GNSS-Sicherheit – Chancen und Risiken
GNSS-Safety – Opportunities and Risks

Philipp Berglez, Graz

Kurzfassung

Die Verwendung von Globalen Navigationssatellitensystemen (GNSS) und die damit verbundene ständige Verfügbarkeit einer Position sowie einer genauen Zeitmessung werden in vielen Bereichen des täglichen Lebens immer mehr zur Selbstverständlichkeit. Durch die stetig steigende Zahl von Anwendungen und Nutzern wird es zunehmend wichtiger, sich nicht nur über die Chancen, sondern auch über die Schwächen und Risiken einer satellitengestützten Positionsbestimmung Gedanken zu machen. Viele Anwender sind sich des Gefahrenpotentials und dessen Auswirkungen derzeit nicht bewusst. In den letzten Jahren wurden GNSS-Anwendungen vermehrt das Ziel von Störattacken. Studien belegen, dass durch Störsignale beträchtliche wirtschaftliche aber auch materielle Schäden entstehen können, denn Störsignale können den Einsatz von GNSS signifikant beeinflussen. Dies kann von einer schlechteren Positionsgenauigkeit bis zu einer falschen Position oder zum totalen Ausfall der Positionierung führen. Neben unbeabsichtigten Störeinflüssen stellen absichtliche Störungen der GNSS-Signale ein besonders hohes Gefahrenpotential dar. Extrem gefährlich sind dabei Attacken von Spoofern, die GNSS-Signale imitieren, um so die berechnete Positions- und Zeitinformation des GNSS-Empfängers gezielt zu manipulieren. Die vorliegende Arbeit beschreibt das Gefahrenpotential von beabsichtigten GNSS-Signalstörungen. Die Auswirkungen von Jamming und Spoofing werden diskutiert und mögliche Gegenmaßnahmen aufgezeigt. Abschließend wird die besondere Stärke des Europäischen Satellitennavigationssystems Galileo im Falle von Jamming und Spoofing beschrieben.

Schlüsselwörter: GNSS, Interferenz, Jamming, Spoofing

Abstract

The use of Global Navigation Satellite Systems (GNSS) and the associated permanent availability of position and precise time measurement as well become more and more a matter of course in many areas of everyday life. Due to the increasing number of applications and users, it is becoming more important to consider not only the opportunities, but also the weaknesses and risks of a satellite-based position determination. Currently, many users are unaware of the potential threats and impacts. In recent years, GNSS applications have become the target of interference attacks. Studies show that interference can cause considerable economic but also material damage, as interference signals can significantly influence the operation of GNSS. This can lead to degraded position accuracies or to a total failure of the positioning. In addition to unintentional interference, intentional interference of GNSS signals represents a high threat potential. Particularly dangerous are attacks by spoofers imitating GNSS signals, in order to specifically manipulate the calculated position and time solution of the GNSS receiver. The present work describes the potential threat of intentional GNSS interference. The effects of jamming and spoofing are discussed and possible counter-measures are presented. Finally, the added value of the European satellite navigation system Galileo in the case of jamming and spoofing is described.

Keywords: GNSS, Interference, Jamming, Spoofing

1. Einleitung

Am 15. Dezember 2016 gab die Europäischen Kommission offiziell bekannt, dass die ersten drei Dienste (Open Service, Search and Rescue Service und Public Regulated Service) des europäischen Satellitennavigationssystems Galileo für Navigationszwecke zur Verfügung stehen [1].

Das bedeutet, dass nun Bürger, Unternehmen und Behörden die Galileo Signale, wenn auch derzeit nur limitiert, nutzen können. Damit reiht sich Galileo in die Liste globaler Satellitennavigationssysteme (GNSS) ein und trägt mit seinem zivilen Konzept und seinen optimierten Signalstrukturen wesentlich zur Steigerung der Genauigkeit, Verfügbarkeit und Integrität einer satellitengestützten Position bei. Seit vielen Jahren ist die Verfügbarkeit und fehlerfreie Funktion von GNSS für die stetig steigende Zahl von Nutzern selbstverständlich. Das Bewusstsein der Anwender für die Störanfälligkeit der GNSS-Signale und die damit verbundenen Auswirkungen ist jedoch noch

