jednotlivých naměřených vzdáleností, ve tvaru (6). Jedná se o nelineární rovnice, k jejichž řešení je nutné využít iteračního postupu.

Existuje několik přístupů měření vzdálenosti založených na TOF. My v této práci budeme především využívat určování polohy na základě **pasivní vzdálenosti**, který si nyní rozvedeme.

U pasivní vzdálenosti měří přijímač uživatel v ideálním případě čas příchodu t^a_{GPS} i vyslání t^t_{GPS} v přesném čase konstelace GPS. Odečtením těchto časů a vynásobením rozdílu rychlostí světla $c = 299792458[m/s]$ získáme vzdálenost, viz (7), tj. teoretickou vzdálenost lze spočítat jako

$$r_{su} = (t^a_{GPS} - t^t_{GPS}) \cdot c. \tag{7}$$

Výpočet vzdálenosti uvedený vztahem (7) lze provést pouze v ideálním případě, kdy jsou hodiny satelitů a přijímače zcela synchronizovány se systémovým časem, tj. časem konstelace GPS, a nedochází k žádnému zpoždění signálu. Toho se však ve skutečnosti, prostřednictvím dostupných a kompaktních prostředků, nedá zcela dosáhnout. Neboť pohybuje-li se signál v reálném prostředí, je jeho rychlost nižší než rychlost světla a dochází tak k jeho zpoždění v rámci nanosekund, což odpovídá chybě v měření vzdálenosti v jednotkách metrů. Rovněž synchronizace vzdálených a nezávislých hodin dvou různých zařízení nebude tak příliš přesná.

V případě pasivního polohování, kde družice vysílají navigační signály, je nezbytná synchronizace hodin jednotlivých družic. Přijímač uživatele následně tyto signály pouze přijímá a zpracovává. Synchronizace hodin satelitního systému je proveditelná, a to díky přesným atomovým hodinám, umístěných na palubě satelitu a řídícímu segmentu, který vždy v určité periodě poskytuje satelitům referenční čas světových normálů v podobě korekčních dat.

Princip pasivního polohování v současnosti využívají veškeré GNSS. Aktivní polohování, kdy se vyšle signál satelitu, který jej po dané době pošle zpět a na základě toho se určí vzdálenost, se v tomto případě tolik nevyužívá.

Jedinou odlišností od vztahu (6), resp. (7), kterou tedy nyní budeme uvažovat je rozdíl času hodin přijímače uživatele od času satelitního systému. V okamžiku změření doby příchodu signálu tak získáme časový posun hodin uživatele oproti hodinám satelitním, který je daný nejen dobou letu signálu, ale i rozdílnými vlastnostmi hodin. Tento časový posun se také označuje jako offset, a aby vyjadřoval jednotku vzdálenosti lze jej zapsat takto

$$\Delta t_u = (t^a_u - t^t_{GPS}) \cdot c, \tag{8}$$

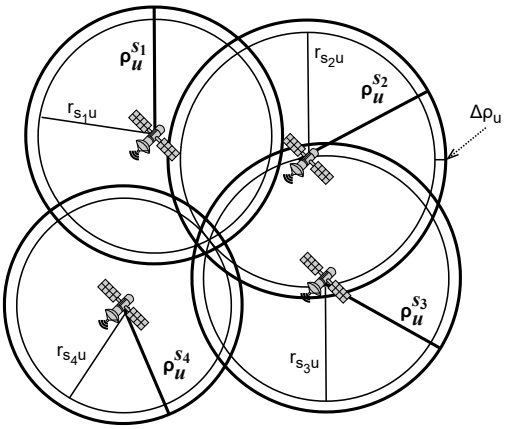
kde t^t_{GPS} je synchronizovaný čas vyslání signálu satelitním systémem GPS, t^a_u je čas přijetí signálu přijímačem uživatele zatížený chybou působící offset a c je rychlost světla. Na základě tohoto posunu (8) a rovnice vzdálenosti (6), resp. (7) jsme schopni určit pseudo-vzdálenost ρ^s_u pomocí následujícího vztahu

$$\rho^s_u = r_{su} + \Delta t_u, \tag{9}$$

kde pseudo-vzdálenost ρ^s_u od satelitu k uživateli zavádíme s cílem odlišit vzdálenost určenou s vlivem chyby hodin od pasivní vzdálenosti v ideálním případě, viz (7).

Pokud se na základě známého času vyslání signálů satelity t^t_{GPS} snažíme synchronizovat hodiny konstelace s hodinami přijímače s rozdílnou časovou základnou, offset mezi těmito časovými základnami není známý. Nicméně se jedná a posuv společný pro veškerá měření pseudo-vzdáleností provedených daným přijímačem v konkrétním čase, tudíž ho lze určit jako součást navigačního řešení zároveň s polohou uživatele. Takové řešení je čtyř-dimenzionální, kde jednou dimenzí je čas a zbylými třemi poloha. Pro získání řešení takového problému je zapotřebí obdržet měření nejméně od čtyř různých družic stejné konstelace. Pokud je poloměr kulových prostorů umístěných kolem satelitů rovný pseudo-vzdálenosti, pak běžně neexistuje bod ve kterém by došlo k protnutí všech sfér. Chybu vzdálenosti způsobenou offsetem hodin přijímače je však možné odečíst od jednotlivých pseudo-vzdáleností. To povede na získání odpovídající vzdálenosti, vytvářející nové sféry, které se již budou protínat v poloze uživatele, viz Obr. 9. Poloha a offset hodin uživatele se ve skutečnosti řeší současně.

Doposud jsme uvažovali ideální případ měření bez působení dalších chyb a šumů. Ve skutečnosti však měření podléhají i jiným chybám než jsou chyby hodin, ať už se jedná o neúmyslné chyby měření či chyby úmyslně zavedené do šířeného signálu. Měření pseudo-vzdálenosti ovlivněné dalšími chybami pak označujeme jako $\tilde{\rho}$.

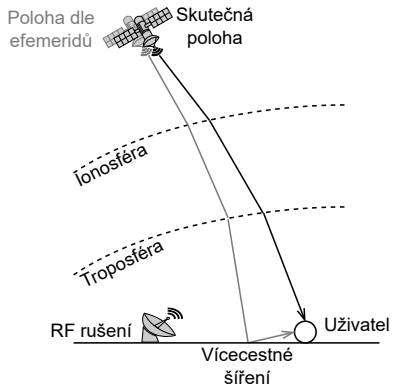


Obrázek 9: Určení polohy pseudo-vzdáleností.

2.5 Zdroje neúmyslných chyby měření

Jak již bylo zmíněno signály poskytované GNSS mají velice nízký výkon, což je zapříčiněno značnou vzdáleností kterou musí urazit od satelitu k přijímači. Slabé signály jsou pak více náchylné k různým chybám, které jsou daná průchodem různými vrstvami atmosféry. To představuje zásadní aspekt, který ovlivňuje přesnost a spolehlivost určované polohy pomocí GNSS.

Kromě již zmíněné chyby hodin způsobené převážně méně přesnými, cenově dostupnějšími, hodinami přijímače, je zde ještě několik vlivů ovlivňujících kvalitu výsledného signálu, které lze vidět na Obr. 10.



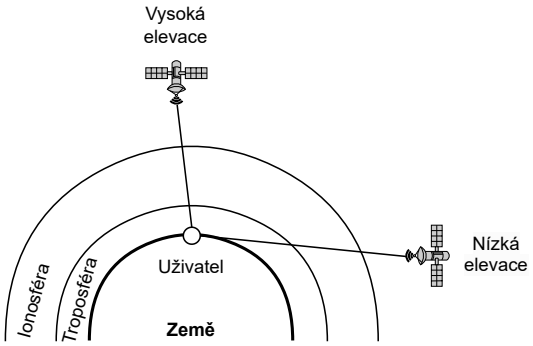
Obrázek 10: Vlivy působící na kvalitu signálu.

2.5.1 Atmosférické vlivy

Jedním z významných zdrojů chyb jsou atmosférické podmínky. Dříve jsme uvedli, že se signál síří rychlostí světla. To však neplatí pro všechny vrstvy atmosféry, ale jen pro ty nejvyšší s vlastnostmi podobnými vakuu. Ionosféra a troposféra však má větší koncentraci atmosférických plynů a rychlost je tak závislá na teplotě, tlaku, atd., u nichž může docházet v čase k rychlým i pomalým změnám.

V ionosféře se vyskytuje významné množství plynů. Prostřednictvím slunečního záření dochází k ionizaci těchto plynů, což vede vytvoření iontů a volných elektronů v ionosféře. Jejich přítomnost způsobuje změnu rychlosti šíření signálu. Jelikož je přítomnost ovlivněna slunečním zářením, bude

docházet k většímu zpoždění signálu, a tedy i chybě, během dne než v noci. Zpoždění signálu způsobené ionosférou představuje jednu z nejvýznamnějších chyb při polohovaní GNSS, která se dle [6] pohybuje na základě lokálního času (den/noc) od 1m do 15m. Chybu ionosféry je však možné částečně kompenzovat v přijímači pomocí různých modelů (např. Klobuchar pro GPS, Nequick pro Galileo). Model je schopen kompenzovat přibližně 50% chyby v závislosti na informacích vysílaných satelity.



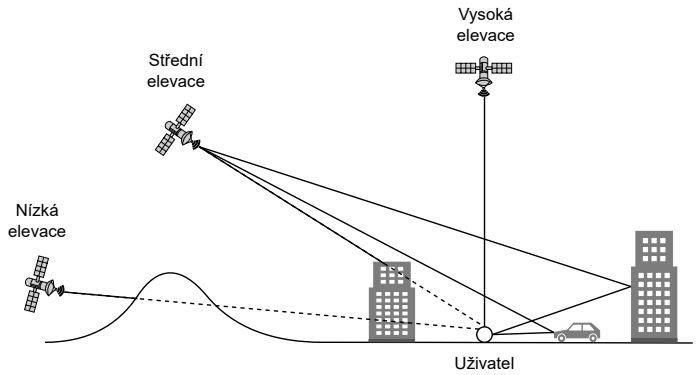
Obrázek 11: Délky šíření signálu atmosférou při nízké a vysoké elevaci satelitu.

Další vrstvou ovlivňující dobu letu signálu je troposféra. Jedná se o nejnižší vrstvu atmosféry, která je složena převážně ze suchých plynů a vodních par. Největší vliv na zpoždění signálu mají v této vrstvě suché plyny, které jsou relativně stabilní, a tak je možné je modelovat. Vodní páry pak zastávají zbylých 10% zpoždění a jsou dost odlišné. Ve výsledku je chyba způsobená troposférickým zpožděním přibližně 2.5m měnící se na základě počasí a klimatu o $\pm 10\%$. Tuto chybu jsme také schopni v jistém rozsahu kompenzovat různými modely, jako například STANAG.

Chyba způsobená atmosférickými vlivy závisí také na elevaci satelitu. Signály s nízkým elevačním úhlem mají totiž daleko větší chybu z důvodu průchodu větší částí atmosférické vrstvy než signály s vyšším úhlem, viz Obr. 11. Z toho důvodu většina přijímačů bere pro zpracování v potaz až signály přicházející nad určitým úhlem. Tento úhel se nazývá maskovací úhel a jeho velikost se běžně volí mezi 5°až 15° [7], [10], [11].

2.5.2 Chyba vícecestným šířením

Mezi další významné zdroje chyby signálu patří tzv. vícecestné šíření signálu. U GNSS signálů využívaných pozemními aplikacemi, dochází k odrazu nejčastěji na základě prostředí ve kterém se přijímač uživatele nachází. Signály se tak v tomto prostředí mohou odrážet od nejrůznějších struktur, jako jsou budovy, vozidla, země, hory či stromy. Kromě okolního prostředí nám poté

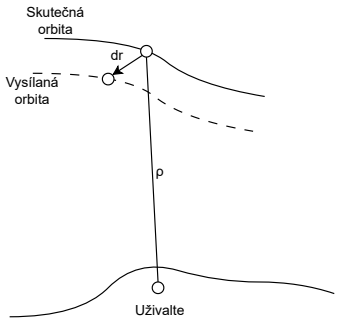


Obrázek 12: Vícecestné šíření signálu.

velikost chyby vícecestným šířením značně ovlivňuje elevace. Jak můžeme vidět na Obr. 12, u signálů poskytovaných satelity s nízkou elevací spíše dojde k jejich odrazu či blokaci, než-li u satelitů s elevací vyšší. Odražený signál je vždy opožděný oproti signálu přímému a jeho amplituda je menší. I když se chyby způsobené odražením signálu pohybují většinou v rozmezí několika metrů, pokud dojde k odrazu od vysoké vzdálené budovy, je možné se dostat i na chybu vyššího rádu. Oblasti, ve kterých k této chybě nejčastěji dochází jsou hory nebo města [6], [11].

2.5.3 Chyba efemerid

Přijímač získá polohu satelitů na základě výpočtu z informací obsažených v navigační zprávě, které se nazývají efemeridy. Ty jsou odhadovány pomocí kontrolního segmentu a posílány zpět satelitu, který jejich aktualizovanou hodnotu opět vysílá. Jelikož se však jedná o odhadované parametry na základě jisté křivky, vznikne nám zde odchylka od skutečné orbity. Tato chyba je dána pomocí vektoru, viz Obr. 13 [12], a její velikost je běžně mezi 1-6m [7], [13]. Tuto chybu je možné snížit užitím globálních nebo lokálních korekčních sítí, jsou-li k dispozici.



Obrázek 13: Chyba efemerid.

2.5.4 Chyba přijímače

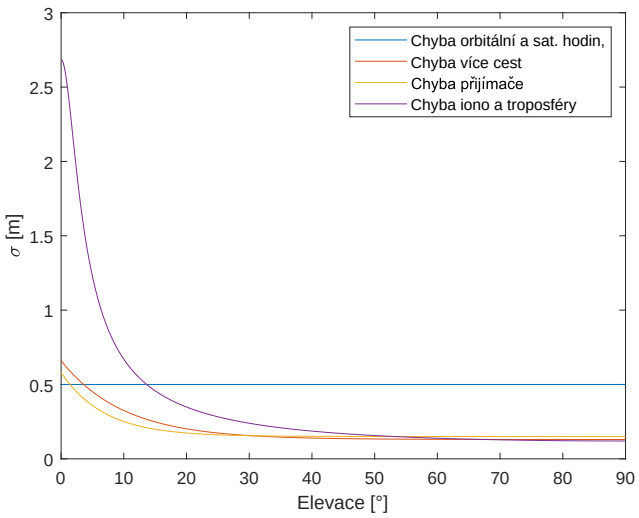
Poslední chybou kterou si zde uvedeme je chyba přijímače. Jedná se o komplexní chybu vznikající na přijímači při získávání satelitního signálu. Tato chyba zahrnuje široké spektrum šumů. Jde například o snímání zájmového pásma mikrovlnného záření nesouvisejícím se signálem. Dále sem také spadá šum způsobený součástmi systému (kabely, zesilovače, antény), a šum zavedený kvantováním. Chyba přijímače je pokládána za bílý šum, a tudíž se jí nelze zcela zbavit. Nicméně s moderními technologiemi přijímače je možné tuto chybu snížit na hodnoty centimetrů.

2.5.5 Modelování celkové chyby

Jak již bylo zmíněno, chyby je možné různými způsoby modelovat. My v této práci budeme využívat modelování směrodatné odchylky σ. Jelikož jsou některé chyb závislé na elevaci, označené jako ϵ, budou se v průběhu pohybu satelitu po své orbitě měnit. Hodnoty, které pro naše účely budeme později využívat jsme získali z práce [14] a můžeme je vidět v Tab. 2.

Chyba	σ [m]
Sat. hodin, efemerid	0.5
Vícecestného šíření	$0.13 + 0.53e^{-\frac{\epsilon}{10}}$
Přijímače	$0.15 + 0.43e^{-\frac{\epsilon}{6.9}}$
Ionosféry, Troposféry	$0.12\frac{1.001}{\sqrt{0.002001+\sin^2\epsilon}}$

Tabulka 2: Směrodatné odchylky šumů signálu GPS.



Obrázek 14: Vliv elevace na směrodatnou odchylku σ pro jednotlivé chyby.

Jednotlivé neúmyslné chyby jsou pak pro satelit popsány v měření pseudo-vzdálenosti pomocí aditivního šumu označovaného jako ν_u^s. Jedná se o šum s předpokládaným normálním rozložením, nulovou střední hodnotou a celkovou variancí, získanou součtem variancí modelů neúmyslných chyb jako

$$\sigma^2 = \sum_{i=1}^{4} \sigma_i^2, \tag{10}$$

kde i udává prvek v Tab. 2. Vycházíme-li tedy z rovnice pseudo-vzdálenosti (9), můžeme tento vztah upravit do tvaru, který uvažuje chybu jako

$$\tilde{\rho}_u^s = r_{su} + \Delta t_u + \nu_u^s. \tag{11}$$

Šum ν_u^s působící na signál od satelitu s k uživateli u je možné standardně uvažovat jako bílý nebo časově korelovaný šum.

Bílý šum je náhodný signál s rovnoměrnou výkonovou spektrální hustotou. To znamená, že má stejný výkon v jakémkoli pásmu shodné šířky. Na druhé straně, korelovaný šum je takový šum, jehož hodnoty jsou závislé na hodnotách předchozích. Každý z těchto šumů muže být způsoben jiným chybovým vlivem působícím na signál. V praxi tak v šumu ν_u^s mohou být z tohoto důvodu zastoupeny složky obou těchto šumů.

2.6 Odhad parametrů ze satelitních měření

Jelikož u systémů GNSS vycházíme ze vzdálenostní metody, můžeme na základě pseudo-vzdálenosti měřené od jednotlivých satelitů určit polohu a offset hodin přijímače. Tyto parametry jsme z měření schopni získat prostřednictvím různých metod odhadu, kde některé z nich si v této části představíme.

2.6.1 Metoda nejmenších čtverců

Jednou z nejvyužívanějších metod odhadu je metoda nejmenších čtverců (MNČ), kterou lze uplatnit v mnoha oblastech, nejen v oboru inženýrství. Jedná se o proces nalezení odhadu parametrů modelu, který nejlépe odpovídá měřeným hodnotám. Princip MNČ spočívá v minimalizaci ztrátové funkce, která je dána součtem kvadrátů rozdílů mezi měřenými a predikovanými hodnotami [15].

Uvažujme tedy pro měření model lineární regrese, který můžeme popsat vztahem

$$y_k = \varphi_k^T \Theta + v_k, \tag{12}$$

kde y_k je měřené veličina, v_k šum na ní působící, φ_k^T je známý vektor regresních proměnných dimenze n, Θ je vektor neznámých parametrů dimenze n. Pokud máme k dispozici N měření, získáme z (12) soustavu N lineárních rovnic, kterou lze zapsat v maticovém tvaru jako

$$Y = \Phi\Theta + \mathbf{e}, \tag{13}$$

kde Y je vektor obsahující N měření, $\mathbf{e}$ představuje vektor šumů dimenze N působících na měření a Φ je matice regresních proměnných dimenze $N \times n$.

Možností jak nalézt z tohoto vztahu odhad parametrů Θ, označovaný $\widehat{\Theta}$, je několik. Využijeme-li stejný počet měření N, jako je neznámých parametrů n, obdržíme jednoznačné řešení soustavy. Nicméně kvůli nedokonalosti modelu a působícím šumům je praktičtější využít větší počet měření než je neznámých parametrů ($N > n$). To nám zajistí vylepšený odhad, avšak vytvoří soustavu s často neexistujícím jednoznačným řešením. Proto je dobré zavést vektor chyb rovnice jako

$$\varepsilon = Y - \underbrace{(\Phi\Theta + \mathbf{e})}_{\widehat{Y}}, \tag{14}$$

kde Y je skutečná hodnota měření a $\widehat{Y}$ její odhad. Odhad $\widehat{\Theta}$ minimalizující kvadrát odchylek popsaný kriteriální funkcí

$$V(\Theta) = \varepsilon^T \varepsilon, , \tag{15}$$

je možné zapsat ve formě

$$\begin{aligned} \widehat{\Theta} &= \underset{\Theta}{argmin}\, V(\Theta), \\ \widehat{\Theta} &= (\Phi^T\Phi)^{-1}\Phi^T Y, \end{aligned} \tag{16}$$

za předpokladu, že matice $\Phi^T\Phi$ je pozitivně definitní. V takovém případě má ztrátová funkce (15) právě jedno minimum [6], [15].

2.6.2 Metoda vážených nejmenších čtverců

Jelikož však na většinu měření v praxi působí šumy, bílé i korelované (tzv. barevné), o různých charakteristikách, lze MNČ rozšířit na tzv metodu vážených nejmenších čtverců (VMNČ).

MNČ a VMNČ zpracovávají stejná data, avšak VMNČ zde navíc uvažuje známé vlastnosti poruchy. Každému měření je následně přiřazena váha, která odráží jeho přesnost. Tu lze definovat jako inverzi kovarianční matice měření R, tj.

$$W = R^{-1}. \tag{17}$$

Aktuálnější měření nebo měření s vyšší přesností pak mají vyšší váhu než měření starší nebo s nižší přesností.

