AMREI

Advanced Manipulating transReceiver Emitting Interference

Programm / Ausschreibung	FORTE, FORTE, FORTE - Kooperative F&E-Projekte KFE 2023	**Status**	laufend
Projektstart	01.02.2025	**Projektende**	31.01.2027
Zeitraum	2025 - 2027	**Projektlaufzeit**	24 Monate
Keywords	Jamming, Spoofing, Interference		

Projektbeschreibung

Für das GNSS Jamming und Spoofing existieren derzeit am Markt Geräte der ersten Generation. Meist sind diese auf GPS L1 beschränkt, weder miniaturisiert noch abstimmbar, oder können nicht phasensynchron oder gar in Echtzeit spoofen. Aktuell existieren beim BMLV/ÖBH unterschiedliche Jamming & Spoofing Systeme. Diese sind jedoch in ihrer Genauigkeit unter anderem dadurch eingeschränkt, dass die Sendeleistung manuell einzustellen ist, und somit die Handhabung umständlich und die Sendeleistung meist viel zu stark, wodurch das Spoofing von Empfängern erkennbar wird.
Es ist deshalb notwendig, wissenschaftliche und technische Untersuchungen für einen Jamming- und Spoofing Generators der 2. Generation zu starten. Hierbei sollen die Möglichkeiten hinsichtlich Smart Jamming und einer Interferenz -Cloud, sowie ein geeignetes einfaches, möglichst passives Verfahren und Sensor zur Bestimmung der Anfangsposition und Relativgeschwindigkeit des zu spoofenden Objektes aufweist (Kamera, Laser, Radar, hybride Sensorik, etc.) erforscht werden. Auf der innovativen Seite sollte ein Gerät der zweiten Generation in der Lage sein u. a. synchron mehrere Dienste ausführen können und von mehreren Geräten kombiniert zu spoofen. Dies ermöglicht es, die Herkunft des Signals zu verschleiern, und damit die Möglichkeiten von CRPAs (Controlled Reception Pattern Antenna) zur Erkennung von GNSS Spoofing bei dem Zielempfänger auszuhebeln.
Für die Entwicklung ist es deshalb unbedingt notwendig, die folgenden Forschungsfragen zu untersuchen und eine Lösung zu finden:
1. Untersuchungen zu einer so-genannten Interferenz-Cloud zur Verschleierung der Herkunft des gefälschten Signals
2. Integration von Smart Jamming für zielgerichtete Störungen von GNSS-Diensten
3. Entwicklung geeigneter Sensoren zur Bestimmung der Position und Geschwindigkeit des Ziel-Objekts
4. Implementierung von Multi-Frequenz-Jamming/Spoofing für eine breitere Angriffspalette
5. Reduzierung der Wartezeit zur NavBit-Prädiktion für verbessertes Spoofen
6. Entwicklung von Lösungen zur Vermeidung von „Self-spoofing“
Das Projekt wird in enger Kooperation mit BMLV/ÖBH durchgeführt, um die militärischen Anforderungen aufzunehmen und zu erfüllen, und zwar bezüglich des GNSS Jamming und Spoofing Generators selbst, sowie auch hinsichtlich eines Sensorsystem zum Tracken von Objekten, die für a) ein NavWar Center/ÖBH GNSS Test Center zur Integration und b) das Gefechtsfeld geeignet sind.

Die IGASPIN GmbH hat beste Voraussetzungen, das Vorhaben erfolgreich auszuführen. Ein Kerngebiet der Firma sind die GNSS-Interferenzen, wo sie seit mehreren Jahren forscht, entwickelt, Dienstleistungen ausführt und somit zahlreiche Erfahrungen sammeln konnte.
Das Joanneum Research bringt mit seinen Bereichen 3D Computer Vision und Navigation GNSS seine Kompetenz zur Untersuchung und Entwicklung eines geeigneten, möglichst passiven Trackingsystems des GNSS-Zielempfängers ein.
Sofern die o. g. Forschungsfragen erfolgreich gelöst werden können, sollte als Ziel ein GNSS Jamming und Spoofing Generators der zweiten Generation als Demonstrator mit dem Technology Readiness Level TRL 4: Versuchsaufbau, im Labor vorliegen. Erste Feldtests sind ebenfalls geplant.
Für diesen positiven Fall haben die IGASPIN und Joanneum Research einen Verwertungsplan entworfen, der u. a. vorsieht, dass die IGASPIN aus eigenen Mitteln den Prototyp zur Serienreife weiterentwickelt, und Joanneum Research seine Trackingmethodik an IGASPIN lizensiert.

Abstract

There are currently first-generation devices on the market for GNSS jamming and spoofing. Most of these are limited to GPS L1, are neither miniaturised nor tunable, or cannot spoof phase-synchronously or even in real time. The BMLV/ÖBH currently has various jamming and spoofing systems. However, these are limited in their accuracy by, among other things, the fact that the transmission power has to be set manually, making handling cumbersome and the transmission power usually far too high, which makes the spoofing of receivers recognisable.
It is therefore necessary to start scientific and technical investigations for a 2nd generation jamming and spoofing generator. Here, the possibilities with regard to smart jamming and an interference cloud, as well as a suitable simple, preferably passive method and sensor for determining the initial position and relative speed of the object to be spoofed (camera, laser, radar, hybrid sensor technology, etc.) should be researched. On the innovative side, a second-generation device should be able to perform several services synchronously and to spoof from several devices in combination. This would make it possible to disguise the origin of the signal, thereby overriding the ability of CRPAs (Controlled Reception Pattern Antenna) to detect GNSS spoofing at the target receiver.
It is therefore essential for the development to investigate the following research questions and find a solution:
1. investigations into a so-called interference cloud to conceal the origin of the falsified signal
2. integration of smart jamming for targeted interference of GNSS services
3. development of suitable sensors to determine the position and speed of the target object
4. implementation of multi-frequency jamming/spoofing for a broader range of attacks
5. reduction of the waiting time for NavBit prediction for improved spoofing
6. development of solutions to avoid self-spoofing
The project will be carried out in close cooperation with BMLV/ÖBH to address and fulfil the military requirements regarding the GNSS jamming and spoofing generator itself, as well as a sensor system for tracking objects suitable for a) a NavWar Center/ÖBH GNSS Test Center for integration and b) the battlefield.
IGASPIN GmbH is ideally placed to successfully realise the project. One of the company's core areas is GNSS interference, where it has been researching, developing and providing services for several years and has thus been able to gather a wealth of experience.
With its 3D Computer Vision and GNSS Navigation divisions, Joanneum Research is contributing its expertise in the investigation and development of a suitable, preferably passive tracking system for the GNSS target receiver.
If the above-mentioned research questions can be successfully solved, the goal should be a second-generation GNSS

jamming and spoofing generator as a demonstrator with the Technology Readiness Level TRL 4: test setup, in the laboratory. Initial field tests are also planned.
In this positive case, IGASPIN and Joanneum Research have drawn up a commercialisation plan which, among other things, envisages IGASPIN using its own funds to develop the prototype to series maturity and Joanneum Research licensing its tracking methodology to IGASPIN.

Projektkoordinator

- IGASPIN GmbH

Projektpartner

- Bundesministerium für Landesverteidigung
- JOANNEUM RESEARCH Forschungsgesellschaft mbH