Techniky pro detekci podvržených signálů v satelitní navigaci

Ondřej Dohnal[1]

1 Úvod

Satelitní navigace se stala nedílnou součástí moderní společnosti od svých počátků v 2. polovině 20. století. Systémy jako GPS (z angl. Global Positioning System) se původně vyvíjely pro vojenské účely, avšak s postupem času se staly dostupné i pro civilní sektor. Tato technologie umožňuje určovat přesnou polohu přijímače a globální čas pomocí signálů vysílaných z družic obíhajících Zemi po svých orbitách. S rostoucí spolehlivostí a dostupností se satelitní navigace stala klíčovou pro mnoho odvětví, včetně leteckého průmyslu, bankovnictví, telekomunikací, energetiky a plánování dopravy.

Nicméně s rozšířením používání satelitní navigace přicházejí i nové výzvy a bezpečnostní hrozby. Jednou z hlavních hrozeb je možnost spoofingu, nebo-li falšování signálů GPS. Ta může mít vážné následky pro integritu a spolehlivost těchto systémů, ale i mnohá odvětví, která na ně spoléhají. Příkladem takového útoku je incident z roku 2011, kdy Írán úspěšně zachytil americký bezpilotní dron díky falšovaným GPS signálům, viz (Mit , 2021).

Tato diplomová práce se tak zaměřuje na detekci hrozeb spojených s falšováním signálů GPS, s důrazem na oblast synchronizace času. Cílem je zkoumat metodu založenou na Alanově varianci (AVAR), která se ukázala jako účinná při detekci anomálií v pozičních datech. Metoda AVAR nabízí možnost detekce falšovaných signálů bez potřeby speciálního hardwaru či softwaru, což může být klíčové pro zlepšení bezpečnosti a spolehlivosti satelitní navigace i pro přijímače, které nemají specifické vybavení.

Výsledky této práce mohou přispět k vývoji nových technologií založených na satelitní navigaci s větší důvěryhodností a spolehlivostí. Díky lepšímu porozumění hrozbám spojeným s falšováním signálů GPS by mohlo dojít k většímu využití těchto systémů v kritických aplikacích a k dalšímu pokroku v oblasti bezpečnosti a ochrany dat.

2 Ilustrace metody pro detekci spoofingu

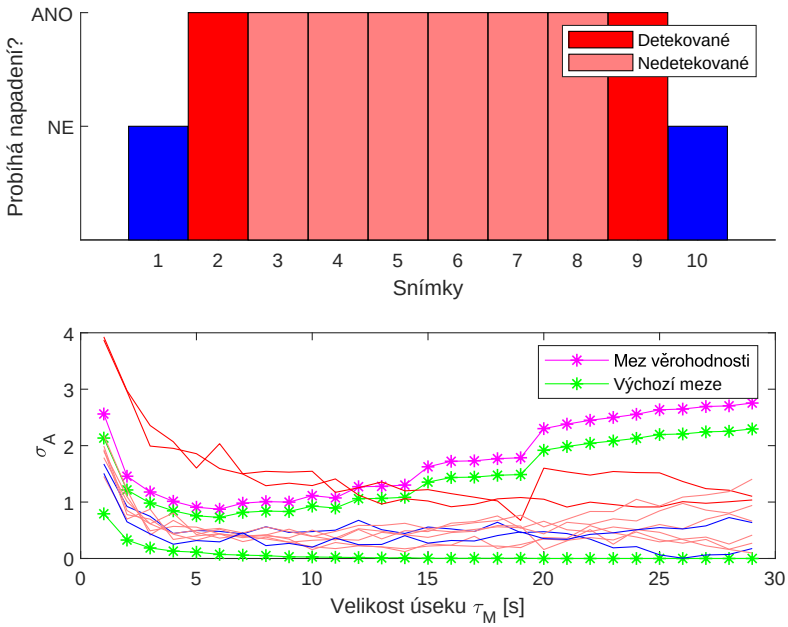
Uvažovaná metoda pro detekci spoofingu je založena na AVAR. Výpočet AVAR můžeme stručně ilustrovat pomocí dostupných $T+1$ odhadů času konstelace GPS $\widehat{t}^u_{GPS}$ poskytnutých přijímačem. Z těch jsme schopni určit drift satelitních hodin v časovém kroku k ze vztahu

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

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

Těchto T vypočtených hodnot driftu rozdělíme do $K = \frac{T}{M}$ úseků o M vzorcích. Z

[1] student navazujícího studijního programu Aplikované vědy a informatika, obor Kybernetika a řídící technika, specializace Automatické řízení a robotika, e-mail: doondra@students.zcu.cz



Obrázek 1: Detekce AVAR s nepřekrývajícími se úseky o délce $M = 60$ vzorků.

každého úseku je vypočten průměr hodnot $\overline{\delta t}_k(M)$, na jehož základě je spočtena AVAR pomocí

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

Takto získaná AVAR je pak porovnána s mezemi, které byly dopředu statisticky určeny v situaci, kdy jistě nebyl přijímač pod útokem či pod vlivem spoofingu.

Metoda je ilustrována na obrázku 1. Horní obrázek ukazuje simulace trvající $T = 600s$, která je rozdělena na 10 úseků po $60s$, kdy modrá barva značí, že spoofing nebyl aktivní (tj. GPS měření jsou správná), a červená barva značí oblast s aktivním útokem (spoofingem). Spodní obrázek pak ilustruje meze (zelená barva) a aktuální průběhy AVAR pro jednotlivé intervaly. Za povšimnutí stoji fakt, že spolehlivě jsou detekovány jen dva úseky, kdy byl spoofing aktivní. Důvod proč v ostatních úsecích spoofing nebyl detekován a jak detekci zajistit je s dalšími tématy řešen v diplomové práci, která je čtenářům volně přístupná na stránkách školy. Zároveň je však také budeme řešit a diskutovat v prezentaci, jejíž obsah je tímto rozšířeným abstraktem nastíněn.

Literatura

Groves, Paul D. (2013) *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, Second Edition*. Artech House.

Psiaki, Mark L. and Humphreys, Todd E. (2016) *GNSS Spoofing and Detection*. Proceedings of the IEEE, Volume 104, pp. 1258–1270.

Mit, Roi (2021) *Top 10 GPS Spoofing Events in History*. Threat.Technology.

Hwang, Patrick Y. and McGraw, Gary A. (2014) *Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis*. 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014, pp. 270-281.