Metoda poté hledá takový vektor parametrů Θ minimalizující součet vážených nejmenších čtverců odchylek. Ten popisuje kriteriální funkce

$$V(\Theta) = \varepsilon^T W \varepsilon \tag{18}$$

a řešen tohoto problému je dáno vztahem

$$\widehat{\Theta} = (\Phi^T W \Phi)^{-1}\Phi^T W Y. \tag{19}$$

2.6.3 Kalmanův filtr

Kalmanův filtr je mocným nástrojem pro odhad stavu dynamických systémů v prostředí s šumem. Používá se k optimalizaci odhadu stavu na základě sérií měření získaných v čase. Systém může být ovlivněn různými typy šumů a nepřesností, a Kalmanův filtr tyto faktory zohledňuje při aktualizaci odhadu. Na začátku procesu je filtr inicializován s počátečními podmínkami a znalostí o stavu systému. Během času se odhad stavu mění na základě nově získávaných měření a modelu systému, který zahrnuje informace o pravděpodobnosti šumů a nepřesností. Tímto způsobem Kalmanův filtr poskytuje robustní mechanismus pro sledování a odhad stavu systému v reálném čase, což má široké využití v mnoha oblastech jako navigace, robotika a další [16].

Uvažujme tedy pro odhad stavu diskrétní lineární stochastický systém popsaný

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \mathbf{G}\mathbf{w}_k, \\ \mathbf{z}_k &= \mathbf{H}_k\mathbf{x}_k + \mathbf{v}_k, \end{aligned} \tag{20}$$

kde $\mathbf{x}_k$ je stavový vektor neznámých proměnných (v našem případě např. časový offset a případně pozice přijímače), $\mathbf{z}_k$ je vektor měření modelu (v našem případě např. linearizované pseudo-vzdálenosti) a $\mathbf{u}_k$ je řídící vektor vstupů v kroku k, $\mathbf{A}$, $\mathbf{B}$, $\mathbf{G}$ a $\mathbf{H}$ jsou matice dynamiky, řízení, vlivu šumů a měření modelu systému. Nakonec $\mathbf{w}_k$ a $\mathbf{v}_k$ jsou zde vzájemně nezávisle gaussovské šumy s nulovou střední hodnotou a kovariančními maticemi $\mathbf{Q}_k$ a $\mathbf{R}_k$. Dále předpokládejme, že počáteční nastavení stavu modelu $\mathbf{x}_0$ má opět gaussovské rozložení se známou střední hodnotou $\overline{\mathbf{x}}_0$ a kovarianční maticí $\mathbf{P}_{x_0}$, tzn. aposteriorní odhad $\widehat{\mathbf{x}}_0 = \overline{\mathbf{x}}_0$ a jeho kovarianční matice $\mathbf{P}_0 = \mathbf{P}_{x_0}$ a Navíc nechť jsou $\mathbf{x}_0$, $\mathbf{w}_k$. $\mathbf{v}_k$ vzájemně nezávislé.

Kalmanův filtr pak provádí odhad stavu tak, aby minimalizoval váženou střední kvadratickou chybu definovanou v (18) na základě rekurzivního algoritmu. Ten se skládá z dvou hlavních částí predikce a filtrace. V predikční části se nejprve učí apriorní odhad kroku k, označovaný $\widehat{\mathbf{x}}'_k$, z aposteriorního odhadu v kroce $k-1$. Můžeme tedy psát vztahy apriorního odhadu

$$\begin{aligned} \widehat{\mathbf{x}}'_{k+1} &= \mathbf{A}\widehat{\mathbf{x}}_k + \mathbf{B}\mathbf{u}_k, \\ \mathbf{P}'_{k+1} &= \mathbf{A}\mathbf{P}_k\mathbf{A}^T + \mathbf{G}\mathbf{Q}\mathbf{G}^T. \end{aligned} \tag{21}$$

Ve filtrační části je apriorní odhad stavu prováděný na základě modelu systému upraven pomocí získaných měření v kroce k, díky čemuž je obdržen odhad aposteriorní. Vztahy pro začlenění měření do apriorního odhadu pak mají tvar

$$\begin{aligned} \mathbf{P}_{k+1} &= \left[(\mathbf{P}'_{k+1})^{-1} + \mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right]^{-1} \\ \widehat{\mathbf{x}}_{k+1} &= \widehat{\mathbf{x}}'_{k+1} + \mathbf{P}_{k+1}\mathbf{H}^T\mathbf{R}^{-1}(\mathbf{z}_{k+1} - \mathbf{H}\widehat{\mathbf{x}}'_{k+1}) \end{aligned} \tag{22}$$

Algoritmus tak nejprve provede predikci a následně korekci pomocí měřených dat. Z výše uvedených vztahů (22) vidíme, že korekce závisí na reziduích a jejich váhovém koeficientu označovaném

$$\mathbf{K}_{k+1} = \mathbf{P}_{k+1}\mathbf{H}^T\mathbf{R}^{-1}. \tag{23}$$

Kalmanův filtr představuje nejlepší lineární estimátor v případě mají-li $\mathbf{x}_0$, $\mathbf{w}_k$ a $\mathbf{v}_k$ libovolné rozložení. Pokud jsou však tyto náhodné veličiny gaussovské, pak se jedná i o optimální estimátor [6], [16], [17].

Pro naše účely budeme k odhadu času a případně polohy z měřených pseudo-vzdáleností využívat základní metodu nejmenších čtverců. Na základě této metody tak budeme schopni získat odhad offsetu hodin přijímače $\widehat{\Delta t}_u$ resp. čas hodin GPS $\widehat{t}_{GPS}$ a jeho polohu $\mathbf{p}^e_u$. Tyto odhady nám poskytují informace, které může uživatel zpracovat a využít k nejrůznějším účelům.

3 Motivace

V dnešní době, kdy se technologie stávají stále sofistikovanějšími a satelitní signály hrají klíčovou roli v mnoha aspektech našeho života, jako doprava, bankovnictví, telekomunikace a

energetika. Je důležité pochopit a řešit hrozby, které mohou ohrozit integritu a spolehlivost těchto systémů. Tato kapitola se zabývá motivací našeho výzkumu v oblasti napadení satelitních signálů a jejich detekce.

Naše motivace je dvojí. Za prvé, chceme poskytnout hlubší pochopení toho, jak mohou být satelitní signály napadeny, a jak se tyto útoky projevují v datech. To nám umožní navrhnout a implementovat efektivní detekční metody, které mohou tyto útoky identifikovat.

Za druhé, chceme přispět k širšímu pochopení tohoto problému v akademické a průmyslové komunitě. Věříme, že naše práce může inspirovat další výzkum v této oblasti a pomoci vytvořit robustnější a bezpečnější satelitní komunikační systémy pro budoucnost.

Tato kapitola poskytuje podrobný přehled o našich motivacích a cílech, a nastavuje scénu pro následující kapitoly, které se zabývají konkrétními aspekty našeho výzkumu.

Uveďme si tedy příklad, ilustrující důležitost detekce napadení v situaci, kdy se objekt nepohybuje, tzn. je statický, nebo-li fixní.

3.1 Motivační příklad

Uvažujme soustavu radarů, jejichž úkolem je sledování polohy letadla, vyskytujícího se v dané oblasti. Tyto radary určují polohu na základě vzdálenosti získané z doby letu signálu, kdy radar vyšle signál a čeká na jeho návrat. Tuto vzdálenost mezi daným radarem r a letadlem l pak, uvažujeme-li vyslání signálu letadlem zpět k radaru bez zpoždění, můžeme popsat pomocí následujícího vzorce

$$r_{rl} = \frac{(t_r^a - t_r^t) \cdot c}{2}, \tag{24}$$

kde t_r^t je čas vyslání signálu radarem, t_r^a je čas opětovného přijetí signálu radarem a c je rychlost světla. Radary jsou pak jistým způsobem rozmístěny a svým dosahem pokrývají určité území. Na základě své známe polohy a hodin jsou pak schopny dopočítat polohu letadla.

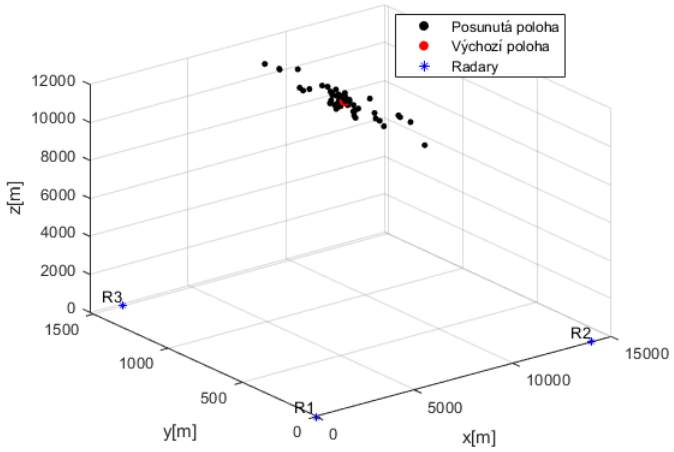
Jelikož jsou tyto radary statické, jediným možným způsobem ohrožení, bez možnosti okamžité detekce, je napadení odhadované časové základny, která může být synchronizována přes systém(y) GNSS. Změna v čase poskytovaného radaru, ovlivní jejich vysílané signály, a tím naruší jejich schopnost synchronizace a přesného určení polohy letadla.

Přesné určení polohy letadla pomocí radarů vyžaduje precizní synchronizaci času, mezi vysíláním signálů a jejich opětovným přijetím, napříč všemi radary. Pokud dochází k napadení, které působí odchylky v čase poskytovaném radarovým zařízením, může dojít k nesprávné interpretaci časových prodlev mezi dobou vyslání a opětovného přijetí signálů radary. Tato odchylka v čase může vést k nepřesným údajům o vzdálenosti, a tedy i poloze letadla. To je možné vidět na výsledku simulace znázorněné na Obr. 15. Zde máme soustavu tří radarů, což je minimální počet nutný k určení polohy ve tří-dimenzionálním prostoru. Těmto radarům je následně současně měněna doba letu signálu, což může znázorňovat napadení časové osy či časové synchronizace. Změny jsou následně propagovány do určení polohy letadla, což vede k jeho chybnému sledování v prostoru. Jaký má vliv změna času radarů na polohu letadla je vidět na Obr. 16. Poziční chyba určené polohy může dosahovat až několika set metrů při domnělém zpoždění signálu v řádu mikrosekund

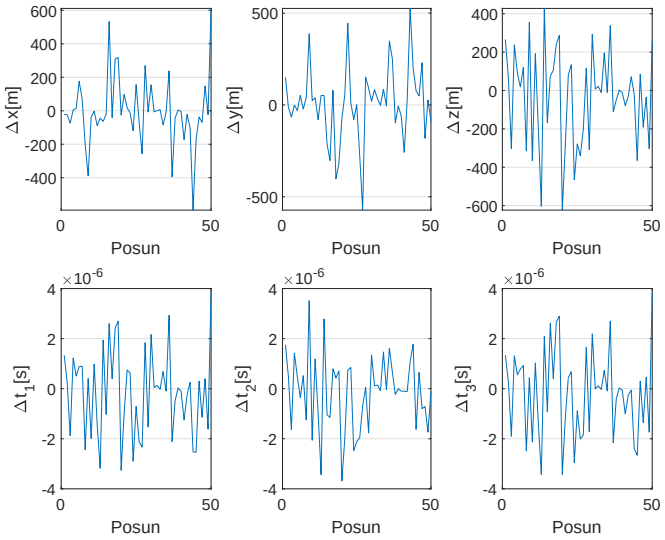
Každé radarové zařízení má určitou odchylku v měření času, která vychází z typu použitých hodin a vlivů okolního prostředí. Z tohoto důvodu je vyžadována pravidelná kalibrace, například na základě přesného času GPS. Kalibrace zahrnuje porovnání měřeného času radaru s referenčním časem GPS a případnou korekci odchylek. Bez správné kalibrace, či jejího napadení tak může docházet k chybným závěrům získaných z radarových soustav.

3.2 Cíl práce

S neustálou narůstající závislostí společnosti na satelitních systémech a rostoucí složitostí kybernetických hrozeb je nezbytné provádět neustálý výzkum. Tento výzkum probíhá jak z pohledu napadení, tak jeho detekce a může vést k vývoji nových technologií a metod pro detekci a ochranu před různými druhy útoků. Na základě těchto metod a technologií můžeme předcházet rizikům spojeným s neoprávněnou manipulací satelitních signálů.



Obrázek 15: Vliv časového napadení radarů na určení polohy letadla.



Obrázek 16: Změna polohy letadla při změně doby letu signálů od radarů.

Z toho důvodu byla představena oblast satelitní navigace s možnými způsoby záměrného rušení jejich signálů, jako jsou jamming (rušení signálu) či spoofing (falšování signálu), pro které uvedeme dosavadní techniky detekce.

Na tomto základu pak tato diplomová práce staví a snaží se přinést nové poznatky v oblasti softwarové detekce napadení GNSS signálů, s cílem rozšířit možnosti odhalování potenciálních hrozeb. Za tímto účelem budou simulovány různé scénáře spoofingu pozměňující časovou osu, které se pokusíme pomocí detekční metody AVAR odhalit.

Tato kapitola a její rovnice jsou implementovány v MATLAB® skriptu 4

4 Úmyslné rušení signálů satelitní navigace

Vzhledem k zavedené terminologii v této oblasti budeme v této práci používat v anglicky psané literatuře zavedené pojmy jamming a poofing.

Úmyslné napadení navigačních signálů v posledních letech představuje zásadní problematiku satelitní navigace, která má významný dopad na spolehlivost a bezpečnost mnoha aplikací. V této kapitole se zaměříme na představení různých typů napadení a jejich vliv na signály GNSS.

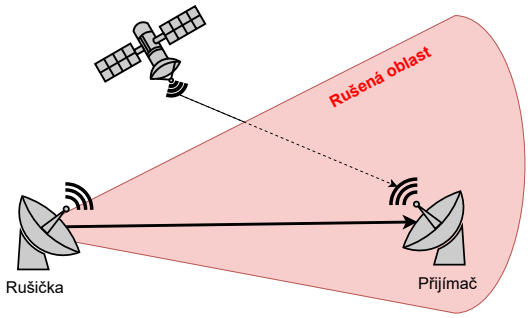
Jak již bylo dříve uvedeno přijímané GNSS signály jsou velice slabé. Z toho důvodu i útoky o malém výkonu mohou tyto signály jednoduše napodobit či podvrhnout. Navíc jelikož je popis většiny signálů GNSS systémů veřejně dostupný, jsou signály náchylnější k různým druhům napadení, jelikož útočník může imitovat strukturu systému a vysílaných signálů. Tyto útoky lze provádět v okruhu až několika kilometrů od sabotážního vysílače.

Úmyslné napadení je dle [8] možné rozdělit do dvou skupin. První se označuje jako neinformovaný útok nebo-li jamming. V tomto případě se rušení provádí bez detailní znalosti o struktuře, obsahu nebo provozu signálů GNSS. Cílem takového napadení však nemusí být způsobit veliké škody. Jako příklad zde lze uvést užití rušících zařízení, využívaných k zamezení sledování řidičů nákladních vozidel zaměstnavateli, které neúmyslně ovlivňují další systémy kolem kterých projíždí.

Druhou skupinou jsou následně informované útoky nebo-li spoofing. U těchto napadení má útočník informaci o navigačních signálech a vysílá rušivé signály s cílem způsobit škodu či dosáhnout konkrétních cílů, například podvržení signálů. Jednotlivé druhy napadení je následně možné rozdělit do dvou skupin. Tyto skupiny jsou meaconing a generativní spoofing.

4.1 Jamming (Neinformovaný útok)

Jamming, nebo-li rušení, patří mezi nejčastější typy úmyslného rušení. Jeho základní princip spočívá na vysílání signálu se stejnou nebo přibližně podobnou frekvencí, na které pracují GNSS systémy. Takový rušící signál může být generovaný jako kontinuální vlna, pulsní kontinuální vlna nebo ve formě bílého Gaussova šumu. Vyslání takového signálu způsobí že navigační signál bude překryt a přijímač nebude schopen získat jiný signál než ten ovlivněný jammingem. Cílem jammingu je tak překrývat nebo zcela blokovat přenosy GNSS signálů k přijímačům, a tak zabránit řešení pro určení polohy a času [8], [18].

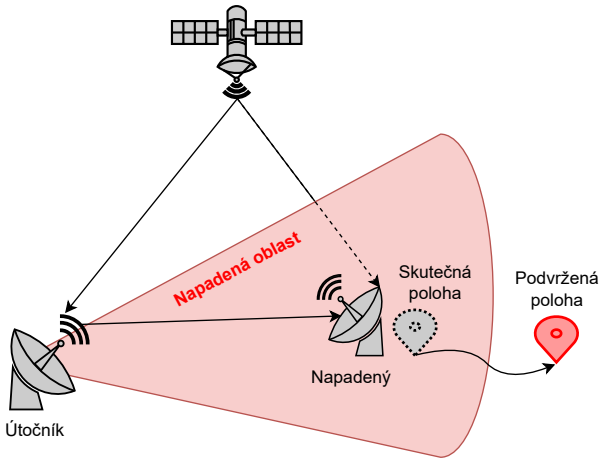


Obrázek 17: Znázornění principu jammingu přijímače.

4.2 Spoofing (Informovaný útok)

Jako druhý způsob rušení zmíníme spoofing, nebo-li podvržení. Ten se v porovnání s jammingem nevyskytuje tak často, nicméně je daleko nebezpečnější, neboť může trvat delší dobu ho odhalit. Jedná se o napadení, kdy je satelitní signál nahrazen signálem útočníka s co nejvěrnějšími vlastnostmi tak, aby byl skryt před detekcí. Spoofing je definovaný jako způsob vysílání falešných signálů s cílem oklamat přijímač [19]. Přijímače pak tyto signály vnímají jako legitimní signály

GNSS, což má za následek způsobení chyby v PVT řešení. Spoofing může být dále klasifikován do dvou skupin, meaconing a generování signálu [20].



Obrázek 18: Znázornění principu spoofingu přijímače.

4.2.1 Meaconing

Z těchto dvou možností se jedná o snadněji realizovatelný útok, jelikož jeho princip vychází z přijetí autentického signálu GNSS, který útočník zpozdí a opětovně jej vyšle k přijímači. Přijímač tak obdrží autentický signál s pozměněnou dobou letu, což bude mít za následek změnu v jeho PVT řešení [21]. Chyba vzniklá zpožděním v PVT řesení je však z hlediska útočníka obtížně kontrolovatelná. Z toho důvodu se pro moderní útoky využívá spíše generativního spoofingu.

4.2.2 Generativní spoofing

Jako další tu je generativní spoofing, který je založený na generativním modelování. Pomocí generativního modelování se vytváří a simulují autentické signály GNSS, které již obsahují falešnou informaci o PVT řešení. Tímto způsobem dokáže útočník vytvořit velmi realistické falešné signály, které jsou následně předány přijímači. To opět vede na změnu navigačního řešení přijímače, která může ovlivnit další chování objektu, na tomto řešení závislém. Generativní spoofing je pokročilá forma napadení, vyžadující pokročilé znalosti a schopnosti v oblasti signálového zpracování a umožňuje provádět útoky s vysokou účinností a obtížností detekce. Generativní spoofing lze rozdělit do tří hlavních kategorií [18], [21].

A. Asynchronní spoofing

Jak již název napovídá takovýto spoofer generuje signály, které nejsou synchronizovány s GNSS signály. Tedy spoofer nevyužívá ke generování aktuální informace poskytované pomocí GNSS. Z toho důvodu se jedná se o nejjednodušší typ spooferu, vhodný pro napadení komerčních přijímačů, který lze odhalit mnoha anti-spoofingovými technikami [18], [21].

B. Synchronní spoofing

Druhý pokročilejší druh generování vychází z příjímače GNSS signálů spojeného s vysílačem spooferu. V tomto případě nejprve dojde k synchronizaci s aktuálními signály GNSS, tzn. dostaneme požadované parametry družic. Nakonec generujeme podvržený signál, založený na znalosti směrového vektoru směřujícího od vysílače spooferu k přijímači napadeného uživatele. Jde

o složitější a obtížněji detekovatelnou variantu spooferu. Složitost realizace pak spočívá převážně v promítnutí podvrženého signálu přijímači se správným zpožděním a silou signálu pro úspěšné zmatení cíle [18], [21].