gering. Neben unbeabsichtigten Störeinflüssen stellen absichtliche Störungen der GNSS-Signale ein besonders hohes Gefahrenpotential dar. In den letzten Jahren waren GNSS-Anwendungen vermehrt das Ziel von Störattacken. Die Auswirkungen solcher Störattacken reichen von einer schlechteren Positionsgenauigkeit bis zu einer falschen Positionsangabe oder bis zum totalen Ausfall der Positionierung. Erst durch diese Vorfälle begann eine allmähliche Paradigmenverschiebung und Anwender beginnen sich nun über die Schwächen und Risiken einer satellitengestützten Position Gedanken zu machen.

Der Artikel beschreibt das Bedrohungspotential von absichtlichen GNSS-Signalstörungen sowie die Auswirkungen von Jamming und Spoofing. Durch eine rasche und zuverlässige Detektion der Störsender können sowohl die Zuverlässigkeit als auch die Integrität erheblich verbessert und somit auch das Vertrauen der Nutzer in diese Technologie gesteigert werden. Die Detektion ist der erste notwendige Schritt, um wirksame Gegenmaßnahmen einleiten zu können. Durch ein Netz von Überwachungsmodulen ist es möglich, die Störquelle zu lokalisieren und somit einerseits die Quelle zu eliminieren und andererseits eine Strafverfolgung einzuleiten. Besonders gefährlich sind dabei Attacken von Spoofern, die GNSS-Signale imitieren, um gezielt die berechnete Positions- und Zeitinformation des GNSS-Empfängers zu manipulieren. Der Artikel zeigt, wie einfach Spoofing zu realisieren ist, welche Auswirkungen zu erwarten sind und welche Gegenmaßnahmen getroffen werden können. Abschließend wird der Mehrwert des Europäischen Satellitennavigationssystems Galileo im Fall von Jamming und Spoofing beschrieben.

Die hier beschriebene Forschungsarbeit wurde im Rahmen der von der Forschungsförderungsgesellschaft (FFG) geförderten Projekte „Detection, countermeasures and demonstration of GNSS spoofing“ (DECODE) [2] und „Impacts and Countermeasures of Austrian PRS application scenarios in GNSS denied environments (PRSAustria)“ [3] durchgeführt. Das Ziel des derzeit laufenden Projekts DECODE ist die Implementierung und Erprobung von leistungsfähigen Algorithmen zur Erkennung und Minderung des Effekts von GNSS Spoofing-Attacken. PRSAustria beschäftigt sich mit der Untersuchung der realen Auswirkungen von GNSS-Störsignalen auf die satellitengestützte Positionierung und im Speziellen auf die Leistungsfähigkeit des Galileo Public Regulated Service. Dieser Artikel spiegelt die wichtigsten Erkenntnisse wieder, die vom Autor im Rahmen eines Vortrags für das OVN Navigations-Get-Together publiziert wurden [4].

2. Wir alle sind Navigatoren

In den frühen Morgenstunden des 2. Mai 2000 wurde die bis dahin aktive künstliche Verschlechterung des amerikanischen Global Positioning System (GPS) Signals deaktiviert. Die Deaktivierung von Selective Availability (SA) und Anti-Spoofing (AS) führte zu einer deutlichen Verbesserung der Positionierungsgenauigkeit im Einsatz von GNSS in unserem täglichen Leben. Abbildung 1 zeigt die signifikante Steigerung der Positionierungsgenauigkeit in der Höhe durch das Abschalten der künstlichen Verschlechterung, wie sie am 2. Mai 2000 um 04:00 UTC an der GPS Permanentstation Graz Lustbühel zu beobachten war.

