

RADIAL2017

Real Time GNSS Signal Jamming/Spoofing Detection and Localization

Programm / Ausschreibung	ASAP, ASAP 13. Ausschreibung (2016)	Status	abgeschlossen
Projektstart	01.07.2017	Projektende	31.07.2019
Zeitraum	2017 - 2019	Projektlaufzeit	25 Monate
Keywords	GNSS, Spoofing / Interference detection		

Projektbeschreibung

Es ist allgemeiner Konsens, dass die Bedeutung satellitengestützter Positionierung (d. h. mit Hilfe von Global Navigation Satellite Systems (GNSS)) weiter zunehmen wird und die Abhängigkeit sicherheitskritischer Infrastruktur oder zukünftiger Technologien von GNSS bereits jetzt signifikant ist. GNSS ist aufgrund der geringen Signalstärken sehr störfähig. Insbesondere stellen „Jamming“ und „Spoofing“ potentielle Schwachstellen dar, deren Detektion und Unterdrückung (Mitigation) in den letzten Jahren durchaus intensiv erforscht wurden. Die Lokalisierung der Störquellen (insbesondere von GNSS-Spoofern) wurde hingegen weniger erforscht.

Es ist die Aufgabe der Regulierungsbehörden, die gesetzeskonforme Nutzung des Frequenzspektrums sicherzustellen. Dafür wird eine aufwändige Infrastruktur unterhalten, welche insbesondere das korrekte Funktionieren der mannigfaltigen Kommunikationsdienste sicherstellt. Diese Infrastruktur ist aber nur bedingt in der Lage Störungen der Satellitennavigation festzustellen, geschweige denn zu lokalisieren, da das vorhandene kommerziell verfügbare Equipment nur Kommunikationssignale detektiert, deren Modulation sich signifikant von Navigationssignalen unterscheidet und deren Sendeleistung auch weit über der für GNSS-Signale liegt. Das ist durch Präzedenzfälle belegt und wurde in Diskussionen mit namhaften Herstellern bestätigt.

Vor diesem Hintergrund soll ein existierender GNSS-Softwareempfänger über eine rotierende Antenne zu einer Echtzeit-GNSS-Monitoring-Station ausgebaut werden. Mit dem Hintergrund typischer Störszenarien und unter Berücksichtigung operationeller Aspekte sollen zum einen effizienten Algorithmen für den Softwareempfänger, als auch ein optimiertes mechanisches Design für die rotierende Antenne entwickelt werden. Insbesondere soll ein Verfahren zur Echtzeit-Lokalisierung von nicht-kooperativen Spoofern umgesetzt werden und die rotierende Antenne mit einer Richtantenne zur Lokalisierung von „Jamming“-Signalen erweitert werden.

Die Tauglichkeit, insbesondere die Messgenauigkeit des Systems soll im Rahmen einer Testkampagne experimentell für repräsentative Störquellen und Lokalisierungsverfahren bestimmt werden. Insbesondere sollen vorläufige Spezifikationen für die Azimut-Genauigkeit, Winkelauflösung, und horizontale Genauigkeit aufgestellt werden, wie auch die Fähigkeit, mehr als eine Störquelle zu lokalisieren. Die IGASPIN GmbH wird sich für die Tests um Zugang zu einem Truppenübungsplatz des

österreichischen Bundesheers bemühen, kann aber auch auf die Testgebiete der IFEN GmbH in Deutschland zurückgreifen. Angedacht sind ebenfalls Messkampagnen im GNSS-Testgebiet GATE (Berchtesgaden) wo unterschiedlichste Testszenarien unter möglichst realistischen Bedingungen ermöglicht werden können.

Abstract

It is commonly agreed that Global Navigation Satellite Systems (GNSS) will gain importance in future and the dependency of safety critical infrastructure or of future key technologies on GNSS will further increase. However, GNSS is known to be vulnerable especially by jamming or spoofing. Those threats have been investigated intensively during the past focusing of detection and mitigation. Localization of interfering signal sources (especially of GNSS spoofers) has received less research attention so far.

Regulatory authorities ensure proper use of the electromagnetic frequency spectrum. The authorities maintain a sophisticated infrastructure to ensure mainly proper functioning of the various communication services within a state. This infrastructure has only limited ability to be used to monitor navigation services like GNSS and is unable to localize those interfering sources. This is because the signal structure of a communication signal differs significantly from navigation signals and communications signals use signal powers far above the ones used for navigation signals. The inability of regulatory authorities to protect the GNSS frequency spectrum has been seen in several incidents during the past years.

The proposed project aims at developing a real-time GNSS monitoring station by using a GNSS software receiver together with a rotating dual purpose antenna. Considering typical jamming and spoofing scenarios yields the necessity to develop improved spoofer localization algorithms to cope with non-cooperative (low cost) spoofers. Furthermore, a new mechanical design shall be developed for the rotating antenna to include a directional antenna element to localize jamming signals.

The ability of the developed demonstrator system to detect and localize interfering sources shall be tested within a dedicated measurement campaign. Considering the complexity of the task due to the low signal power and the inevitable signal reflections, large efforts will be spent to characterize the system performance in terms of angular accuracy and horizontal localization performance. We also plan test to localize more than one interfering source. IGASPIN GmbH intends to perform the tests on a "Truppenübungsplatz" of the Federal Army of Austria. In case this is not possible, test areas of IFEN GmbH in Germany can be used. In particular, the German Galileo Test Bed (GATE) operated by IFEN offers the possibility to conduct a number of different tests under various realistic conditions.

Projektkoordinator

- IGASPIN GmbH

Projektpartner

- Schimpl Franz Josef
- Technische Universität Graz Institut für Geodäsie / Arbeitsgruppe Navigation