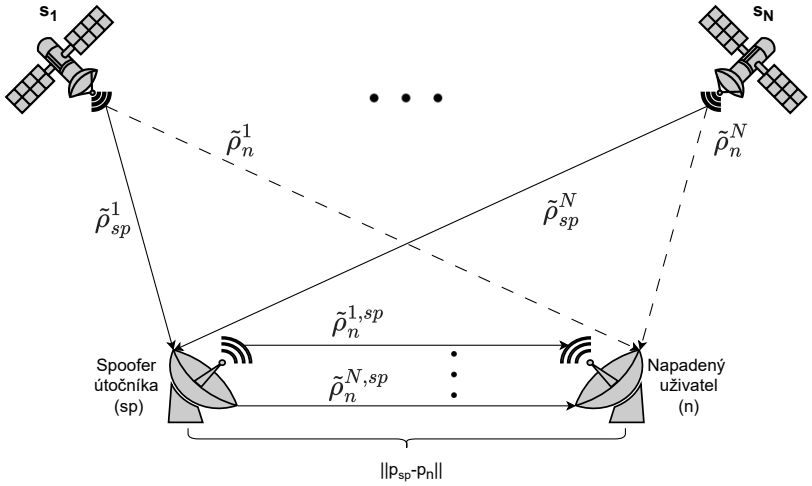
C. Spoofing se známou polohou napadeného

Poslední nejsložitější a zároveň nejúčinnější variantou je rozšíření případu B, kdy při generování předpokládáme znalost polohy napadeného přijímače s přesností v řádu centimetrů. V takovém případě je pak možné přesně synchronizovat podvržený signál s autentickým GNSS signálem na přijímači. Složitost konstrukce spooferu tohoto typu je nejvyšší ze všech zmíněných. V mnoha případech je zcela nemožná vzhledem k pohybu a geometrii cílového objektu [18], [21].

Současné metody pracující na podvržení GNSS signálu se především zaměřují na změnu informací o družicích GNSS, manipulací údajů efemerid nebo posunem času signálu GNSS na základě jeho zpoždění. Metoda manipulující s efemeridy satelitů se však dle práce [2] nejeví jako efektivní řešení, jelikož pro přenos falešných informací je potřeba minimální doba 30 sekund a zároveň jsou tyto informace v určitém časovém intervalu fixní, což vede na omezení při napadení pohyblivého přijímače. Oproti tomu provést podvrhnutí signálu prostřednictvím posunu času je podstatně jednodušší. My se v této práci budeme soustředit na systém GPS, ale pro ostatní GNSS je následující úvaha a realizace obdobná.

4.3 Generování podvrženého signálu pro systém GPS

Při generování podvrženého signálu je úkolem útočníka co nejpřesněji napodobit signál, v našem případě měřenou pseudo-vzdálenost, který by měl obdržet přijímač uživatele. Takový signál by se tedy měl co nejvíce podobat měření pseudo-vzdálenosti určené rovnicí (11). V této práci budeme uvažovat synchronní spoofing, tedy že útočník nejprve určí aktuální parametry z družic, na základě kterých pak generuje pseudo-vzdálenost, vysílanou přijímači napadeného uživatele.



Obrázek 19: Změna signálu při napadení.

Vycházejme tedy z Obr. 19 a předpokládejme daný počet satelitů N, který je pozorovatelný přijímačem napadeného uživatele i útočníka. Ten je určen výběrem všech družic v konstelaci, jejichž elevace je větší než zvolené minimální hodnota, tj. pro naše účely např. 10°. Nedochází-li k napadení, pak přijímač získává měření přímo od jednotlivých dostupných satelitů. Z rovnice (11) tak můžeme psát

$$\tilde{\rho}_n^i = ||\mathbf{p}_{s_i}^e - \mathbf{p}_n^e|| + \underbrace{(t_{GPS} - t_n) \cdot c}_{\Delta t_n} + \nu_n^i, \tag{25}$$

kde $\tilde{\rho}_u^i$ udává pseudo-vzdálenost i-tého satelitu ($i = 1, 2, .., N$) od přijímače uživatele, ν_u^i aditivní šum působící na signál od i-tého satelitu k uživateli a Δt_n offset hodin přijímače napadeného uživatele proti času GPS.

Nyní chceme-li pomocí spooferu napadnout přijímač uživatele, musíme nejprve získat data ze signálu poskytovaného spooferu pomocí GPS. Pseudo-vzdálenost, kterou přijímá spoofer, je principiálně podobná té, kterou přijímá zatím nenapadený uživatel, viz (25). Můžeme ji tedy popsat takto

$$\tilde{\rho}_{sp}^i = ||\mathbf{p}_{s_i}^e - \mathbf{p}_{sp}^e|| + \underbrace{(t_{GPS} - t_{sp}) \cdot c}_{\Delta t_{sp}} + \nu_{sp}^i, \tag{26}$$

kde $\tilde{\rho}_{sp}^i$ udává pseudo-vzdálenost i-tého satelitu od přijímače spooferu, ν_{sp}^i aditivní šum působící na signál od i-tého satelitu ke spooferu a Δt_{sp} offset hodin spooferu proti času GPS.

Obecně víme, že přijímače získají informace o satelitech prostřednictvím efemerid. Můžeme tak uvažovat, že spoofer zná polohu jednotlivých satelitů p_{s_i}, svou vlastní polohu p_{sp} a čas hodin t_{sp}. Nezná tak jen čas GPS t_{GPS}, který si však můžeme odhadnout jako součást PVT řešení, a aditivní šum ν_{sp}, který můžeme s různou přesností modelovat. Odhad času GPS útočníkem však nelze provést zcela přesně. Vznikne nám tak chyba odhadu offsetu hodin útočníka ξ definovaná následovně.

$$\begin{aligned} \xi &= \Delta t_{sp} - \widehat{\Delta t}_{sp}, \\ \xi &= (t_{GPS} - t_{sp}) \cdot c - (\widehat{t}_{GPS}^{sp} - t_{sp}) \cdot c, \\ \xi &= (t_{GPS} - \widehat{t}_{GPS}^{sp}) \cdot c. \end{aligned} \tag{27}$$

Pseudo-vzdálenost generovanou útočníkem můžeme v obecném tvaru zapsat jako

$$\tilde{\rho}_n^{i,sp} = ||\mathbf{p}_{s_i}^e - \widehat{\mathbf{p}}_n^e|| + ||\mathbf{p}_{sp}^e - \mathbf{p}_n^e|| - ||\mathbf{p}_{sp}^e - \widehat{\mathbf{p}}_n^e|| + \Delta t_n^{sp} + \widehat{\nu}_n^i, \tag{28}$$

kde $\widehat{\nu}_n^i$ je aproximativní šum generovaný útočníkem, $||\mathbf{p}_{sp}^e - \mathbf{p}_n^e||$ je skutečné zpoždění vniklé letem signálu mezi útočníkem a napadeným uživatelem. Toto zpoždění se útočník při generování signálu snaží kompenzovat, jelikož však nezná skutečnou polohu napadeného, použije nejlepší dostupný odhad, tj. $||\mathbf{p}_{sp}^e - \widehat{\mathbf{p}}_n^e||$. Nakonec zde máme offset hodin napadeného uživatele od útočníkem odhadovaného času GPS Δt_n^{sp}. Ten lze rozepsat jako

$$\Delta t_n^{sp} = (\widehat{t}_{GPS}^{sp} - t_n) \cdot c, \tag{29}$$

kdy vyjádříme-li z rovnice (27) útočníkův odhad času GPS, můžeme po dosazení a úpravách tento vztah zapsat tímto způsobem

$$\Delta t_n^{sp} = \underbrace{(t_{GPS} - t_n) \cdot c}_{\Delta t_n} - \xi, \tag{30}$$

kde ξ zde tedy udává chybu odhadu hodin t_{GPS}. Ve skutečnosti bude mít však i čas atomových hodin t_{GPS} jistou chyb. Ta bude však oproti chybě ξ výrazně menší, a tak jí pro naše účely v této práci můžeme zanedbat.

Dosazením tohoto tvaru do rovnice (28) tak obdržíme pseudo-vzdálenost obdrženou napadeným přijímačem ve formě

$$\tilde{\rho}_n^{i,sp} = ||\mathbf{p}_{s_i}^e - \widehat{\mathbf{p}}_n^e|| + ||\mathbf{p}_{sp}^e - \mathbf{p}_n^e|| - ||\mathbf{p}_{sp}^e - \widehat{\mathbf{p}}_n^e|| + \Delta t_n - \xi + \widehat{\nu}_n^i. \tag{31}$$

V této práci se zabýváme napadením stacionárních přijímačů, jejichž polohu převážně uvažujeme známou, tzn. $\widehat{\mathbf{p}}_n = \mathbf{p}_n$. Polohu je možné získat například z družicových snímků nebo dálkovým geodetickým zaměřením. Dosazením známé pozice se nám v rovnici (31) vynuluje rozdíl skutečného zpoždění mezi útočníkem a napadeným uživatelem s jeho odhadem, což vede na redukovaný tvar,

$$\tilde{\rho}_n^{i,sp} = ||\mathbf{p}_{s_i}^e - \mathbf{p}_n^e|| + \Delta t_n + \xi + \widehat{\nu}_n^i, \tag{32}$$

K takto generovanému signálu můžeme dále přidávat různými způsoby napadení γ, které následně ovlivní ovlivní odhadované řešení PVT.

$$\tilde{\rho}_n^{i,sp} = ||\mathbf{p}_{s_i}^e - \mathbf{p}_n^e|| + \Delta t_n + \xi + \widehat{\nu}_n^i + \gamma, \tag{33}$$

V našem případě, kdy uvažujeme konstantní polohu napadeného, se nám takový zásah projeví pouze v offsetu hodin. Pokud by totiž došlo k propagaci tohoto zásahu do řešení polohy, napadený by mohl porovnat toto řešení se známou polohou a okamžitě detekovat útok.

Tato kapitola a její rovnice jsou implementovány v MATLAB® skriptu 5

5 Metody detekce spoofingu

Před napadením se dá efektivně bránit jednině v případě, pokud jej zaznamenáme. Následně se můžeme pokusit obnovit skutečné ověřené informace o času a poloze, popřípadě využít alternativní poziční nebo časový algoritmus. V této sekci si představíme některé z metod používaných k detekci napadení.

Existuje několik druhů detekce, kde v praxi se pro odhalení napadení používá souběžně více z nich. Mezi základní z nich patří metoda založená na monitorování výkonu signálu. Tu je možné provádět sledováním poměru C/N_0 (angl. Carrier-to-Noise Density) nebo sledováním absolutního výkonu. Ty pracují na nízké hardwarové úrovni přijímače a sledovacích smyček.

Poměr C/N_0 se ve většině případů využívá jako parametr určení kvality signálu. Tento parametr je, za předpokladu dobré viditelnosti, ovlivňován pouze pohybem satelitů a změnami v ionosféře. Ovlivnění je hladké a postupné, pokud však útočník napadne přijímač uživatele s vyšším výkonem, lze pozorovat skokovou změnu C/N_0 a využít ji jako ukazatel napadení. Přijímač může průběžně ukládat a sledovat signál satelitů s neobvyklým chováním C/N_0, které mohou indikovat napadení.

Dalším je sledování absolutního výkonu. Útočník se snaží, co nejlépe odhadnout výkon signálu tak, aby nepřekračoval běžnou hodnotu GNSS signálu, a zároveň byl dostatečně velký k ovlivnění napadeného přijímače. To je však velice složitá úloha, jelikož dochází k výrazné změně útlumu vzniklým mezi útočníkem a napadeným. Z tohoto důvodu lze tedy tvrdit, že signál s výrazně vyšší výkonem než jsme očekávali u autentického signálu je napadený.

Tyto metody a mnohé další, ať se jedné o metodu založenou na směru, ze kterého anténa přijímače signál obdržela nebo metodu vycházející z metriky podílového kritéria pracují však převážně na hardwarové bázi, byly podrobněji studovány v pracích [18], [21], [22].

V naší diplomové práci se zaměřujeme na detekci napadení prostřednictvím softwarových nástrojů, které by mohly sloužit jako doplněk k existujícím hardwarovým detekčním metodám. Vzhledem k omezením statických přijímačů, které neumožňují využití inerciálních senzorů pro detekci změn polohy, hledáme vhodnější metodu založenou na analýze časové domény. Naším cílem je představit efektivní softwarové řešení, které by umožnilo detekci napadení bez nutnosti fyzických úprav nebo rozšíření přijímačů, což by mohlo přispět k celkově robustnější ochraně navigačních systémů.

5.1 Allanova variance

Allanova variance (AVAR), jinak také známá jako dvou vzorková variance je statistický nástroj charakterizující fluktuace signálů nebo šumů v čase. Není tedy vhodná k odhadu systematických chyb nebo nedokonalostí. Nejčastěji se využíván k měření stability frekvence hodin, oscilátorů a jejich přesnosti, čehož v této kapitole využijeme.

Uvažujeme-li odhad offsetu hodin přijímače uživatele $\widehat{\Delta tu}$, jsme schopni nepřímo odhadnout čas konstelace t_{GPS}, tj. čas generovaný atomovými hodinami satelitů, jako

$$\widehat{t}_{GPS}^u = \frac{\widehat{\Delta t}_u}{c} + t_u \tag{34}$$

kde jednotky odhad offsetu hodin $\widehat{\Delta t}_u$, jsou, dle (8), uváděny v metrech. Na základě získaného odhadu poté můžeme zkoumat vlastnosti kvality odhadu těchto atomových hodin, které jsou viděny daným přijímačem. Jsou tak zároveň ovlivněny typem přijímače, využívanou konstelací, působícími chybami, atd. Změna těchto vlastností nám poté může detekovat napadení. Vycházíme totiž z předpokladu, že útok způsobí změnu matematického modelu pseudo-vzdálenosti, což se projeví na změně vlastností hodin.

5.1.1 Zavedení AVAR

AVAR je možné popsat jako polovinu časového průměru druhých mocnin rozdílů mezi po sobě jdoucími vzorky frekvenční odchylky vzorkované během daného období. AVAR tak závisí na časové periodě daného úseku, běžně označovaného jako τ_M, kde M nám udává počet vzorků v úseku [4], [23].

Předpokládejme tedy, že jsme z postupného měření signálu obdrželi $T+1$ odhadů času konstelace $\widehat{t}^u_{GPS}$. Z takto získaných odhadů jsme následně vypočetli rozdíl po sobě jdoucích vzorků udávající drift hodin v časovém kroku k jako

$$\delta t_k = \widehat{t}^u_{GPS_{k+1}} - \widehat{t}^u_{GPS_k}, \tag{35}$$

kde $k = 1, 2, ..., T$.

Takto získaných T měření driftu δt_k se následně rozdělí do K úseků po M vzorcích. Tedy platí $K = \frac{T}{M}$ a $\tau_m = \frac{M}{f_s}$, kde f_s je vzorkovací frekvence. Pro každý úsek pak můžeme vypočíst průměr hodnot ze vzorce

$$\overline{\delta t}_k(M) = \frac{1}{M} \sum_{i=1}^{M} \delta t_{(k-1)M+i}. \tag{36}$$

Samotnou varianci, jakožto hlavní část Allanovy variance, je pak možné vypočíst podle tohoto vzorce

$$\sigma^2_A(\tau_M) = \frac{1}{2(K-1)} \sum_{k=1}^{K-1} [\overline{\delta t}_{k+1}(M) - \overline{\delta t}_k(M)]^2. \tag{37}$$

Algoritmus obsahující rovnice (36) a (37) je pak dále opakován pro různé délky úseků τ_M. Zobrazení výsledné AVAR se následně prezentuje spíše ve formě grafu, než-li samostatného čísla. Tento graf nám zobrazuje směrodatnou odchylku Allanovy variance $\sigma_A(\tau_M)$ závislou na délce periody úseku τ_M [24], [25].

Metoda AVAR se převážně využívá pro učení vlastností bílého a časově korelovaného šumu, které ovlivňují měření časových základen. Pro tyto šumy se jedná o konečnou varianci s mocninným zákonem

$$\sigma^2_A(\tau_M) = k_\sigma \tau^\mu_M, \tag{38}$$

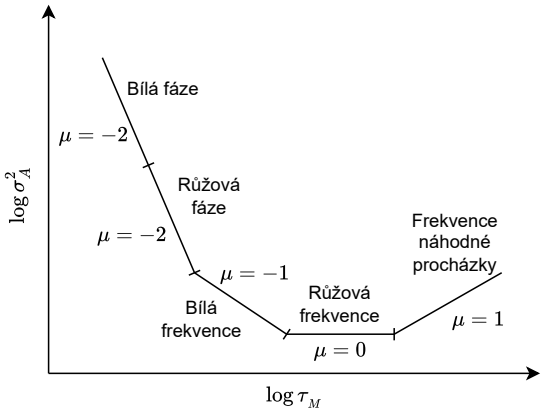
kde k_σ je konstanta. Po zlogaritmování obdržíme vztah

$$\log \sigma^2_A = \log k_\sigma + \mu \log \tau, \tag{39}$$

z čehož vyplývá, že v bilogaritmických souřadnicích je AVAR šumu s mocninným zákonem přímka. Schématické zobrazení tohoto vztahu můžeme vidět na Obr. 20. V rámci různých intervalů pozorování τ_M má Allanova variance $\sigma^2_A(\tau_M)$ různou charakteristiku, kdy každá charakteristika odpovídá jinému typu šumu vznikajícího v hodinách. Čím vyšší je tak AVAR, tím nižší je stabilita pozorovaných hodin.

Běžně se v AVAR hodin experimentálně, dle [23], pozoruje kombinace pěti typů hodinového šumu. Jedná se o bílý fázový i frekvenční šum, odpovídající Gaussovu šumu v daných oblastech, růžový fázový i frekvenční šum, odpovídající náhodnému procesu s výkonovým spektrem $1/f$, který lze často pozorovat v elektronických zařízeních a frekvenční šum náhodné procházky, který odpovídá Brownovu pohybu a lze modelovat pomocí Gauss-Markova procesu [23].

Čas systému GPS t_{GPS} je však dán atomovými hodinami, u kterých je dominantní pouze bílý frekvenční šum a frekvenční šum náhodné procházky.

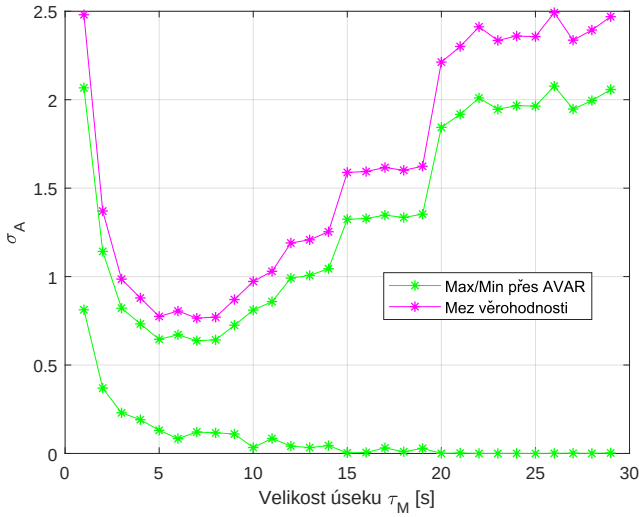


Obrázek 20: Tvar AVAR běžně pozorovaných šumů [23].

V této práci se budeme zabývat dvěma základními formami AVAR, ke zpracování odhadovaných vzorků, a to nepřekrývající a překrývající se formou. Výsledky mezi těmito formami jsou do značné míry statisticky podobné. U překrývající se formy však AVAR zpracovává více dat pro daný datový záznam o velikosti T, tudíž poskytuje odhady s menší variancí (chyby odhadu). Na druhou stranu nepřekrývající se forma AVAR je snaží analyzovat data z hlediska vzorkové statistiky, protože se vyhýbá dodatečným komplexitám korelací, které jsou nalezeny v předchozí formě [4], [23]–[25].

5.1.2 Detekce napadení pomocí AVAR

Detekce vychází z vlastností kvality odhadu atomových hodin systému GPS, kdy je na základě jejich změny schopna detekovat napadení. Vlastnosti jsou získány prostřednictvím odhadu času konstelace $\widehat{t}_{GPS}$ z měřených pseudo-vzdáleností obdržených ze satelitních signálů konkrétním přijímačem [4].

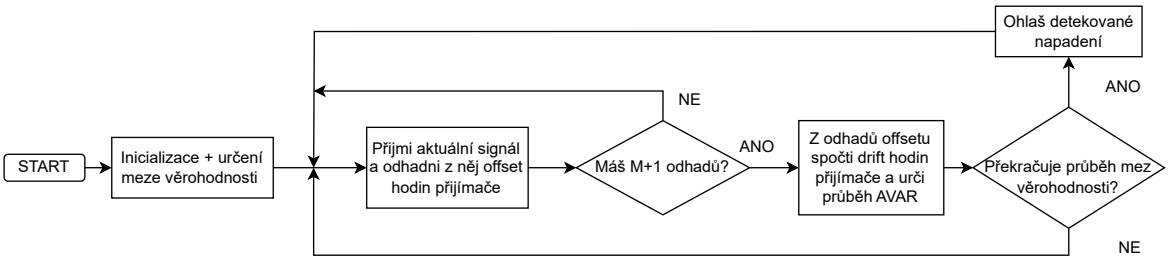


Obrázek 21: Mez věrohodnosti, získaná při autentickém signálu během jedné epochy satelitů.