Seit diesem Zeitpunkt wurden satellitengestützte Positions- und Zeitinformationen, sowie damit verbunden Orientierung und Navigation immer tiefer in unserem täglichen Leben verankert. Wie tief das bereits der Fall ist, zeigt der Marktbericht der Europäischen GNSS Agency GSA aus dem Jahr 2015 [5]. Der Bericht schätzt, dass derzeit weltweit ca. 4,5 Milliarden GNSS-Empfänger im Einsatz sind. Im Jahr 2019 sollen es bereits sieben Milliarden, also in etwa ein Empfänger pro Erdenbürger, sein. Mittlerweile ist auch GNSS zu einem wichtigen Wirtschaftsfaktor geworden. Eine Studie aus dem Jahr 2011 geht davon aus, dass 6-7 % des Bruttoinlandprodukts (ca. 800

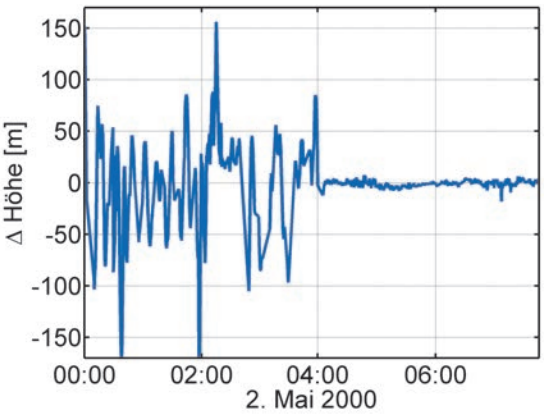

Abb. 1: Steigerung der GPS Positionierungsgenauigkeit durch Deaktivierung von Selective Availability und Anti-Spoofing am 2. Mai 2000

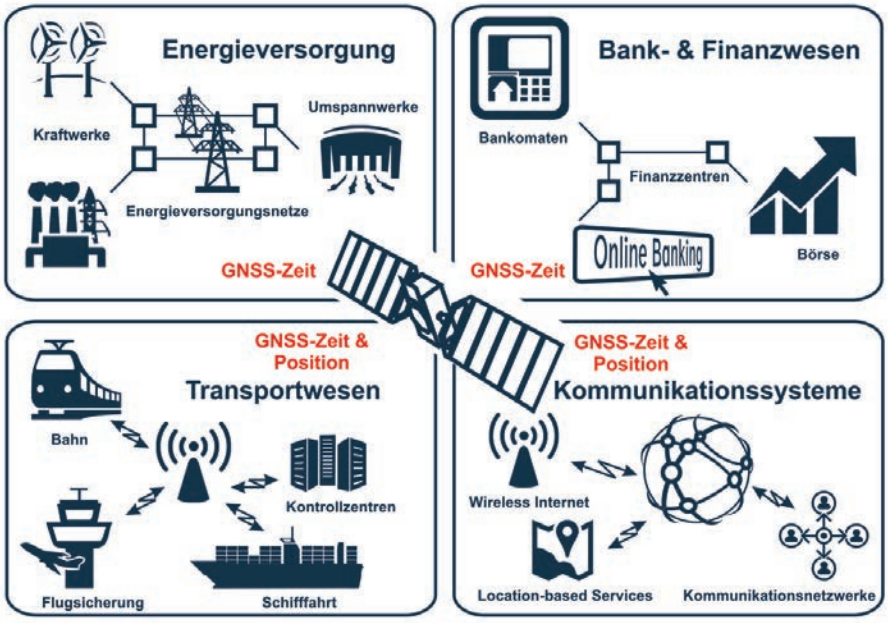

Abb. 2: GNSS Abhängigkeiten

Milliarden Euro) der westlichen Welt direkt oder indirekt von Satellitennavigation abhängig sind [6].

2.1 GNSS-Anwendungen und Fehlerquellen

GNSS-Empfänger stellen abgesehen von der geographischen Breite und Länge sowie der Höhe eine vierte wesentliche Dimension – die Zeit – zur Verfügung. Mit Hilfe der von den Satelliten abgestrahlten Signale ist es möglich, die Zeit mit einem GNSS-Empfänger zu bestimmen [7]. Dies ermöglicht es den Nutzern, eine hochgenaue Zeitinformation jederzeit, global und mit einer Genauigkeit von weniger als einer Nanosekunde zu erhalten. Die präzise Zeitbestimmung ist weltweit von entscheidender Bedeutung für eine Vielzahl von Anwendungen und Verfahren. Abbildung 2 zeigt anhand einiger Beispiele die Abhängigkeit unserer heutigen Gesellschaft von GNSS.