Samotná metoda detekce pak nejprve provede nastavení velikosti úseku a využívané formy, se kterou bude AVAR pracovat. Následně se z odhadovaných časů $\widehat{t}_{GPS}$ vypočtou průběhy AVAR pro různé konstelace družic, buď z dostatečně přesných modelů nebo z měření v "ideálních"podmínkách, kdy s jistotou víme, že nedochází k napadení.

Tyto průběhy bereme jako referenční, kde vezmeme-li minimální a maximální hodnoty přes všechny průběhy AVAR, obdržíme výchozí meze. Jelikož však vyhodnocujeme kvalitu odhadu atomových hodin, záleží toto vyhodnocení na nejrůznějších vlivech, jako je druh přijímače, využívaná konstelace, chybové modely, atd. Při jakékoliv změně vlastností těchto vlivů tak bude nutné meze přetrénovat.

Meze vycházející z hodnot extrémů AVAR však nemusí být zcela vyhovující. Je tedy možné zavést uživatelský parametr tolerance k horní mezi, viz Obr.21. Toleranci přidáváme pouze k horní mezi, jelikož čím vyšší je hodnota AVAR, tím horší jsou vlastnosti hodin. Pokud by jsme se tedy dostali pod dolní mez, obdrželi by jsme přesnější kvalitu odhadu času t_{GPS}, což napadením pravděpodobně nedocílíme. Volba tolerančního pásma a jeho vztahu k pravděpodobnosti chybné a falešné detekce je nad rámec této práce. Pro znázornění jí tedy zvolme konstantně jako 20% maximální hodnoty. K detekci v této práci nicméně budeme využívat mez získanou pomocí extrémů AVAR.



Obrázek 22: Postup detekce napadení metodou AVAR nepřekrývající se formou.

Následně pak po uvedení přijímače do provozu přijímáme signály, které mohou nebo nemusí být napadeny. Toto napadení jsme pak schopni detekovat tak, že pro dané velikosti časových úseků opět určujeme průběhy AVAR. Pokud se tyto průběhy vyskytují pod toleranční mezí, předpokládáme že přijímáme autentický signál a k napadení nedochází. V opačném případě, kdy takový průběh toleranční mez překročí považujeme signál od tohoto časového úseku za napadený. Celkový průběh detekce je pak popsán pomocí vývojového diagramu, který můžeme vidět na Obr. 22.

Tato kapitola a její rovnice jsou implementovány v MATLAB® skriptu 6

6 Simulační model GPS a odhady z měření

V této kapitole se zaměříme na rozbor simulačního modelu nezbytného pro simulaci námi využívaného GPS satelitního systému. Pro simulaci a následný odhad polohy a času je zásadní porozumět jednotlivým aspektům ovlivňujícím chování tohoto systému.

Nejprve se zaměříme na představení simulačního modelu GPS a jeho generátorů. Budeme zkoumat modely trajektorie satelitů, generátorů měřených signálů, chyby hodin a další. Tyto modely nám umožní simulovat chování GPS signálů a jejich interakci s okolním prostředím.

Dále se budeme věnovat procesu odhadu polohy a času ze simulovaných měření, k čemuž využijeme výše představenou metodu nejmenších čtverců. Tyto odhady budou následně využity jako vstup pro detekční metodu AVAR, kterou v této práci zkoumáme. Na základě jejíž výstupů budeme provádět detekci napadení.

Cílem této kapitoly tak bude poskytnout lepší porozumění chování GPS satelitního systému prostřednictvím simulace a analyzovat odhady přijímačů.

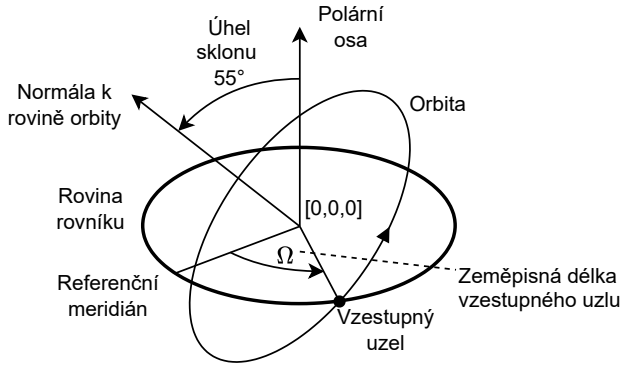
6.1 Simulace pohybu satelitů

V této kapitole vycházíme z rovnic uvedených a popisů podrobněji rozvedených v práci [6]. Z CD přiloženého k této práci jsme také bez větších úprav následně využili skript generující realistickou polohu satelitů na základě simulačního času a nastavení GPS. Z toho důvodu není tato metoda přiložena k této práci, která bude volně dostupná širší veřejnosti. Generování GPS konstelace je však níže popsáno.

Abychom vůbec mohli přistoupit k přijímání satelitního signálu, je nejdřív nutné vytvořit model, který bude simulovat pohyb družic po jednotlivých oběžných drahách. V případě kdy chceme simulovat konstelaci GPS se tak bude jednat o pohyb satelitů po 6 orbitálních rovinách, kdy první orbitální rovina je posunuta o úhel sklonu 55°, jak je uvedeno v Tab. 1. Úhel sklonu je úhel, který svírá normála k rovině oběžné dráhy s polární osou Země nebo-li naklonění vůči rovině rovníku, což je znázorněno na Obr. 23. Každá další z orbitálních rovin je následně posunuta o úhel 60° oproti předchozí. Vzestupný resp. sestupný, uzel zde popisuje bod, ve kterém se protíná oběžná dráha s rovinou rovníku v kladném, resp. záporném, směru otáčení kolem osy z v rámci ECI nebo ECEF, tj. z jihu na sever. Tyto uzly jsou běžně pevně dané v ECI rámci, avšak pro ECEF se vlivem rotace Země pohybují. Z toho důvodu je nutné zeměpisnou délku vzestupného uzlu Ω uvést v době vyslání signálu, kterou lze při zanedbání excentricity získat pomocí zjednodušeného vzorce

$$\Omega = \Omega_0 - \omega \cdot t_s^t, \tag{40}$$

kde Ω_0 udává výchozí zeměpisnou délku vzestupného uzlu orbity, ω označuje předpokládanou konstantní rychlost rotace Země, která je dle WGS84 dána $\omega = 7.292115 \cdot 10^{-5}[rad/s]$ a t_s^t je doba vyslání signálu satelitem.



Obrázek 23: Rovina primární oběžné dráhy GPS vzhledem k rovině rovníku.

Oběžné dráhy GPS se pro přesné určení polohy družic modelují pomocí Keplerova modelu, který zohledňuje excentricitu a předpokládá pohyb družic po elipse, na kterou působí gravitační síla tělesa. My pro jednoduchost budeme v našem modelu uvažovat základní kruhové oběžné dráhy.

Po těchto orbitách se následně u GPS pohybuje od 24 do 36 družic. Pro naše účely jsme k simulaci zvolili počet třiceti aktivně vysílajících satelitů. Budeme tedy uvažovat, že každá orbitální rovina bude obsahovat 5 družic. V praxi není rozmístění těchto satelitů, pro GPS systém, na orbitě rovnoměrné, z důvodu minimalizace dopadu výpadku satelitu. Pro náš základní princip fungování však postačí uvažovat jejich rozložení rovnoměrné.

Abychom byli schopni určit polohu satelitů je nutné zavést ještě pojem perigeum. Jedná se o bod na oběžné dráze, kde je satelit nejblíže Zemi. Argument perigea ψ pak udává úhel od vzestupného uzlu satelitu k jeho perigeu, měřený ve směru pohybu. V našem zjednodušeném případě je nutné podotknout, že se může jednat o libovolný bod na orbitě, čehož bylo v simulaci využito.

Polohu satelitů pak nejprve určíme v souřadnicovém systému oběžných drah, ze které ji následně transformujeme do požadovaného rámce, tj. pro naše účely ECEF. Polohu v orbitálním souřadnicovém rámci můžeme určit pomocí polárních souřadnic skládajících se z poloměru Země r_o a argument zeměpisné šířky φ, ty jsou běžně závislé na excentricitě a harmonických perturbacích a jsou dány jako

$$\begin{aligned} r_o &= 26561750\,m, \\ \varphi &= \psi + \overline{\omega}_{is} \cdot t_s^t, \end{aligned} \tag{41}$$

kde t_s^t je doba vyslání signálu satelitem a $\overline{\omega}_{is}$ je střední úhlová rychlost orbitálního pohybu družice popsaná vztahem

$$\overline{\omega}_{is} = \sqrt{\frac{\mu}{(r_o)^3}}. \tag{42}$$

$\mu = 3.986004418 \cdot 10^{14}\ [m^3/s^2]$ je dle WGS84 hodnota gravitační konstanty Země.

Polohu satelitů v orbitálním rámci lze následně z polárních souřadnic získat následujícím způsobem

$$\mathbf{p}_s^o = \begin{bmatrix} x_s^o \\ y_s^o \\ z_s^o \end{bmatrix} = \begin{bmatrix} r_o \cos\varphi \\ r_o \sin\varphi \\ 0 \end{bmatrix}. \tag{43}$$

Takto získanou polohu můžeme převést do ECEF souřadnicového rámce využitím transformační matice. Jelikož mají rámce stejné počátky, můžeme psát převod ve tvaru

$$\mathbf{p}_s^e = \mathbf{C}_e^o \mathbf{p}_s^o, \tag{44}$$

kde $\mathbf{C}_e^o$ je transformační matice z orbitálního souřadného rámce do rámce ECEF definovaná takto

$$\mathbf{C}_e^o = \begin{bmatrix} \cos\Omega & -\cos 55^\circ \sin\Omega & \sin 55^\circ \\ \sin\Omega & \cos 55^\circ \cos\Omega & -\sin 55^\circ \cos\Omega \\ 0 & \sin 55^\circ & \cos 55^\circ \end{bmatrix}. \tag{45}$$

Na základě rovnic (43), (44) a (45) pak můžeme psát polohu satelitu v souřadnicovém rámci ECEF jako

$$\mathbf{p}_s^e = \begin{bmatrix} x_s^e \\ y_s^e \\ z_s^e \end{bmatrix} = \begin{bmatrix} x_s^o \cos\Omega - y_s^o \cos 55^\circ \sin\Omega \\ x_s^o \sin\Omega - y_s^o \cos 55^\circ \cos\Omega \\ y_s^o \sin 55^\circ \end{bmatrix} \tag{46}$$

Pro naše účely si vystačíme pouze s polohou satelitů. Pokud bychom potřebovali využít i jejich rychlost, je možné ji získat pomocí derivace takto získané polohy.

Z výše uvedených vztahů je patrné, že poloha satelitů se bude v čase měnit. Pro znázornění si tak uvedeme jen simulaci jejich výchozí polohy. Na Obr. 24 můžeme vidět tuto výchozí polohu družic, rovnoměrné rozmístěních po jednotlivých kruhových oběžných drahách.

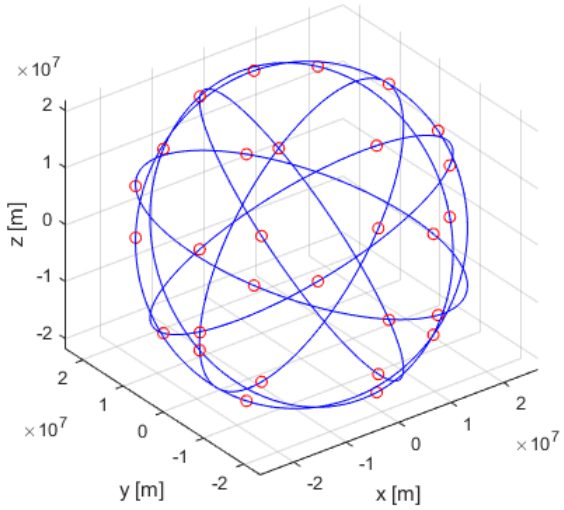
Každý satelit pak na bázi své polohy generuje měření, které vysílá k povrchu planety. V tomto měření satelit zároveň předává informaci o jeho čase vyslání, který získá z atomovými hodinami. Model, pomocí kterého čas získáme je poté rozebrán v další kapitole.

6.2 Generátor chyby hodin

Abychom byli schopni správně modelovat generátor měřených pseudo-vzdáleností, které obdrží přijímač od satelitu. Potřebujeme nejprve získat rozdíl hodin GPS konstelace a přijímače, tzn. jejich offset definovaný dle rovnice (8). Bylo by možné simulovat hodiny jednotlivých zařízení a vzápětí provézt jejich rozdíl. V praxi se však většinou využívá možnosti modelovat přímo časový offset hodin daného přijímače Δt_r.

K modelování offsetu hodin je možné využít autoregresní (AR) stavový model, který se obvykle využívá pro analýzu časových řad a predikci budoucích hodnot na základě historických dat. Základní forma AR stavového modelu je

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{w}_k, \tag{47}$$



Obrázek 24: Simulace výchozí polohy jednotlivých satelitů na oběžných drahách.

kde $\mathbf{x}_k$ je vektor stavů, $\mathbf{w}_k$ je vektor náhodných šumů s normálním rozložením v čase k a $\mathbf{A}$ matice parametrů modelu.

Vektor stavů našeho modelu tak bude obsahovat dva stavy offset hodin přijímače Δt_r a jejich drift δt_r

$$\mathbf{x}_k = \begin{bmatrix} \Delta t_{r_k} \\ \delta t_{r_k} \end{bmatrix}. \tag{48}$$

Dále máme matice parametrů modelu, jejíž parametry jsou dány závislostí aktuálních časových okamžiků stavu na minulých jako

$$\mathbf{A} = \begin{bmatrix} 1 & \tau_s \\ 0 & 1 \end{bmatrix}, \tag{49}$$

kde τ_s je vzorkovací perioda, pro nás o velikosti 1 s, který zároveň odpovídá i periodě získávání signálu přijímačem.

Vektor náhodných šumů $\mathbf{w}$ nakonec uvažujeme s nulovou střední hodnotou a kovarianční maticí popsanou dle [6] ve tvaru

$$\mathbf{Q}_{GNSS} = \begin{bmatrix} S^r_{cp}\tau_s + \frac{1}{3}S^r_{cf}\tau_s^3 & \frac{1}{2}S^r_{cf}\tau_s^2 \\ \frac{1}{2}S^r_{cf}\tau_s^2 & S^r_{cf}\tau_s \end{bmatrix}, \tag{50}$$

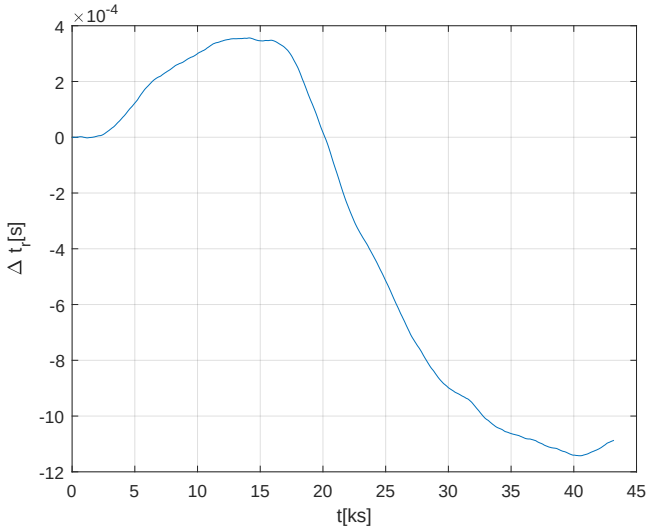
kde S^r_{cf} je drift frekvence hodin přijímače a S^r_{cp} je drift fáze hodin přijímače. Jejich běžná hodnota využívající se pro teplotně kompenzované hodiny je pak dle [6], [26] $S^r_{cf} = 0.04\ m^2/s^3$ a $S^r_{cp} = 0.01\ m^2/s^1$. Pro malé τ_s je dále možné tento vztah aproximovat do zjednodušeného tvaru

$$\mathbf{Q}_{GNSS} = \begin{bmatrix} S^r_{cp}\tau_s & 0 \\ 0 & S^r_{cf}\tau_s \end{bmatrix}. \tag{51}$$

Na Obr. 25 můžeme vidět průběh offsetu hodin přijímače na daném simulačním intervalu, získaný prostřednictvím odvozeného modelu.

Takováto chyba hodin, tedy offset, nicméně vzniká i u atomových hodin satelitů. Atomové hodiny satelitů však mají o mnoho řádů vyšší přesnost a stabilitu nežli hodiny přijímače, pro které se typicky využívá krystalového generátoru hodin. Z toho důvodu jsme v této práci chybu atomových hodin neuvažovali.

Tato kapitola a její rovnice jsou implementovány v MATLAB® skriptu 8



Obrázek 25: Průběh offsetu hodin přijímače.

6.3 Generátor satelitních měření

Nakonec se dostáváme k neméně důležitému generátoru satelitních měření. Pro naše účely postačí, když takové měření bude obsahovat polohu a pseudo-vzdálenost od jednotlivých satelitů.

Přijímače následně získávají tyto informace v daném časovém okamžiku, od každého satelitu, jehož elevační úhel je větší nebo roven maskovacímu úhlu 10°. Tento úhel je také možné definovat z tzv. vektoru viditelnosti. Jedná se o jednotkový vektor, který popisuje směr, ze kterého signál přichází k anténě uživateli u od satelitu s. Tento vektor je v rámci ECEF pomocí rovnice (6) definován jako

$$\mathbf{u}_{us}^{e} = \frac{\mathbf{p}_{s}^{e} - \mathbf{p}_{a}^{e}}{||\mathbf{p}_{s}^{e} - \mathbf{p}_{a}^{e}||} = \frac{\mathbf{p}_{s}^{e} - \mathbf{p}_{a}^{e}}{r_{as}^{e}}. \tag{52}$$

Elevační úhel mezi anténou uživatele a satelitu pak získáme ze vztahu

$$\varphi_{us}^{n} = -\arcsin(\mathbf{C}_{n}^{e}(3,:) \cdot \mathbf{u}_{as}^{e}), \tag{53}$$

kde $\mathbf{C}_{n}^{e}(3,:) \cdot \mathbf{u}_{us}^{e}$ je transformace vektoru viditelnosti (52) na složku dolů (D) rámce NED pomocí transformační matice definované vztahem (5) [6].

Získali jsme tak elevační úhel v radiánech. Převedeme-li ho na stejné jednotky s maskovacím úhlem, můžeme tyto úhly porovnat a simulovat viditelnost jednotlivých družic pro konkrétní anténu uživatele.

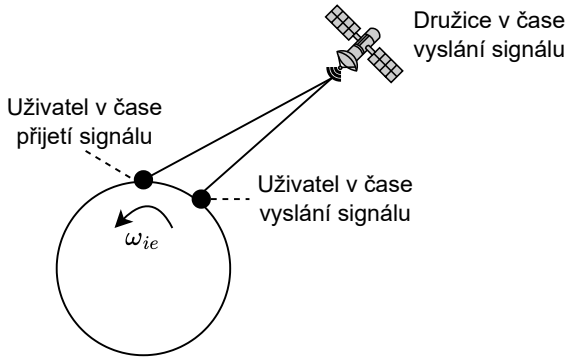
Určili jsme tedy, které satelity budou poskytovat měření a informace o své poloze přijímači. Nyní si uvedeme, jak je měření pseudo-vzdálenosti získáno. Jak již bylo podrobněji rozvedeno v kapitolách 2.4.3 a 2.5 tuto pseudo-vzdálenost jsme schopni popsat pomocí rovnice (11).

Nicméně tento vztah neuvažuje rotaci Země během doby letu signálu od satelitu k uživateli, což způsobuje chybu v určení vzdálenosti, jak můžeme vidět na Obr. 26. Tato chyba v některých místech planety může dosahovat až 41m [6]. Tuto chybu je nutné kompenzovat, čehož lze dosáhnout spřažením os ECEF a ECI rámce v čase vyslání nebo přijetí signálu. Z rovnic (3) a (4) platí

$$\mathbf{p}_{u}^{i}(t_{u}^{a}) = \mathbf{p}_{u}^{e}(t_{u}^{a}), \qquad \mathbf{p}_{s}^{i}(t_{s}^{t}) = \mathbf{C}_{i}^{e}(t_{s}^{t})\mathbf{p}_{s}^{e}(t_{s}^{t}). \tag{54}$$

Transformační matice $\mathbf{C}_{i}^{e}(t_{s}^{t})$ pro rotaci Země během doby letu signálu může být aproximována jako

$$\mathbf{C}_{i}^{e}(t_{s}^{t}) = \begin{bmatrix} 1 & \omega_{ie}(t_{u}^{a} - t_{s}^{t}) & 0 \\ -\omega_{ie}(t_{u}^{a} - t_{s}^{t}) & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \omega_{ie} r_{su}/c & 0 \\ -\omega_{ie} r_{su}/c & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{55}$$



Obrázek 26: Změna vzdálenosti stacionárního uživatele od satelitu vlivem rotace Země.

kde r_{su} je pasivní vzdálenost definovaná vztahem (7). Kompenzovanou vzdálenost nyní můžeme psát takto

$$r'_{su} = ||\mathbf{C}_i^e(t_s^t)\mathbf{p}_s^e(t_s^t) - \mathbf{p}_u^e(t_u^a)||. \tag{56}$$

V případě těchto rovnic jsme vycházeli ze vztahů uvedených v práci [6].

Na základě kompenzované vzdálenosti poté můžeme psát upravenou pseudo-vzdálenost, kterou obdrží přijímač uživatele ve tvaru

$$\tilde{\rho}_u^s = r'_{su} + \Delta t_u + \nu_u^s, \tag{57}$$

kde šum ν_u^s působící na signál od satelitu s k uživateli u je možné v simulaci volit mezi bílým šumem a časově korelovaným Gauss-Markovským (GM) procesem. V obou případech se jedná o šum s normálním rozložením, nulovou střední hodnotou a celkovou variancí, získanou součtem variancí modelů neúmyslných chyb (10), popsaných v Tab. 2, které udávaly chybu v závislosti na elevaci.

6.3.1 Bílý šum

V případě bílého šumu se jedná o náhodný proces s konstantní rovnoměrně rozloženou spektrální hustotou, jehož hodnoty jsou vzájemně nekorelované a mají konstantní rozptyl. Pro naše využití jsme pro bílý šum zvolili rozptyl daný výše uvedenou celkovou variancí, viz (10), a nulovou střední hodnotou.

Bílý šum se často vyskytuje v měřeních a signálech v důsledku různých zdrojů, jako jsou elektronické šumy, termální šumy a další. Jedním z příkladů, kde se bílý šum používá v kontextu satelitní navigace, je v systémech GPS, jelikož se jedná o jeden z hlavních typů šumu, které ovlivňuje přesnost jeho měření. Při modelování systémů GPS se tak často předpokládají chyby jako bílý šum.

Ačkoliv může být bílý šum v satelitních signálech rušivý, je také nezbytný pro správné fungování mnoha navigačních systémů, jelikož nám pomáhá lépe porozumět a modelovat chyby v navigačních datech. Z tohoto důvodu je klíčový pro návrh a kalibraci navigačních systémů.

6.3.2 Korelovaný šum

Při využití GM procesu se jedná o náhodný proces, který má vzájemně korelované hodnoty s normálním rozložením. Tento šum je možné zavést pomocí AR modelu, popisujícího vztah mezi aktuální hodnotou šumu a jeho předchozími hodnotami. Ze základní formy uvedené v rovnici (47) můžeme tedy psát

$$\chi_{k+1} = \beta_D \chi_k + \zeta_k, \tag{58}$$

kde χ_k je hodnota korelovaného šumu v čase k, ζ_k je řídící šum s nulovou střední hodnotou a β_D konstantní koeficient autoregrese, určující vliv minulých hodnot šumu na jeho současnou hodnotu,

vyplývající z diskretizace spojitého procesu

$$\beta_D = \exp\left(-\frac{1}{\tau \cdot \tau_s}\right). \tag{59}$$

Parametr τ je časová konstanta a τ_s je perioda vzorkování, nebo-li perioda aktualizace GPS, kdy dochází k získání dat z družic.

V případě GM procesu (58) jsme pak varianci Q, řídícího šumu ζ schopni vyjádřit ze vztahu pro hodnotu ustálené variance tohoto procesu definované jako

$$P = \beta_D^2 \cdot P + Q, \tag{60}$$

tímto způsobem

$$Q = (1 - \beta_D^2) \cdot P, \tag{61}$$

kdy P představuje požadovanou varianci GM procesu.

Celkovou varianci, získanou z (10), jsme posléze v tomto procesu rovnoměrně rozdělili mezi bílý a korelovaný šum (60), abychom docílili přesnějšího modelu.

Sestrojením všech modelů a generátorů jsme získali kompletní model simulující GPS konstelaci, která vysílá signály obsahující danou informaci. Tyto signály jsou následně zpracovávány prostřednictvím přijímačů. Přijímače jsou poté, na základě pseudo-vzdálenosti obdržené ze satelitů, schopny odhadovat nejrůznější informace, ať už se jedná o polohu přijímače uživatele či čas GPS systému. Pro odhady těchto parametrů se dá využít nejrůznějších metod, kdy pro naše účely využijeme metodu odhadu založenou na nejmenších čtvercích.

Tato kapitola a její rovnice jsou implementovány v MATLAB® skriptu 7

6.4 Odhad parametrů metodou nejmenších čtverců

Pokud jde o situaci uvažovanou v této práci, budeme na základě měřených pseudo-vzdáleností získaných ze signálu konstelace odhadovat především offset hodin daného přijímače. Kromě offsetu hodin mohou však odhadované parametry dále obsahovat polohu statického přijímače a to v situaci, že nebyla přijímači poskytnuta předem z přesnějších zdrojů, například dálkovým geodetickým zaměřením.

6.4.1 Odhad při neznámé poloze

Pro znázornění tedy uvažujme rozšířenou možnost s odhadem parametru polohy, potom má vektor měření a odhadovaných parametrů tvar

$$Y = \begin{bmatrix} \tilde{\rho}_u^1 \\ \tilde{\rho}_u^2 \\ \vdots \\ \tilde{\rho}_u^N \end{bmatrix}, \qquad \Theta = \begin{bmatrix} \Delta t_u \\ x_u^e \\ y_u^e \\ z_u^e \end{bmatrix}. \tag{62}$$

Pro takto definovaný model jsme k odhadu parametrů posléze využili iterativní MNČ. Ta pomocí předchozích odhadu a získaných měření opakovaně aktualizuje odhad parametrů modelu $\widehat{\Theta}$, dokud není dosaženo určitého kritéria konvergence. Takové kritérium poté indikuje, že bylo dosaženo dostatečně přesného odhadu.

Pro iterativní MNČ je ze všeho nejdřív nutné inicializovat počáteční odhad. Pro jednoduchost jsme ho zvolili jako nulový vektor, tj. $\Theta_0 = [0, 0, 0, 0]^T$.

Na základě aktuálních odhadů offsetu hodin a polohy uživatele jsme schopni sestavit matici regresních proměnných, kterou lze získat prostřednictvím parciálních derivací modelovaných měření,

definovaných v (13), podle neznámých parametrů jako

$$\Phi_k = \begin{bmatrix} \frac{\partial \rho_u^1}{\partial \Delta t_u} & \frac{\partial \rho_u^1}{\partial x_u^e} & \frac{\partial \rho_u^1}{\partial y_u^e} & \frac{\partial \rho_u^1}{\partial z_u^e} \\ \frac{\partial \rho_u^2}{\partial \Delta t_u} & \frac{\partial \rho_u^2}{\partial x_u^e} & \frac{\partial \rho_u^2}{\partial y_u^e} & \frac{\partial \rho_u^2}{\partial z_u^e} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial \rho_u^N}{\partial \Delta t_u} & \frac{\partial \rho_u^N}{\partial x_u^e} & \frac{\partial \rho_u^N}{\partial y_u^e} & \frac{\partial \rho_u^N}{\partial z_u^e} \end{bmatrix} = \begin{bmatrix} 1 & \mathbf{u}_{u1,x}^e & \mathbf{u}_{u1,y}^e & \mathbf{u}_{u1,z}^e \\ 1 & \mathbf{u}_{u2,x}^e & \mathbf{u}_{u2,y}^e & \mathbf{u}_{u2,z}^e \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \mathbf{u}_{uN,x}^e & \mathbf{u}_{uN,y}^e & \mathbf{u}_{uN,z}^e \end{bmatrix}, \tag{63}$$

kde jsme jednotkový vektor viditelnosti získali z rovnice (52) díky aktuálnímu odhadu polohy uživatele a polohy jednotlivých satelitů, jenž byla součástí satelitní zprávy [6].

Jelikož není ve většině reálných úloh možné získat měření s dokonalou přesností, z důvodů šumů či chyb měření. Můžeme k odhadu v takových případech využít místo měřených hodnot chyba odhadu, také označovanou jako residuum, které lze zapsat pomocí vztahu

$$\tilde{Y} = Y - \Phi_k \widehat{\Theta}_k. \tag{64}$$

Tento přístup umožňuje zohlednit chyby měření a zajistit tak spolehlivý odhad parametrů modelu. S využitím reziduí a struktury modelu tak můžeme psát rovnici pro aktualizaci odhadu, vycházející z (19) jako

$$\tilde{\Theta}_{k+1} = \tilde{\Theta}_k + (\Phi_k^T \Phi_k)^{-1} \Phi_k^T \underbrace{(Y - \Phi_k \Theta_k)}_{\tilde{Y}}, \tag{65}$$

která upravuje odhad a parametry modelu tak, aby minimalizovala kvadráty reziduí.

Iterační postup je opakován do chvíle, kdy dojde k splnění konvergenčního kritéria, které jsme zvolili jako

$$||\widehat{\Theta}_{k+1} - \widehat{\Theta}_k|| < 10^{-3}. \tag{66}$$

Toto kritérium nám říká, že změna odhadovaných parametrů modelu mezi dvěma po sobě jdoucími iteracemi je menší než zvolená hodnota. To znamená, že optimalizační proces již nevede k významné změně parametrů modelu, a tedy lze předpokládat, že algoritmus dosáhl dostatečné konvergence.

Odhad polohy a offsetu hodin přijímače uživatele získaný ze simulovaného modelu GPS je možné vidět na Obr. 27, kde vidíme jejich porovnání se skutečnými hodnotami. Tyto grafy je možné vykreslit jen při simulaci, tedy když známe skutečnost, jelikož pouze pak můžeme vykreslit chybu odhadu.

6.4.2 Odhad při známé poloze

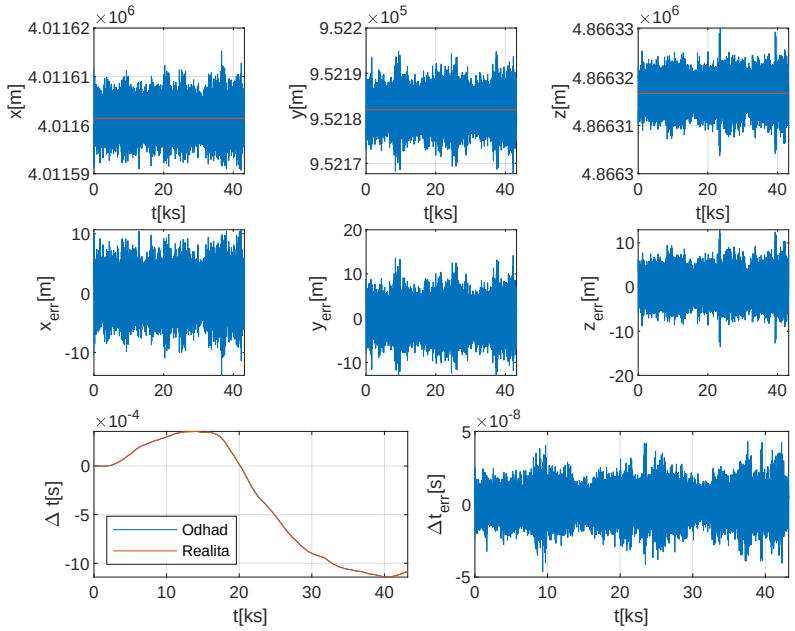
Pokud však uvažujeme možnost, že je přijímači uživatele poskytnuta jeho poloha, za pomoci přesnějšího zaměření. Není nutné polohu odhadovat a z odhadovaných parametrů modelu nám zbude pouze offset hodin. Odhad offsetu je možné extrahovat ze získaných pseudo-vzdáleností (57) na základě známých poloh uživatele a satelitů s pomocí (56) tímto způsobem

$$Y = \begin{bmatrix} \Delta t_u^1 \\ \Delta t_u^2 \\ \vdots \\ \Delta t_u^N \end{bmatrix} = \begin{bmatrix} \tilde{\rho}_u^1 - r'_{1u} \\ \tilde{\rho}_u^2 - r'_{2u} \\ \vdots \\ \tilde{\rho}_u^N - r'_{Nu} \end{bmatrix}. \tag{67}$$

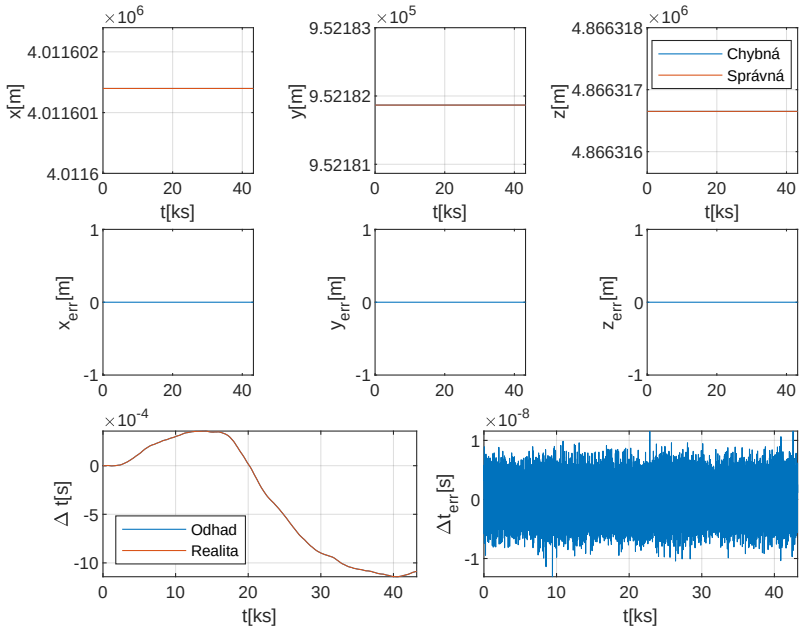
Matice regresních proměnných uvedená v (63) se nám tedy redukuje na vektor samých jedniček. Z toho vyplývá, že odhad offsetu hodin maticově definovaný v (19) se nám redukuje na skalární formu odhadu vycházející z (12), kdy tato forma ve výsledku odpovídá pouze aritmetickému průměru

$$\widehat{\Delta t_u} = \frac{1}{N} \sum_{i=1}^{N} \Delta t_u^i. \tag{68}$$

Odhad offsetu hodin uživatele vycházející z jeho známé předem dané polohy je zobrazen na Obr. 28.



Obrázek 27: Odhad PT řešení přijímače uživatele z autentického signálu GNSS.



Obrázek 28: Odhad offsetu hodin přijímače uživatele při zadané poloze.

Z Obr. 27 a 28 můžeme pozorovat, že odhad offsetu hodin přijímače s externě poskytnutým přesnějším zaměřením polohy, je oproti druhé možnosti, odhadující i polohu přesnější. To je způsobeno tím, že je chyba odhadu polohy výrazně menší, v tomto případě nulová, a nepropaguje se tak do odhadu offsetu hodin.

Nyní jsme schopni z pseudo-vzdáleností obdržených skrz přijaté signály odhadnout časový

offset uživatele oproti GPS v obou situacích, kdy mu poloha byla nebo nebyla poskytnuta. Z těchto odhadů dále budeme vycházet v procesu detekce, který se snaží identifikovat napadení stacionárních přijímačů pouze prostřednictvím časové základny.

Tato kapitola a její rovnice jsou implementovány v MATLAB® skriptu 9

7 Výsledky simulací a jejich interpretace

V této kapitole se zaměříme na prezentaci a interpretaci výsledků simulace napadení satelitních signálů a jejich detekce. Simulace byly provedeny s cílem pochopit a kvantifikovat dopady různých typů útoků na satelitní signály a efektivitu námi vybrané detekční metody.

Výsledky simulace nám poskytují hluboký vhled do problému napadení časové základny stacionárních přijímačů. Pomocí vizualizací a kvantitativních měření ukážeme, jak se různé typy útoků projevují v měřených pseudo-vzdálenostech a jak naše detekční metoda reaguje na tyto anomálie.

Každý graf v této kapitole je doprovázen podrobným popisem a interpretací, která čtenářům pomůže pochopit klíčové aspekty našeho výzkumu. Naše analýza se zaměřuje na porovnání výsledků získaných z různých scénářů simulace a diskusi o významu těchto výsledků pro budoucí výzkum a vývoj v oblasti detekce napadení satelitních signálů.

Doufáme, že tato kapitola poskytne čtenářům jasný a srozumitelný přehled o našem výzkumu a poslouží jako pevný základ pro další diskusi a analýzu.

7.1 Přesné modelování vlastností šumu útočníkem

Nejprve jsme pro simulaci zvolili složitější, méně reálnou variantu útoku, kdy byl tento útok v jistém smyslu ideální. To spočívalo v tom, že útočník, který se snažil napadnout přijímač uživatele, byl schopný věrně modelovat vlastnosti šumů působících na autentické GNSS signály a přesně znal polohu přijímače napadeného uživatele.

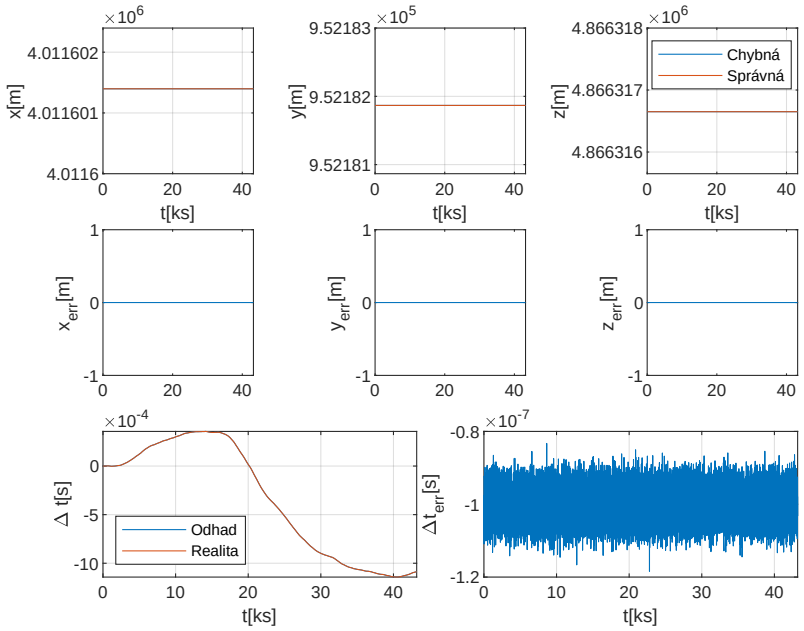
Víme, že znalost polohy nám umožní lépe generovat falešnou pseudo-vzdálenost, neboť nám zde nevznikne chyba vzdálenosti mezi útočníkem a napadeným uživatelem, tj. uvažujeme vztah (33). Odhad působícího šumu v tomto vztahu $\widehat{\nu}_n^i$ a skutečný šum ν_u^i působící na autentické GNSS signály, uvedený v (57) pro jednotlivé satelity konstelace i, má dále stejné vlastnosti. Ty jsme pro jednoduchost zvolili jako bílé gaussovké šumy s nulovou střední hodnotou a variancí získanou ze vztahu (10), vycházejícího z Tab. 2. Jediný rozdíl je zde tedy dán přítomností neurčitosti odhadu času GPS, tj. přítomností členu ξ v (30)

Napadení γ dodávané útočníkem jsme zvolili konstantní o velikosti $10^{-7}[s]$. Do vztahu udávající falešnou pseudo-vzálenost jsme však museli převést tuto hodnotu na metry vynásobením rychlostí světla c. Takovým útokem jsme následně ovlivňovali přijímač uživatele v různých časech simulace o různé délce.

7.1.1 Napadení od začátku

Začali jsme s útokem, jehož délka odpovídala délce celé simulace, tzn. napadený uživatel vůbec neobdržel autentický signál z GNSS a po celou dobu jeho fungování přijímal falešný signál. Odhad offsetu hodin takto napadeného přijímače, který vychází z externě spolehlivě poskytnuté polohy, je možné vidět na Obr. 29. Z těchto grafů lze pozorovat, že v případě kdy probíhá napadení od začátku není vidět žádná výrazná změna v průběhu odhadovaného offsetu. Ten je pouze posunut oproti skutečnému offsetu napadeného přijímače o námi zvolenou hodnotu $\gamma = 10^{-7}[s]$. Přijímač tak není schopen v průběhu offsetu pozorovat žádné výrazné změny, které by mohli ukazovat na útok.

Zde přichází na řadu námi zkoumaná detekční metoda založená na Allanově varianci. Detekční metoda na základě odhadnutých časových offsetů získaných ze simulovaných pseudo-vzdáleností



Obrázek 29: Odhad offsetu při externě zaměřené poloze z pseudo-vzdáleností, napadených od začátku simulace.

spočte daný počet Allanových variancí. Ty následně můžeme porovnat s mezemi získanými ze spolehlivých modelů nebo měření v "ideálních"podmínkách s jistotou nepůsobícího útoku, tak jak je popsáno v kapitole 5.1.2.

Jelikož jsme výpočtem AVAR pro simulovaných 12 hodin obdrželi mnoho jejich průběhů, vykreslíme pro přehlednost pouze několik náhodně vybraných společně s extrémy, získanými přes všechny vypočtené AVAR. Ty označují oblast, ve které se získané AVAR vyskytují.