Sieht man sich die Bandbreite von derzeitigen GNSS-Anwendungen an, so erkennt man, dass GNSS nicht nur im Bereich Location-based Services oder Geodäsie eingesetzt wird, sondern auch in vielen anderen Bereichen. Kommunikationssysteme, Stromnetze und Finanznetzwerke verlassen sich alle auf präzise Zeitinformation für die Synchronisation. Die freie Verfügbarkeit einer GNSS-Zeit bedeutet für Unternehmen Kosteneinsparungen und Vorteile hinsichtlich der Effizienz. So verwenden beispielsweise Mobilfunknetzwerke eine GNSS-Zeit, um Basisstationen zu synchronisieren. Dies ermöglicht eine effizientere Nutzung des begrenzt verfügbaren Frequenzspektrums [8]. Weltweit nutzen Finanzdienstleister GNSS-Zeitstempel um Finanztransaktionen zu koordinieren, zu protokollieren und nachvollziehbar zu machen. Verteilte Netzwerke von Sensoren, die koordiniert werden müssen um genaue Ergebnisse zu erzielen, bedürfen einer Zeitquelle, die an allen Stellen eine hohe Genauigkeit garantieren kann. GNSS-basiertes Timing ist für Anwendungen von Bedeutung, bei denen genaue Zeitpunkte von Geräten, die über weite geographische Gebiete verteilt sind, erforderlich sind. Die gesamte Transportbranche stützt sich ebenfalls auf GNSS – sei es bei der Verfolgung von Gütern und Fahrzeugen oder der Steuerung dieser.

Das bedeutet aber auch, dass selbst geringe Störungen von GNSS gravierende Auswirkung haben können. Die Herausforderung bei GNSS besteht darin, dass die Signale zur Positionsberechnung, welche mit sehr geringer Leistung abgestrahlt werden, einen sehr weiten Weg zurücklegen und diese beim Empfänger bezüglich ihrer Leistung unter dem thermischen Rauschen ankommen. Vergleichbar wäre dies mit einer handelsüblichen Glühbirne, die in Shanghai eingeschalten wird und deren Licht man in Wien zu erkennen versucht. Neben der geringen Signal-

leistung gibt es natürlich bei einem so komplexen System genügend weitere Fehlerquellen. Hier anzuführen wären: Satellitenabhängige Fehler, Ausbreitungsfehler, empfängerabhängige Fehler [7]. Während es für diese Arten von Fehlerquellen genügend Auswertealgorithmen und Korrekturmodelle gibt, rückt das Thema Interferenz immer mehr in den Vordergrund.

3. GNSS-Interferenz

Interferenz beschreibt den Effekt der Amplitudenänderung, der durch Überlagerung von zwei oder mehreren elektromagnetischen Wellen entsteht [8]. Bei Interferenz wird generell zwischen absichtlichen und unbeabsichtigten Störungen unterschieden. Zur Gruppe der unbeabsichtigten Störungen gehören neben der durch die Natur (z.B. Ionosphäre) hervorgerufenen Interferenz die Signale, die außerhalb (Out-of-band) oder innerhalb (In-band) der GNSS-Frequenzbänder auftauchen. Die Signale werden von der International Telecommunication Union (ITU) streng reguliert. In Bezug auf GNSS sind Out-of-Band-Signale beispielsweise terrestrische Funksysteme. In-Band-Interferenz wird zum Beispiel durch andere Globale Satellitennavigationssysteme (z.B. GPS und Galileo) oder durch Signale des gleichen Systems (z.B. zivile und militärische Signale bei GPS) verursacht. Aufgrund der strikten Regularien und des Signaldesigns können diese Effekte beinahe ganz vermieden werden. Im Gegensatz dazu sind absichtliche Störungen ein viel größeres Problem. Der Volpe-Bericht aus dem Jahr 2000 kategorisiert absichtliche Störungen in Jamming, Spoofing und Meaconing [9].

Jamming bezeichnet das bewusste Aussenden eines starken, rauschartigen Störsignals mit dem Ziel, die GNSS-Signale zu verdrängen und damit eine Verschlechterung der Positionierungsgenauigkeit oder einen Ausfall der Positionierung herbeizuführen. Das Aussenden von falschen GNSS-Signalen mit dem Ziel, die berechnete Positions- und Zeitlösung des Nutzers zu kontrollieren, wird als Spoofing bezeichnet. Meaconing, ähnlich dem Spoofing, bezeichnet das Verfahren zur Generierung eines künstlichen Mehrwegeffekts mit dem Ziel, durch zeitversetztes Aussenden von zuvor aufgezeichneten GNSS-Signalen die Positionslösung von der tatsächlichen Position wegzuschieben. An dieser Stelle sei angemerkt, dass das absichtliche Aussenden von Störsignalen rechtswidrig ist und strafrechtlich verfolgt wird.