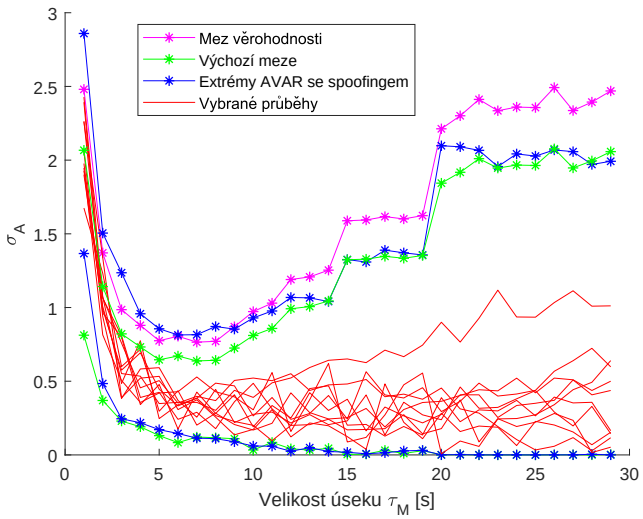
Pro výpočet těchto AVAR jsme nejprve uvažovali dálku úseku $\tau_m = 60[s]$ se vzorkovací frekvencí $1[Hz]$. Díky tomu jsme pro jeden úsek obdrželi $M = 60$ vzorků. Dále je pro výpočet nutné zvolit formu posunu snímků. Pokud nebude řečeno jinak, bude se jednat o nepřekrývající se úseky (tzn. 1-60, 61-120, atd.). Na základě těchto parametrů jsme dopočítali AVAR, dle postupu uvedeného v kapitole 5.1.

Porovnání pro útok působící od začátku vypočtené z přesnějšího dohadu offsetu, tedy s přesně zaměřenou polohou uživatelského přijímače můžete vidět na Obr. 30

Z grafu uvedeného na Obr. 30 je patrné, že maxima AVAR překračují námi stanovené meze. Nicméně detekci provádíme na základě aktuálního průběhů, který jak vidíme ne vždy musí tyto meze překračovat. Z aktuálního průběhu tedy nejsme v tomto případě vždy schopni detekovat napadení. Řešení tohoto problému závisí na délce úseku, jejíž vliv je probírán později v této kapitole.

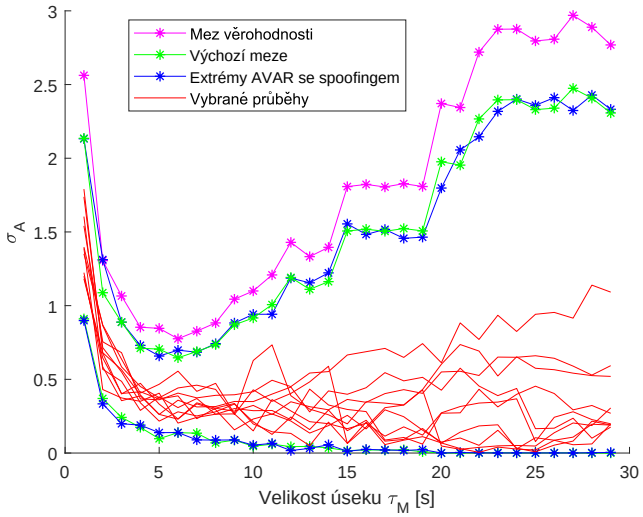
Nyní se zaměřme na to, z jakého důvodu některé získané průběh AVAR překračují stanovené meze. Intuitivně by se dalo říct, že je to kvůli námi přidanému napadení γ, nicméně v tomto případě tomu tak zcela není. Jelikož využíváme jednoduché konstantní napadení, které pouze posune odhad offsetu času, tzn. změní jeho střední hodnotu, ale nijak nemění jeho varianci, díky neuvažování ξ v (30). Nedochází tak k ovlivnění výpočtu AVAR a útok nebude možné detekovat. To můžeme vidět na Obr. 31, kde extrémy AVAR získaných z testovaného signálu přibližně odpovídá referenčním mezím věrohodného signálu.

Změnu AVAR tak v tomto případě ovlivňuje pouze chyba odhadu offsetu hodin, resp. chyba odhadu času GPS, ξ, útočníka. Ať útočník využívá k napadení sebelepších metod odhadu a zařízení, bude tato chyba v útočníkem generované pseudo-vzdálenosti obsažena vždy. Útočník totiž nikdy



Obrázek 30: Porovnání získaných AVAR s referenčními mezemi, při napadení působícím od začátku.

nebude schopen přesně určit čas t_{GPS}, který je obsažen v autentické psudo-vzdálenosti poskytované konstelací GPS.

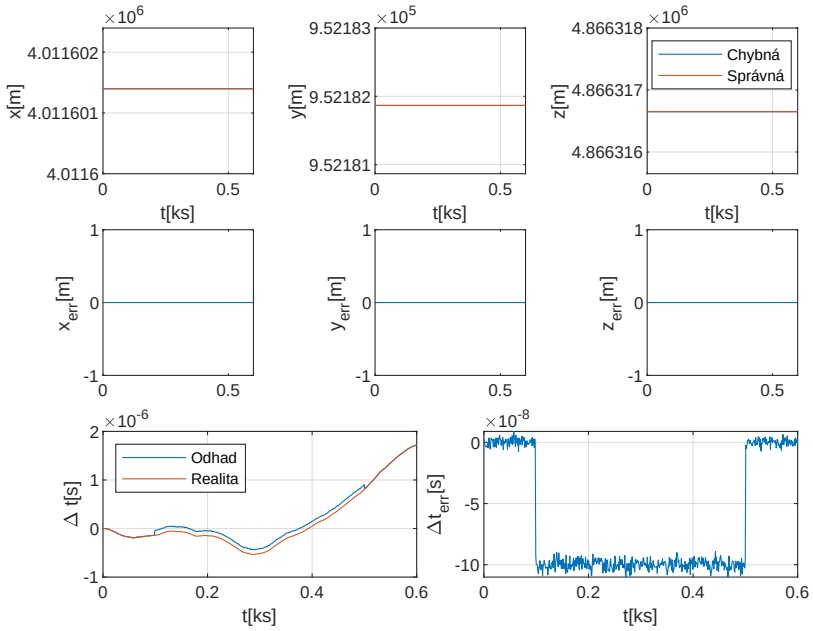


Obrázek 31: AVAR dat testovaného signálu, bez působení chyby odhadu času GPS v podvržené pseudo-vzdálenosti.

Tímto jsme ověřili, že při konstantním napadení s věrně modelovanými vlastnostmi působícího šumu a přesně známou polohou uživatele vychází možnost jeho detekce z chyby odhadu času GPS útočníkem.

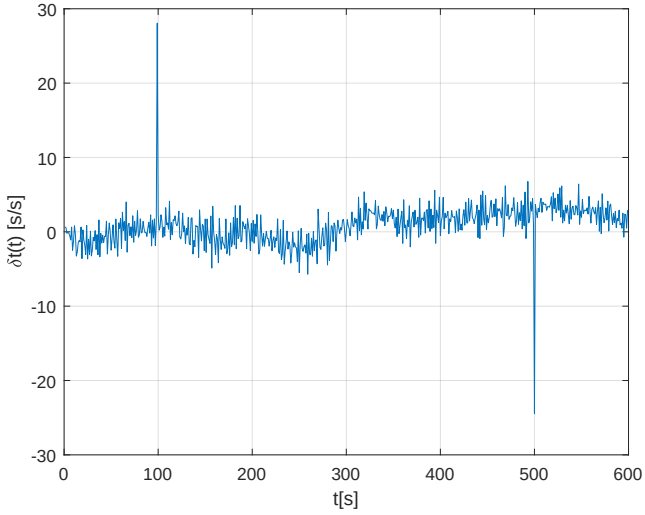
7.1.2 Napadení v průběhu

Ve většině situacích však k útoku dochází v průběhu fungování využívaného přijímače. Proto jsme se soustředili i na tento problém. Útok jsme tak v naší simulaci uvažovali tak, že působil na



Obrázek 32: Odhad offsetu při externě zaměřené poloze z pseudo-vzdáleností, napadených v průběhu simulace.

jejím určitém úseku. Krom tohoto úseku pak přijímá uživatele autentické GPS signály. Z grafu znázorněného na Obr. 32 pak tuto skutečnost můžeme pozorovat. Vidíme, že ke změně dochází pouze u odhadovaného offsetu přijímače, v daném čase, kdy jeho průběh obsahuje skokovou změnu. V takovém případě by jsme byli schopni určit napadení pouze z diference po sobě jdoucích hodnot odhadu získaných v jednotlivých časech, viz. 33. Z tohoto grafu je patrné že v čase 100 a 200

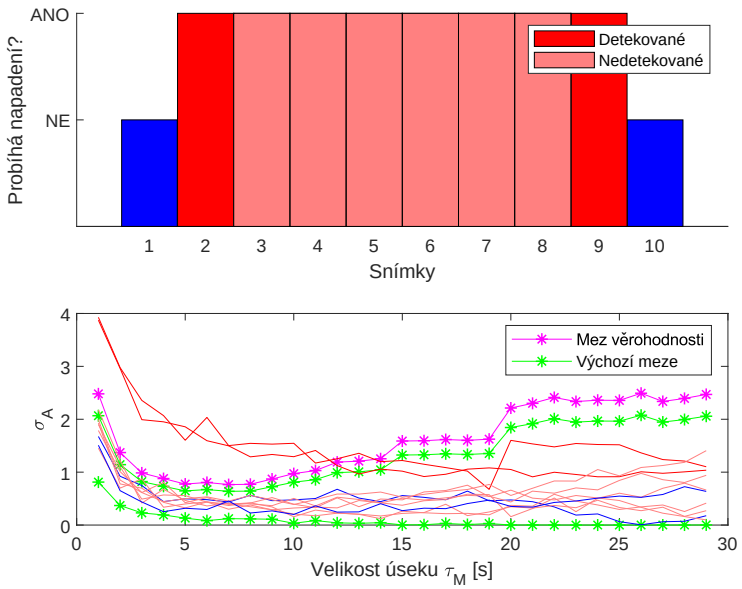


Obrázek 33: Diference po sobě jdoucích hodnot odhadovaného offsetu hodin přijímače.

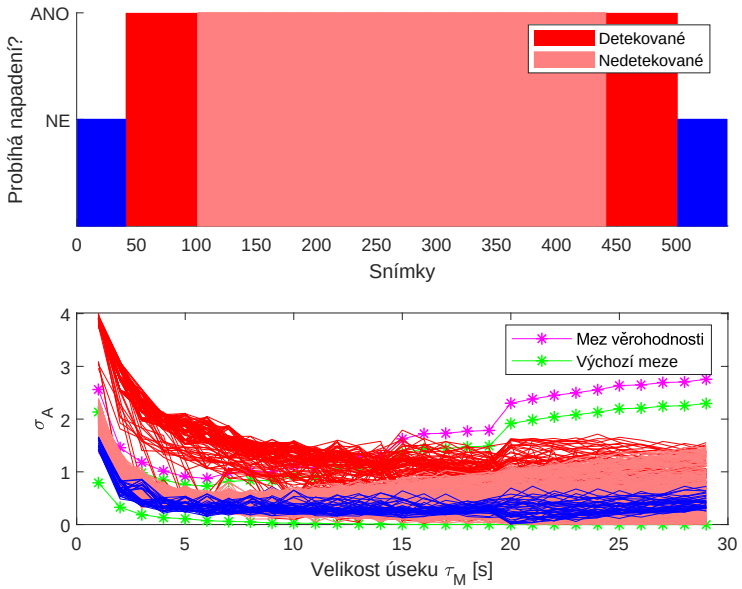
sekund došlo k výrazným změnám dvou po sobě jdoucích odhadů času, které odpovídají začátku a konci útoku. Nicméně ověřme, že v takovém případě bude fungovat i námi zkoumaná detekční

metoda.

Na následujících grafech Obr. 34 a 35 bude znázorněna detekce pomocí AVAR pro obě zmíněné formy, tedy pro nepřekrývající se a překrývající se úseky opět při délce úseku $\tau_M = 60[s]$. Z prvního



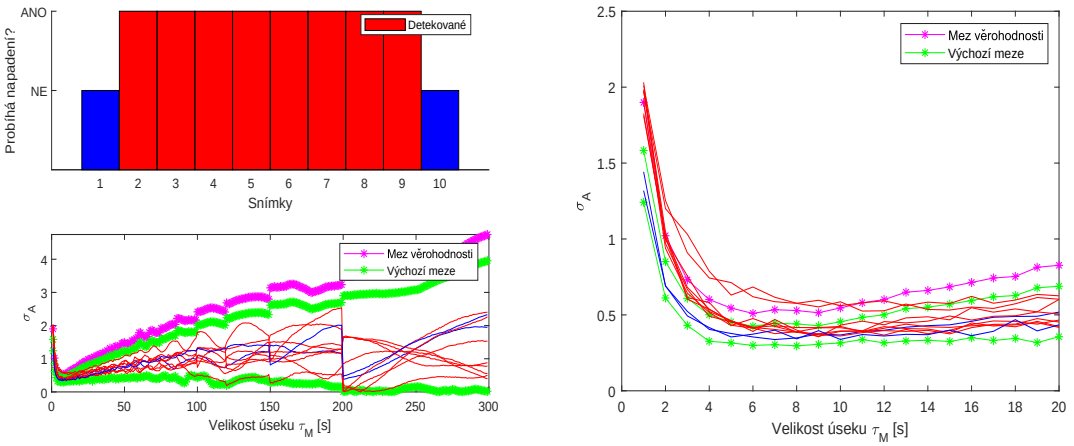
Obrázek 34: Napadené snímky a jím odpovídající průběhy AVAR pro nepřekrývající data.



Obrázek 35: Napadené snímky a jím odpovídající průběhy AVAR pro překrývající data.

Obr. 34 můžeme vidět, že obsahuje méně snímků a tedy i jím odpovídajících průběhů AVAR, než-li Obr. 35. To je způsobeno formou posunu těchto snímků. Nepřekrývající forma pro své úseky využívá neopakující se vzorky času (tzn. 1-60, 61-120, ...), v překrývající formě dochází k jejich opakovanému využití (tzn. 1-60, 2-61, ...). Vezmeme-li tedy prvních $T = 600$ měření s úsekem o

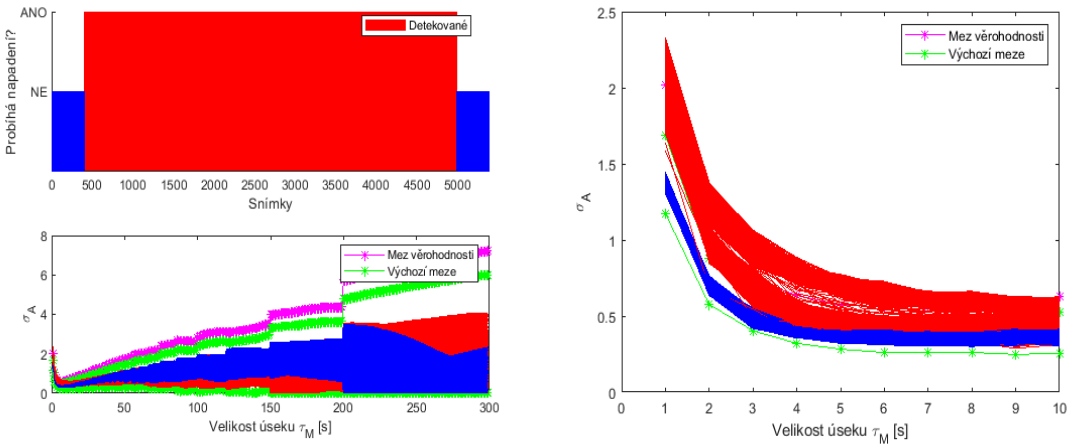
$M = 60$ vzorcích, získáme v prvním případě $T/M = 10$ snímků a v druhém $T - M + 1 = 541$. Každá z těchto forem může mít své výhody i nevýhody. Překrývající formou získáme přesnou informaci o tom kdy k napadení došlo, ale z důvodu opakování vzorků bude výskyt této chyby pozorována po celých M snímků. U nepřekrývající se formy nedojde k opakovanému pozorování chyby, za to ale získáme pouze časový interval, ve kterém se napadení vyskytlo.



Napadené snímky a jejich průběhů AVAR. Přiblížení spodního grafu.

Obrázek 36: Průběhy AVAR napadených snímků s 10x delšími nepřekrývajícími se úseky.

Nyní se zaměřme na funkčnost detekce. V obou formách je patrný útok v případě, kdy snímky využívají zároveň data z napadeného a nenapadeného měření. Pro skokovou změnu jsme tedy schopni detekovat počátek a konec útkou i pomocí AVAR vycházející z předem uvedeného driftu, viz 33. Problém nastává v případě, kdy naše metoda začne k výpočtu AVAR využívat pouze napadená data. Tuto situaci jsme však již zkoumali v případě, kdy útok působil od začátku simulace. Zde pozorujeme, že opět ne všechny průběhy musí překročit zvolené meze. V nepřekrývající formě je nepřekročí žádné a v překrývající pouze některé průběhy AVAR. My však chceme být schopní detekovat útok i z těchto snímků, jelikož zde působí chyba hodin, která by průběh AVAR měla ovlivnit i při výpočtu pouze z napadených dat.



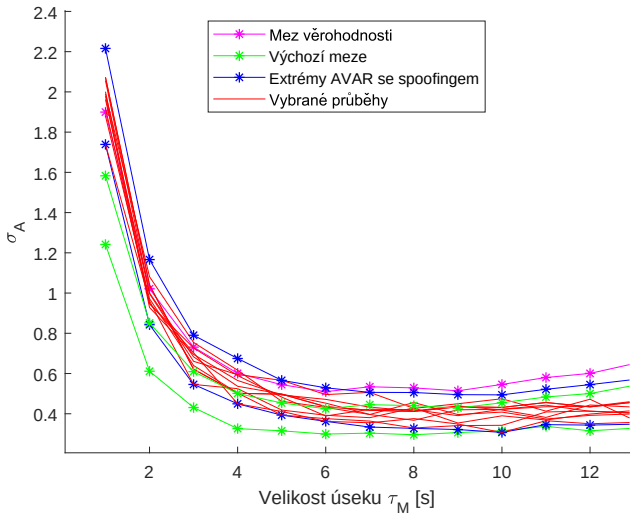
Napadené snímky a jejich průběhů AVAR. Přiblížení spodního grafu.

Obrázek 37: Průběhy AVAR napadených snímků s 10x delšími překrývajícími se úseky.

Jak již bylo naznačeno u předchozí situace, tento problém spočívá v délce úseku využitého pro výpočet průběhu AVAR. My jsme zprvu volili délku úseku $\tau_M = 60[s]$. Vycházeli jsme totiž z práce [4], kde se uvažovalo, že během krátkého časového úseku nemůže dojít k zásadnímu ovlivnění polohy útočníkem. Nicméně v našem případě stacionárního přijímače nás změna polohy netrápí, jelikož by bylo okamžitě možné takové napadení detekovat. Můžeme tak využít delších snímků. Délku snímku jsme tak společně se simulačními časy 10x prodloužili, což vedlo k výsledkům zobrazených na Obr. 36 a 37.

Z těchto grafů můžeme pozorovat, že prodloužení úseku, na kterém je AVAR počítána, má pozitivní dopad na detekci napadení napadení obou forem v oblasti, kdy se využívají pouze napadená data. V tomto případě dojde k překročení výchozí meze ve výrazně vyšším počtu průběhů AVAR. Lze tedy říci, že s využitím nepřekrývající formy je možná detekce napadení ve všech případech. V překrývající formě jsme schopní detekovat napadení z výrazné většiny průběhů AVAR, pro jeden průběhy který nepřekračují mez se může jednat o ojedinělou náhodně způsobenou výjimku.

Tedy i v situaci zmíněné v předchozí podkapitole, kdy napadení působilo od začátku simulace, viz Obr. 30, budeme schopni detekovat napadeni ze všech průběhů AVAR určených nepřekrývající formou. To lze vidět na Obr. 38.



Obrázek 38: Přiblížení získaných AVAR s referenčními mezemi, při napadení působícím od začátku s 10x delšími úseky.