3.1 Jamming

Jamming zielt darauf ab, den Empfänger an der Berechnung einer Positionslösung zu hindern oder diese zu verschlechtern. Durch das Aussenden eines starken Störsignals verliert der Empfänger das Tracking und wird an der Re-Akquisition der GNSS-Signale gehindert. Die GNSS-Signale sind aufgrund ihrer geringen Sendeleistung und der großen Distanz zwischen Satellit und Empfänger besonders anfällig für Störungen. Theoretisch würde ein 10-Milliwatt-Störsender in 10 Kilometer Entfernung ausreichen, um einen GPS C/A-Code Empfänger an der Positionsberechnung zu hindern [10].

Im zivilen Bereich werden Jammer, auch Personal Privacy Devices genannt, von unterschiedlichsten Nutzergruppen zum Schutz der Privatsphäre, für kriminelle Aktivitäten oder aber auch zum Schutz kritischer Infrastruktur eingesetzt. Das Risiko bzw. die Gefahr von absichtlichen Störungen ist schon jetzt beträchtlich. Dass Störsender keine theoretische Gefahr darstellen, sondern eine reale, zeigen unzählige Zwischenfälle in den letzten Jahren [11]. So wurden Ground-based Augmentation Systems (GBAS) in der Nähe von amerikanischen und taiwanesischen Flughäfen bis zu 117-mal pro Tag gestört, meist hervorgerufen durch LKW- und Taxifahrer, die ihre Fahrtrouten verheimlichen wollten. In Südkorea führten Störattacken durch den nördlichen Nachbarstaat zu Überlegungen hinsichtlich Alternativen zu GNSS. Drohnen wurden durch Spoofing zum Landen gezwungen, und eine 65 m Megayacht vom Kurs abgebracht. Im Jahr 2007 lief ein US Kriegsschiff in den Hafen von San Diego ein und hatte dabei seine Störsender noch aktiviert. Dies führte zu einem Ausfall der Notfallpager, zu einer Störung des Verkehrsmanagementsystems und zu einem Ausfall der Geldautomaten.

Diese Störsender sind günstig zu erwerben und sehr effektiv. Je nach spektraler Charakteristik des Störsignals können verschiedene Arten von Jammern unterschieden werden. Die häufigsten Typen von Jammern sind Single Tone Amplitude Modulation, Single Tone Frequency Modulation, Continuous Wave und Swept Continuous Wave. Zusätzlich kann jeder genannte Typ auch als gepulstes Signal mit einer bestimmten Pulsdauer und Wiederholrate vorkommen [12].

Störsignale wirken sich sowohl auf die empfangene Signalstärke als auch auf die Signalqualität aus. Sowohl das Signal-Rausch-Verhältnis (SNR) als auch die Carrier-to-noise-density ratio (C/N0)

wird geringer. Damit verbunden ist eine längere Akquisitionsdauer der Signale (sofern die Akquisition überhaupt möglich ist) und somit auch eine längere Zeitspanne, bis eine Positionsbestimmung erfolgen kann. Auch die Anzahl der Satelliten, die im Tracking sind, reduziert sich und somit stehen weniger Beobachtungen zur Positionslösung zur Verfügung. Die Genauigkeit der Pseudostrecken- und Phasenmessungen wird deutlich herabgesetzt und bewirkt eine wesentliche Verschlechterung der Positionierungsgenauigkeit bis hin zum totalen Ausfall der Positionierung. Im Fall von Phasenmessungen treten vermehrt Phasensprünge auf.