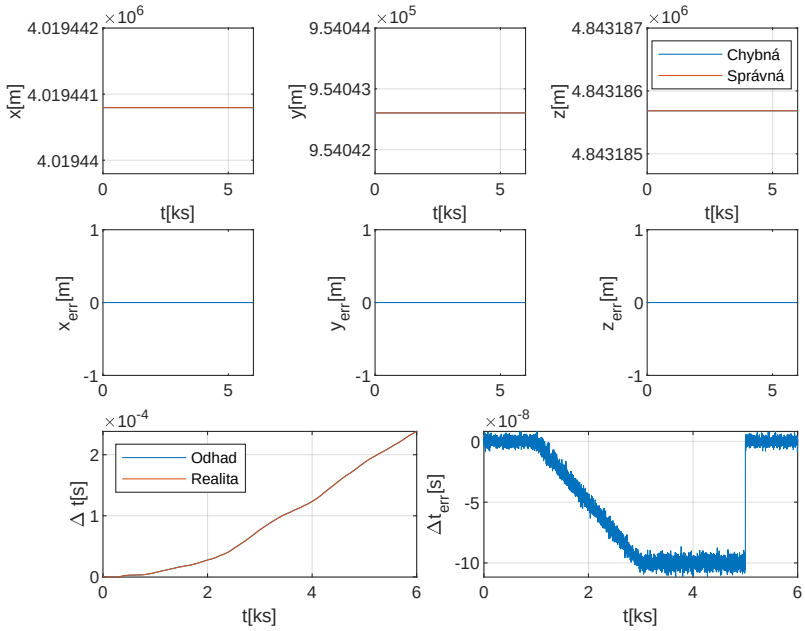
Je vidět, že extremální průběhy, které udávají maximální a minimální hodnoty získané ze všech vypočtených AVAR, překračují výchozí mez. Z toho můžeme usoudit, že data použitá pro výpočet byla získána z podvrženého signálu.

Z jakého důvodu, však délka snímku ovlivňuje schopnost detekce naší metody? Využíváme-li krátký úsek, obdržíme pouze malý počet vzorků ($M = 60$). Z těch nemusí být zcela patrný rozdíl jejich vlastností. Naopak pro delší úsek, který jsme zvolili desetinásobný, jsme obdrželi vzorků více ($M = 600$). Pro větší množství dat je poté detekce změny statistických vlastností určena spolehlivěji a snadněji tak lze odhalit působící útok.

V realitě se však se skokovou změnou napadení často nesetkáme, je však dobrá pro zkoumání našeho dosavadního problému. Nyní si zde představíme případ, ve kterém dochází k postupné změně napadení.

Postupný vliv napadení

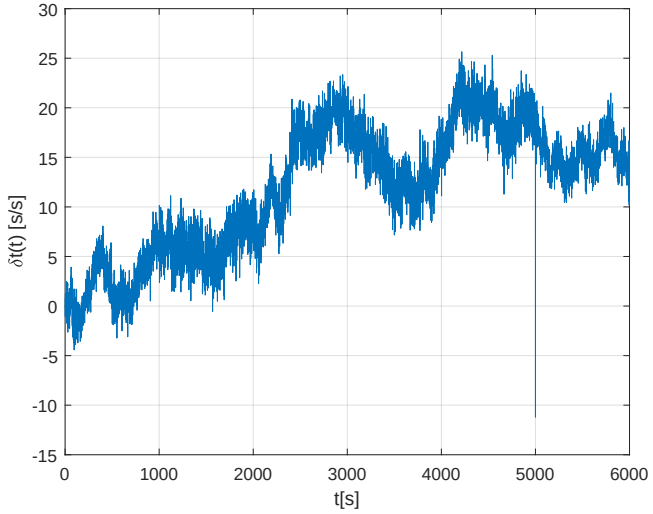
Uvažujme tedy situaci, kdy útočník postupně zvyšuje velikost, a tím i vliv působícího napadení γ. Průběh odhadu offsetu uživatelského přijímače z takto podvrženého měření pseudo-vzdálenosti



Obrázek 39: Odhad offsetu při postupně působícím útoku.

je možné vidět na Obr. 39.

Postupný nárůst vlivu útoku můžeme pozorovat z grafu chyby odhadu, který postupně narůstá až do útočníkem zvolené hodnoty. Tímto způsobem je schopen útočník ovlivňovat hodnoty dle své libosti. Pokud se při napadení využije postupného nárůstu vlivu, je nemožné napadení detekovat pouze na základě diference po sobě jdoucích hodnot, jak bylo ukázáno při skokové změně, Obr. 33. Dochází zde totiž jen k nepatrné změně těchto hodnot, což se ve výsledné diferenci neprojeví a hodnoty se tváří jako autentický průběh, viz. Obr. 40.

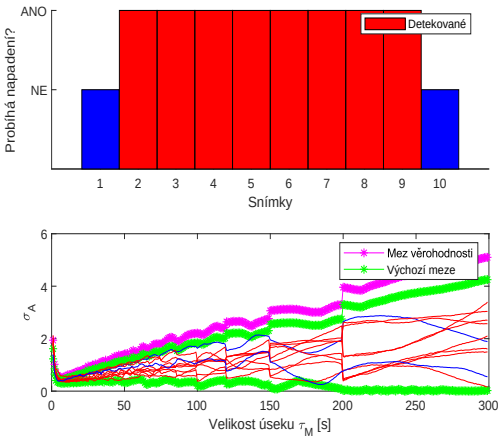


Obrázek 40: Diference odhadovaných hodnot času GPS při postupném nárůstu napadení.

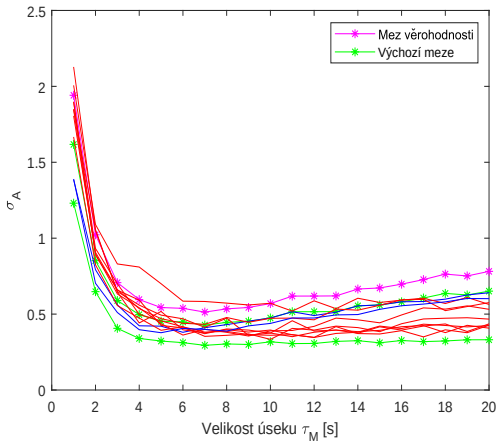
Pokud by útočník pouze neukončil útok, ale vrátil by se stejným způsobem na původní hodnotu

odhadovaného času, nebyl by zde ani vrchol v čase 5000, který je nyní způsoben koncem napadení.

Pokusme se tedy opět využít námi zkoumanou metodu. Z ověřeného předpokladu, že je detekce útoku závislá na chybě hodin, by jsme měli být schopni detekovat i takovýto druh útoku.

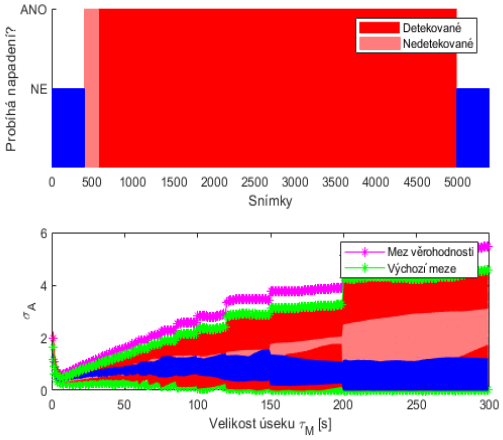


Napadené snímky a jejich průběhů AVAR.

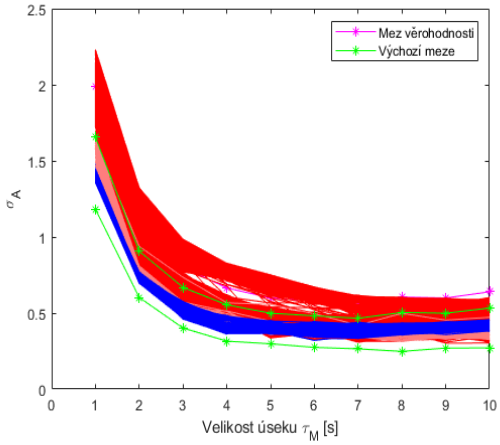


Přiblížení spodního grafu.

Obrázek 41: Průběhy AVAR napadených snímků s nepřekrývajícími úseky pro postupný náběh útoku.



Napadené snímky a jejich průběhů AVAR.

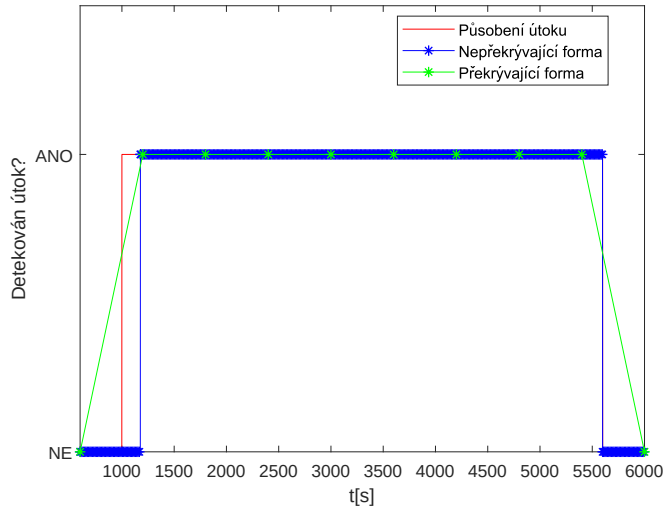


Přiblížení spodního grafu.

Obrázek 42: Průběhy AVAR napadených snímků s překrývajícími úseky pro postupný náběh útoku.

Z Obr. 41 vidíme, že toto napadení je možné z nepřekrývající formou určené AVAR detekovat, nicméně detekce pomocí této formy nám nedá důkladný přehled o začátku napadení. Využili jsme tedy opět i překrývající metodu, kde můžeme vidět, Obr. 42, postupné napadení nemusíme být vždy schopni okamžitě detekovat. To je způsobeno opakovaným využívaní dat.

Předpokládejme, že napadení začalo působit. AVAR v takovém případě začne využívat současně s vzorky z autentického měření i ty podvržené. Nicméně z počátku je počet podvržených vzorků výrazně menší něž-li počet autentických. Z toho důvodu nedojde k detekci napadení okamžitě, ale s jistým zpožděním, viz Obr. 43. Toto zpoždění odpovídá době, kdy počet falešných vzorků stoupne natolik, že bude schopen ovlivnit výpočet AVAR.



Obrázek 43: Detekce napadení v čase pro různé formy posunu snímků.

Tento obrázek tak znázorňuje překročení výchozí meze získanou AVAR. Pro jednoduchost jsme tuto skutečnost vykreslili porovnáním prvního bodu AVAR pro mez i aktuální průběh. První bod byl zvolen, jelikož je zde vliv napadení nejvýraznější. Pokud je tedy AVAR aktuálního průběhu nad mezí, pak je útok detekován.

Nepřekrývající forma je tedy schopna detekce okamžitě, jelikož využívá veškerá poskytnutá data pouze jednou. Je tedy výpočetně méně náročná, ale neposkytuje podrobnější vhled do detekčního problému. Na druhou stranu, pokud se smíříme se větším množstvím výpočtů a vezmeme v úvahu její detekční zpoždění, poskytuje překrývající forma dobrý vhled uživatele na působící útok.

7.1.3 Napadení s chybným zaměřením polohy uživatele útočníkem

Přibližme se opět o krok k reálnějšímu problému, který útočníkovy zhoršuje kvalitu jeho napadení. Doposud jsme uvažovali, že útočník přesně znal polohu přijímače uživatele, kterému poskytoval falešný signál. V praxi tomu tak ale většinou nemusí být a útočník nebude znát jeho polohu zcela přesně. Tuto polohu může určit různými způsoby, jako například využitím snímačů vzdálenosti, kdy poloha napadeného je následně dopočtena na základě známe polohy útočníka.

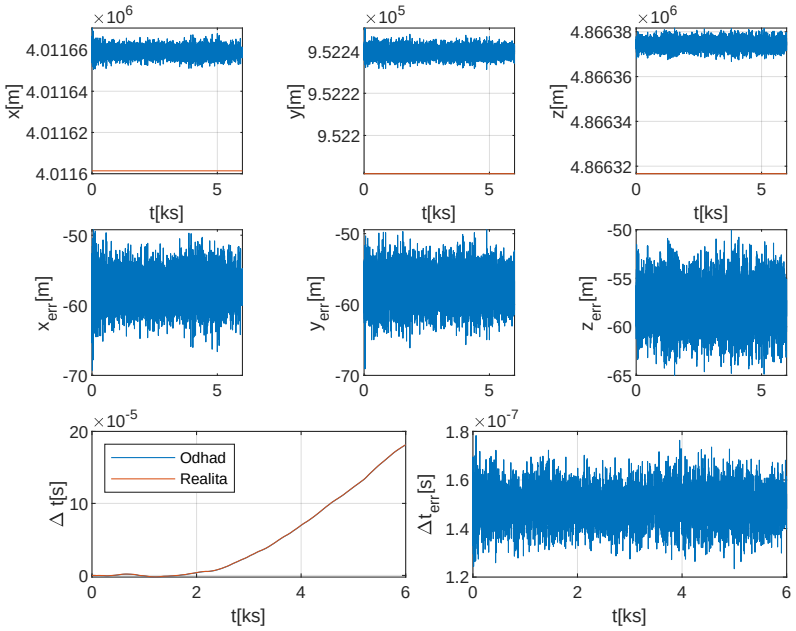
Chyba, která vznikne nepřesným určením polohy nám ovlivní měření pseudo-vzdálenosti, jak je popsáno v rovnici (31). Vede totiž na jinou délku, resp. dobu letu signálu mezi útočníkem a napadeným uživatelem. Působení této chyby se následně projeví v jednotlivých odhadech získávaných z napadeného měření.

Pokud by uživatel odhadoval, jak offset hodin, tak svoji polohu, promítla by se tato chyba zaměření pouze do odhadu polohy a odhad offsetu by nijak výrazně nezatížila, viz Obr. 44. Uživatel by v tomto případě mohl detekovat napadení porovnáním své známé polohy a jejího odhadu.

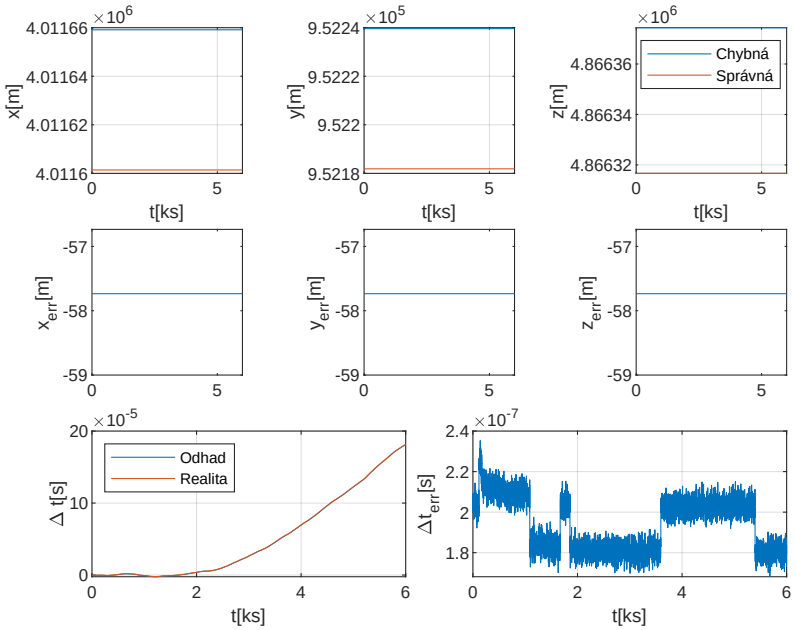
V některých aplikacích si však uživatel svou polohu neodhaduje a spoléhá pouze na její externě poskytovanou hodnotu. Tu získává z přesných a spolehlivých zdrojů, jakými mohou být geodetická zaměřování. Uživatel tedy odhaduje pouze offset jeho hodin. Pro určení jeho hodnoty využívá uživatel této poskytované polohy, s jejíž pomocí je následně schopen získat kvalitnější odhad tohoto offsetu, jak bylo ukázáno v Obr. 28.

Jelikož uživatel odhaduje pouze offset svých hodin, nemá se chybná poloha jak projevit v odhadu jeho polohy. To vede na její propagaci do zbývajícího odhadovaného parametru, kterým je offset hodin uživatele. Tuto skutečnost je možné vidět na Obr. 45.

Na tomto obrázku můžeme vidět graf znázorňující průběh chyby odhadovaného offsetu, v němž



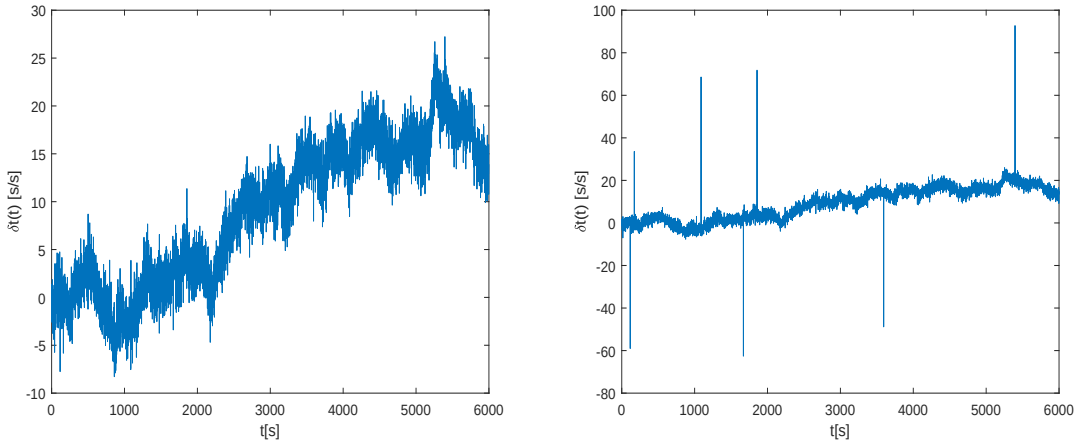
Obrázek 44: Chyba zaměření o velikosti 100m propagovaná do odhadu polohy.



Obrázek 45: Chyba zaměření o velikosti 100m propagovaná do odhadu offsetu.

jsou patrné jisté změny jeho hodnot. Tyto změny závisí na geometrii a počtu dostupných satelitů konstelace GPS. Pokud útočník nemá spolehlivé informace o poloze přijímače uživatele, nemůže spoléhat na to, že bude schopen docílit přesného posuvu časové základny. Výsledný posuv totiž závisí na útočníkem vyslaných signálech, ke kterým se přičte chyba pozice přeložená přes aktuální konstelaci GPS do časové domény.

Takovéto změny je možné pozorovat, pro vyšší chyby v zaměření polohy napadeného uživatele, prostřednictvím diference hodnot odhadů offsetu, tzn. driftu. Nicméně pro menší chyby zaměření se tato chyba ztratí v šumu, kterým zatěžuje měřené signály, z jejichž dat se odhad počítá. Porovnání driftu pro nižší a vyšší chybu zaměření je znázorněno na Obr. 46.



Malá chyba zaměření, vzdálenost 100m. Velká chyba zaměření, vzdálenost 1km.

Obrázek 46: Drift hodin při různě velkých chybách zaměřené polohy.

Chceme-li však útok detekovat i pro nižší chyby zaměření budeme muset opět využít metodu AVAR. Útočníkovo chybné určení polohy napadeného uživatele nám výrazně ovlivní maximální hodnotu variance, které je možné dosáhnout dosáhnout výpočtem AVAR. Vyšší hodnoty takovýchto chyb tak budou mít pozitivní vliv na detekci podvrženého signálu. To lze vidět na Obr. 47.

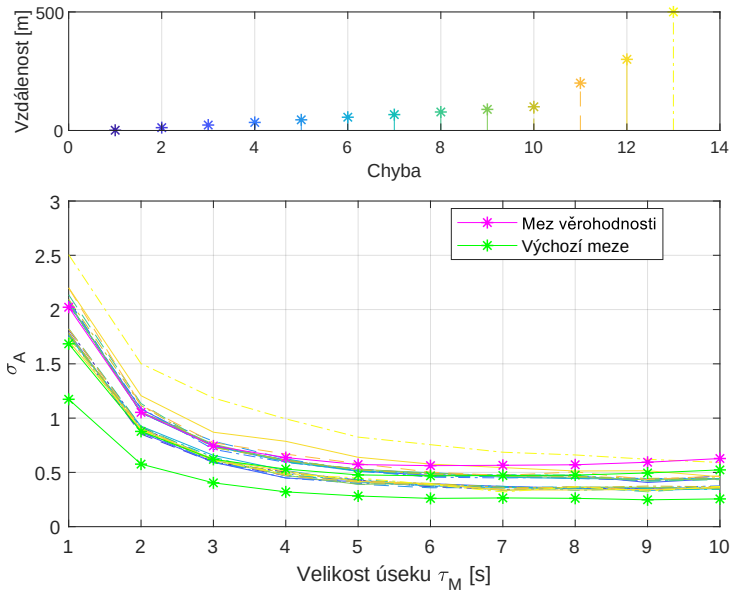
Pro znázornění tohoto problému jsme uvažovali pouze první ze zmíněných situací, tedy skokový útok s chybou odhadu hodin a bílým šumem působící na měřenou pseudo-vzdálenost od začátku simulace.

Na tomto obrázku tak můžeme z prvního grafu vidět velikost chyby útočníkova zaměření polohy uživatele a z druhého jakým způsobem ovlivňuje AVAR. Znázornili jsme zde opět pouze jen extremální průběhy získané přes všechny vypočtené AVAR. Z toho můžeme pozorovat, nám nejvýznamněji ovlivňuje maximální hodnotu určené variance. Můžeme tedy říci, že čím větší tato chyba bude, tím výraznější rozdíl od detekčních mezí nastane a my budeme schopni s větší jistotou útok detekovat.

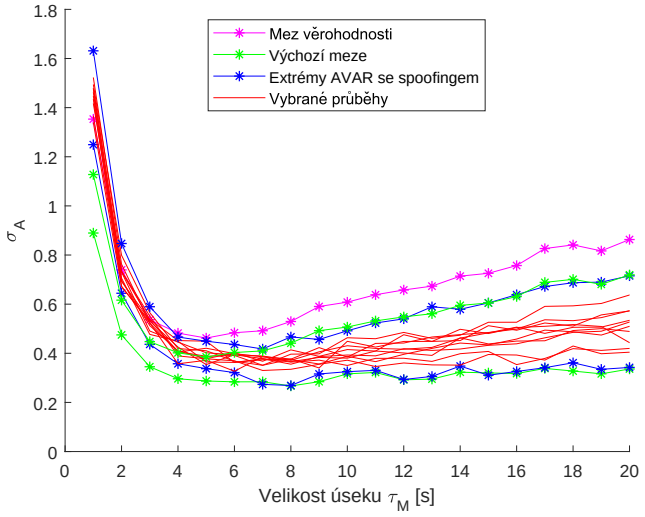
7.2 Nepřesné modelování vlastností šumu útočníkem

Přesuňme se k dalšímu problému, tím je situace, kdy útočník není schopen přesně modelovat vlastnosti šumu působícího na autentické GPS signály. Jde o situaci nejvíce podobnou skutečnosti, jelikož v praxi se pro určení takových šumu a jejich vlastností využívají modely. Ač jsou tyto modely sebelepší, nedokáží modelovat šum působící na GPS signály bez chyby. Rozdílnost v těchto vlivech následně přináší výhody pro uživatele, kteří se snaží detekovat a následně bránit proti napadení.

V naší simulaci jsme uvažovali nepřesné modelování těchto vlastností tak, že jsme autentický signál GPS generovali jako kombinace korelovaného a bílého šumu. Korelovaný šum jsme modelovali pomocí Gauss-Markovského procesu, získaného na základě AR modelu popsaného (58). Střední hodnotu obou šumu jsme uvažovali nulou a varianci jako polovinu hodnoty získané na základě modelů ze vztahu (10). Šum generovaný útočníkem jsme poté uvažovali pouze jako samotný bílý šum s nulovou střední hodnoto a variancí obdržen z rovnice, uvedené v předchozí větě. Taková simulace následně vedla na rozdílné vlastnosti pseudo-vzdáleností měřené z autentického a útočníkem podvrženého signálu.



Obrázek 47: Vliv velikosti útočníkovi chyby zaměření polohy uživatele na výpočet AVAR.



Obrázek 48: Přiblížení průběhů AVAR, kdy podvržené pseudo-vzdálenost nejsou zatížena chybou hodin, ale pouze šumem.

Abychom zde nemuseli vykreslovat všechny grafy znovu, řekněme pouze, že v tomto případě jsme schopni detekovat veškeré napadení probrané v předchozích kapitolách a to i pro krátký interval $\tau_M = 60[s]$. V tomto případě totiž k chybě hodin přibývá i v čase korelovaný šum, který také ovlivňuje výpočet AVAR.

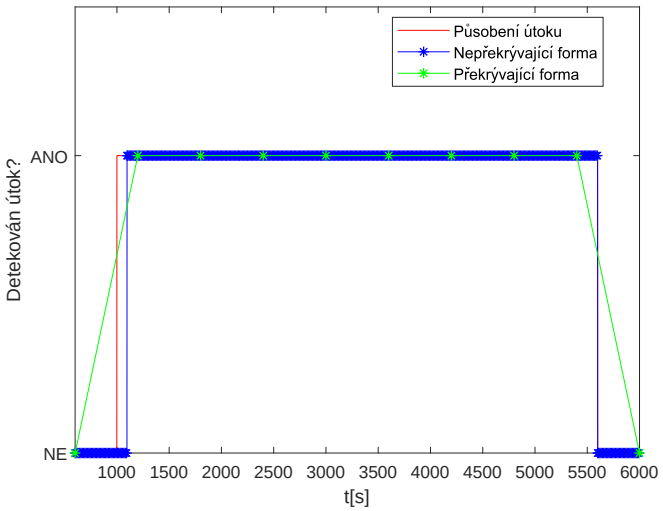
Nicméně jsme v tomto případě schopni detekovat útok i v některých situacích, jež jsme nebyli schopni detekovat v předchozích částech.

Jednou z nich je situace, kdy útočník dostatečně přesně odhadoval čas konstelace GPS. U takového odhadu byla jeho chyba velice malá, ideálně pro útočníka nulová. Pro takový případ jsme nebyli schopni útok detekovat, viz Obr. 31, jelikož se měnila pouze střední hodnota odhadu a

nikoliv její variance. To však zde neplatí, nýbrž varianci ovlivní i korelovaný šum. Pokud by tedy útočník jakýmsi způsobem určil přesný čas GPS, například by přijímal korekční data poskytovaná satelitům, budeme moci i tak útok úspěšně detekovat. Tento vliv na průběhy vypočtených AVAR můžeme vidět z Obr. 48. Pro jednoduchost jsme zde opět uvažovali, stejně jako v situaci na Obr. 31 od začátku působící skokovou změnu poruchy a nepřekrývající formu AVAR.

Zásadní změna průběhů AVAR opět nastává v jeho počátečních hodnotách. To je důvod, proč si zde zobrazujeme přiblížení AVAR spočteného na rozsáhlém časovém úseku $M = 600$ vzorků.

Další situací je postupný útok, který způsobil zpoždění v detekci využívající překrývající formu AVAR. Zde nám metoda také útok neodhalí na základě každého průběhu AVAR. Nicméně umožní napadení detekovat s menším zpožděním, viz Obr. 49, jelikož se současným působením chyby odhadu hodin a rozdílných vlastností šumů navýší variance měřených dat, které ovlivní i určovanou AVAR.



Obrázek 49: Detekce napadení v čase pro různé formy posunu snímků, kratší detekční zpoždění.

Důkladným porovnáním zmíněného grafu s Obr. 43 uvidíme, že v případě využití překrývající formy AVAR jsme schopni detekovat napadení přibližně o 80 sekund rychleji než v případě, kdy útočník spolehlivě modeloval vlastnosti šumu působící na autentický signál.

7.3 Zhodnocení výsledků

Veškeré zmíněné situace, získané a zkoumané na základě sestrojeného simulačního modelu nám poskytly zásadní vhled na funkčnost námi zvolené detekční metody. Zjistili jsme, že pro spolehlivější detekci napadení z časové oblasti, je třeba využít k určení AVAR větší množství dat, nežli pro detekci v oblasti poziční. To vede na spolehlivější určení statistických vlastností odhadu, ze kterých vychází výpočet AVAR. Z obdržených výsledků můžeme říci, že je metoda schopna takový útok v jistých případech detekovat. Nicméně ne vždy jsme schopni detekci získat okamžitě, či s přesnou informací o jeho počátku.

Využíváme-li nepřekrývající formu AVAR detekujeme útok ve většině testovaných případů, avšak nejsme takto schopni s jistotou říci v jakém čase začal. Využíváme totiž každý získaný odhad pouze jednou, což nám ve výsledku neposkytuje kvalitní informaci. Překrývající forma AVAR nám na druhou stranu ne vždy detekuje napadení. Využívá totiž k výpočtu AVAR dvou sousedních snímků vždy, až na jeden odhad, stejné odhady. To způsobuje, že odhady zatížené útokem jsou z počátku převažovány odhady z autentických dat, což způsobuje zpoždění detekce. Ve chvíli, kdy je vliv napadených odhadů překročí jistou mez je pak takový útok detekován.

Výsledky získané v této práci jsme vizuálně znázornili v Tab. 3, která udává schopnost metody založené na AVAR detekovat útok. V níž X znázorňuje pravdivost a — nepravdivost příslušného tvrzení. Dále jsou v tabulce uvedeny zkratky, které popisují nepřekrývající (Nepřekr.) a překrývající (Překr.) formu AVAR či působení kombinace korelovaného a bílého šumu (Kombin.).

Je také nutno zmínit, že tato tabulka je získána na základě AVAR počítaných na delším časovém úseku, tj. $\tau_M = 600[s]$. Zjistili jsme totiž, že délka úseku má zásadní vliv na schopnost detekce. Čím delší úsek k výpočtu využijeme, tím více získáme odhadů offsetu hodin, ze kterých spolehlivěji určíme statistické vlastnosti a tedy i případný útok.

Typ útoku	Šum GPS družic	Nedetekuje		Detekuje		Detekuje se zpožděním	
		Nepřekr.	Překr.	Nepřekr.	Překr.	Nepřekr.	Překr.
Skok s chybou odhadu hodin	Bílý	—	—	X	X	—	—
	Kombin.	—	—	X	X	—	—
Skok bez chyby odhadu hodin	Bílý	X	X	—	—	—	—
	Kombin.	—	—	X	X	—	—
Postupný náběh aditivní chyby s chybou hod.	Bílý	—	—	X	—	—	X
	Kombin.	—	—	X	—	—	X
Postupný náběh aditivní chyby bez chybou hod.	Bílý	X	X	—	—	—	—
	Kombin.	—	—	—	—	X	X

Tabulka 3: Výsledky simulace detekční metody založené na AVAR.

Co se týče detekce útoku při chybném určení polohy napadeného přijímače útočníkem, jsme schopni pro tento případ úspěšně detekovat napadení ve stejných situacích, které jsou uvedeny v Tab. 3. Pokud však uvažujeme oba případy, ve kterých je falešná pseudo-vzdálenost generována s přesným odhadem offsetu hodin přijímače, tedy je jeho chyba $\xi = 0$, závisí schopnost detekce na velikosti chyby útočníkova zaměření polohy uživatele. Čím vyšší tato chyba bude, tím spíše budeme schopni v této situaci útok detekovat.

Na základě detekování podvrženého signálu můžeme následně přejít k procesu identifikace povahy útoku, po které následně můžeme přijmout opatření nutná k ochraně systému a obnovení normálního provozu. To může zahrnovat změnu pracovních frekvencí, zesílení signálů čí využití alternativních metod pro určení polohy a času, které nespoléhají výhradně na satelitní signál. Řešení problémů spojených s následným vypořádáním se s útokem je však mimo rozsah této práce.

8 Závěr

V této diplomové práci jsme se věnovali problematice napadení signálu GNSS, které ovlivňují spolehlivost určené polohy či synchronizace času. Předpokladem v této práci bylo, že uživatel má stacionární přesně zaměřenou polohu. Podrobněji jsme se tedy zaměřili na napadení falšující pseudo-vzdálenost přenášenou signálem GPS, tzv. spoofing, který se zaměřoval na změnu časové informace přenášené signálem. K detekci takto působícího útoku jsme využili Allanovy variance s cílem včasně odhalit napadení působící na autentický signál. Detekce napadení z časové oblasti je v dnešních dobách zkoumána převážně z důvodu přesného časování, tzn. synchronizace hodin uživatele s přesnými hodinami konstelace GPS. Přesnost informace o aktuálním globálním čase může mít zásadní vliv na fungování nejrůznějších aplikací, od finančního sektoru, přes dopravu, až po radarové soustavy určující polohu objektů.

Nejprve jsme si uvedli principy fungování globálních satelitních systémů, kde jsme se podrobně seznámili se vzdálenostní metodou, která je využívána k určení polohy a času z satelitních signálů konstelace dostupných přijímači na základě pseudo-vzdálenosti. Dále jsme si zde představili chyby,

které neúmyslným způsobem ovlivňují hodnotu této pseudo-vzdálenosti, jako jsou chyby přijímače, vícecestného šíření signálu či atmosférické chyby, se kterými se vždy musí jistým způsobem u satelitních signálu počítat.

Rovněž jsme se podrobně zaměřili na představení úmyslných chyb působených útočníkem, které informaci přenášenou signálem mají poškodit či úplně odstranit. Představili jsme si tak metody spoofingu (falšování) a jammingu (rušení) signálu, které jsou k těmto účelům využívány. V této práci jsme se zaměřili výhradně na spoofing signálu, kdy byl uveden i způsob generování falešných pseudo-vzdáleností. Množina upravených (spoofovaných) pseudo-vzdáleností následně působí chybu v odhadu času GPS přijímače uživatele, který využívá k synchronizaci svých hodin či jako vstup pro další zařízení.

Největší pozornost jsme v této diplomové práci věnovali detekční metodě založené na Allanově varianci, ze které jsme vycházeli při detekci útoku. Abychom byli schopni pomocí této metody detekovat napadení, museli jsme nejprve stanovit meze věrohodnosti signálu, jejichž překročení následně povede k detekci signálu. Tyto meze věrohodnosti jsme v této práci zvolili jako extremální hodnoty AVAR, které jsme získali z nenapadených pseudo-vzdáleností během jedné simulační epochy satelitů, tzn. simulovaných 12 hodin. Takové určení mezí však nemusí být zcela vyhovující a bude potřeba dalších výzkumů k získání jejich vhodnějších variant (např. mez vypočtená analyticky na základě statistického popisu přijímaného signálu). Po stanovení mezí jsme přešli na zkoumaní různých situací působícího útoku, jejichž hlavní výsledky jsou shrnuty níže. Díky této metodě jsme byli schopni získat podrobnější vhled na napadení působící v časové doméně.

Výsledky dosažené v této práci jsme prezentovali v poslední kapitole, která byla věnována jejich znázornění, interpretaci a diskusi. Z mnoha simulovaných situací jsme zde došli k výsledkům ilustrující schopnosti detekční metody při spoofingu konstelace GPS. Jelikož jsou vlastnosti kvality odhadu hodin t_{GPS}, na základě kterých počítáme AVAR, závislé na aktuální situaci, jsou průběhy těchto AVAR rovněž závislé na konkrétních realizacích a prostředí. V realitě, šum měření a pak i AVAR driftu, počítaného z odhadnutého offsetu, zahrnuje nejen vlastní chybu atomových hodin satelitů (které jsme nesimulovali, jelikož jsou vůči chybě hodin přijímače, ξ, zanedbatelná), ale hlavně chyby ovlivněné např. použitým hardwarem a softwarem přijímače, předpokládané konstelaci (jedné či více), atmosférických podmínkách a modelech, které mají dominantní vliv na kvalitu odhadu.

Další výzkum tohoto tématu by mohl vést k rozšíření obzorů napadení časové domény satelitních signálů. Dalo by se zaměřit na

- kvalitnější specifikace meze věrohodnosti, které by nebyli závisle na specifických podmínkách působících na odhad času satelitních hodin t_{GPS},
- navázání metody na požadované pravděpodobnosti chybné detekce a falešného alarmu,
- dopad použití metody vážených nejmenších čtverců popř. Kalmanova filtru,
- uvažování vícero konstelací pracujících v jedno- nebo dvou-frekvenčním módu.

Tyto studie by mohly vést k prokázání univerzálnosti metody AVAR pro detekci napadení.

Seznam MATLAB® skriptů

1. DIPLOMKA.m
2. plt_comp.m
3. geo2ecef.m
4. Motiv.m (3)
5. Generate_SPOOF_measurements.m (4.3)
6. AllanVar.m (5.1)
7. Generate_GNSS_measurements.m (6.3)
8. Generate_GNSS_offset_and_drift.m (6.2)
9. LS_PT_sol.m (6.4)

Odkazy

[1] R. Mit, „Top 10 GPS Spoofing Events in History,“ *Threat.Technology*, led. 2021.

[2] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela a A. D. Domínguez-Garca, „Spoofing GPS Receiver Clock Offset of Phasor Measurement Units,“ *IEEE Transactions on Power Systems*, roč. 28, č. 3, s. 3253–3262, srp. 2013.

[3] A. K. Mattei, W. M. Grady, P. J. Caspary a S. A. McBride, „Detection of time spoofing attacks on GPS synchronized phasor measurement units,“ in *2016 69th Annual Conference for Protective Relay Engineers (CPRE)*, 2016, s. 1–8. DOI: 10.1109/CPRE.2016.7914884.

[4] P. Y. Hwang a G. A. McGraw, „Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis,“ in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, 2014, s. 270–281.

[5] „Nvigaion,“ in *Oxford Dictionaries*, Oxford University Press, 2023. URL: https://languages.oup.com/.

[6] P. D. Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, Second Edition*. Artech House, 2013.

[7] E. D. Kaplan a C. Hegarty, *Understanding GPS/GNSS : Principles and Applications*. Artech House, 2017.

[8] T. Vlček, *GNSS Rušení*. České Vyysoké Učení Technické v Praze, 2017. URL: https://dspace.cvut.cz/bitstream/handle/10467/73192/F6-BP-2017-Vlcek-Tomas-GNSS%20ruseni.pdf?sequence=-1&isAllowed=y.

[9] J. Šebesta, *Globální Navigační Systémy*. Vysoké učení Technické v Brně, 2012. URL: https://www.natur.cuni.cz/geografie/geoinformatika-kartografie/ke-stazeni/vyuka/gps/ostatni-studijni-material/globalni-navigacni-systemy.

[10] J. Hadáček, *Odhad polohy objektu na základě satelitních měření s ohledem na integritu řešení*. Západočeská univerzita v Plzni, 2016. URL: https://dspace5.zcu.cz/bitstream/11025/23642/1/dp-final.pdf.

[11] R. B. Rustamov a A. M. Hashimov, *Multifunctional Operation and Application of GPS*. InTech, 2018.

[12] G. Seeber, *Satellite Geodesy 2nd Edition*. Walter De Gruyter, 2003.

[13] D. L. M. Warren a J. F. Raquet, „Broadcast vs. Precise GPS Ephemerides: A Historical Perspective,“ *GPS Solutions*, roč. 7, s. 151–156, pros. 2003.

[14] M. Joerger a B. Pervan, „Fault detection and exclusion using solution separation and chi-squared ARAIM,“ *IEEE Transactions on Aerospace and Electronic Systems*, roč. 52, s. 726–742, dub. 2016.

[15] J. Duník, *Identifikace Systémů a Filtrace*. Západočeská Univerzita v Plzni, 2018. URL: https://dspace5.zcu.cz/bitstream/11025/29322/3/Dun%c3%adk.pdf.

[16] K. Frončková, *Kalmanovy Filtry*. Univerzita Hradec Králové, 2022.

[17] O. Straka, *Teorie Odhadu a Zpracování Signálů*. Západočeská Univerzita v Plzni, dub. 2018.

[18] A. Jahromi, *GNSS Signal Authenticity Verification in the Presence of Structural Interference*. University of Calgary, 2013. URL: https://web.archive.org/web/20170809081851id_/http://theses.ucalgary.ca/jspui/bitstream/11023/927/2/ucalgary_2013_Jafarnia_Ali.pdf.

[19] M. L. Psiaki a T. E. Humphreys, „GNSS Spoofing and Detection,“ *Proceedings of the IEEE*, roč. 104, č. 6, s. 1258–1270, čvn. 2016.

[20] X. Zhu, Z. Lu, T. Hua, F. Yang, G. Tu a X. Chen, „A Novel GPS Meaconing Spoofing Detection Technique Based on Improved Ratio Combined with Carrier-to-Noise Moving Variance,“ *Electronics*, roč. 11, s. 738–738, ún. 2022.

[21] F. Šturc, *Detektor rušení GNSS*. České Vysoké Učení Technické v Praze, led. 2019. URL: https://dspace.cvut.cz/bitstream/handle/10467/80340/F3-DP-2019-Sturc-Filip-Detektor%20ruseni%20GNSS.pdf?sequence=-1&isAllowed=y.

[22] P. Mao, H. Yuan, X. Chen, Y. Gong, S. Li, R. Li, R. Luo, G. Zhao, C. Fu a J. Xu, „A GNSS Spoofing Detection and Direction-Finding Method Based on Low-Cost Commercial Board Components," *Remote Sensing*, roč. 15, s. 2781, led. 2023.

[23] L. Galleani a P. Tavella, „Time and the Kalman Filter," *IEEE Control Systems*, roč. 30, s. 44–65, 2010.

[24] O. Kost, *Odhad Kovariančních Matic Poruch Dynamického Systému*. Západočeská Univerzita v Plzni, květ. 2015. URL: https://dspace5.zcu.cz/bitstream/11025/17951/1/Diplomova%20prace%20Oliver%20Kost.pdf.

[25] J. Duník, O. Straka, M. Šimandl, O. Kost, J. Ajgl, M. Soták, R. Baránek a Z. Kaňa, „Estimation of State and Measurement Noise Characteristics," in *2015 18th International Conference on Information Fusion (Fusion)*, 2015, s. 1817–1824.

[26] R. G. Brown a P. Y. C. Hwang, *Introduction to Random Signals and Applied Kalman Filtering : with Matlab Exercises and Solutions*. John Wiley a Sons, Cop, 2012. URL: https://www.wiley.com/en-us/Introduction+to+Random+Signals+and+Applied+Kalman+Filtering+with+Matlab+Exercises%2C+4th+Edition-p-9780470609699.