Der Einfluss eines Störsignals auf die Positionsgenauigkeit kann über die Tracking-Genauigkeit des Empfängers abgeschätzt werden. Die Tracking-Genauigkeit wiederum ist eine Funktion des effektiven Verhältnisses der Signalleistung des GNSS-Signals zur Rauschleistungsdichte. Die Rauschleistung besteht im Gegensatz dazu aus thermischem Rauschen, von dem angenommen wird, dass es sich um weißes Rauschen handelt und alle übrigen Signale und Störquellen beinhaltet. Die Rauschleistung wird unter Verwendung der spektralen Leistungsdichte (Power Spectral Density (PSD)) der jeweiligen Signale modelliert. Die PSD eines Signals kann entweder analytisch, basierend auf der Signalcharakteristik, oder auf Grundlage einer Zeitbereichsdarstellung des Signals gemessen oder berechnet werden. Die theoretischen Grundlagen dazu können in [13], [14], [15] und [16] nachgelesen werden.

TeleConsult Austria und der Autor im speziellen beschäftigen sich schon seit einigen Jahren mit dem Thema Detektion und Klassifikation von Störsignalen und den entsprechenden Gegenmaßnahmen. Im Rahmen von einigen Forschungsprojekten wurden die Auswirkungen von Jamming und Spoofing untersucht und dabei ein System zur Detektion, Klassifizierung und Lokalisierung von Störsendern entwickelt. Das GIDAS System (GNSS Interference Detection & Analysis System) ermöglicht eine zuverlässige Detektion, Klassifikation und Lokalisierung von GNSS-Störungen in Echtzeit im L1/E1 Signalband. Detektion, Klassifikation und Lokalisierung sind die ersten wesentlichen Schritte, um der Gefahr des Jammings zu begegnen und um Gegenmaßnahme einleiten zu können [17].

Die Detektion kann über unterschiedlichste Verfahren erfolgen. Die bekanntesten Methoden basieren auf dem Monitoring des Spektrums sowie des Zeitbereichs des empfangenen Signals, der Überwachung des Signal-Rausch-Verhältnisses und der Tracking-Genauigkeit, sowie der Detektion von Ausreißern in den Messungen (Pseudostrecken und Phasen) und in der Positionslösung. Ein solches Monitoring erfordert die Möglichkeit, auf die Informationen der Module eines Empfängers zugreifen zu können. Zu diesem Zweck wird ein software-basierter GNSS-Empfänger (SDR) verwendet.

Der Unterschied zwischen einem softwarebasierten und einem herkömmlichen Empfänger besteht darin, dass die rechenintensive Signalverarbeitung, also die Akquisition und das Tracking, nicht mehr in der Hardware implementiert ist, sondern fast zur Gänze durch Software realisiert wird. Dieser Ansatz hat den Vorteil, dass es einerseits sehr einfach ist, neue Signalverarbeitungsalgorithmen zu implementieren und zu testen, aber andererseits auch möglich ist, auf alle Informationen und Zwischenergebnisse (z.B. digitales empfangenes Signal, C/N0, Tracking-Genauigkeit, Messungen, etc.) zuzugreifen. Dadurch ist es möglich, verschiedene Detektionsalgorithmen sehr einfach in einem SDR zu implementieren. In der Praxis hat sich eine Kombination der unterschiedlichsten Methoden als besonders effizient herausgestellt.

Wurde ein Störer detektiert, so erfolgt die Klassifizierung hinsichtlich seiner Signaleigenschaften – wie Sendefrequenz, Leistung, Typ. Die Klassifizierung erfolgt unter anderem über die Short-Time-Fourier-Transform (STFT) des Signals und einen adaptiven Notch-Filter [18]. Wurde der Störer klassifiziert, so kann er in einem nächsten Schritt mit unterschiedlichsten Verfahren unter Verwendung mehrerer Monitoring Stationen lokalisiert werden. Neben Time of Arrival und Angle of Arrival gibt es auch die Möglichkeit, ihn über die empfangene Signalleistung mittels Triangulation zu lokalisieren. Basierend auf der Klassifizierung ist es möglich Gegenmaßnahmen vorzunehmen. Gegenmaßnahmen können sowohl im Frequenzbereich als auch im Zeitbereich vorgenommen werden. Maßnahmen im Frequenzbereich versuchen das Störsignal herauszufiltern und dabei soweit wie möglich das GNSS-Signal zu erhalten. Dies funktioniert allerdings nur, wenn die Bandbreite des Störsignals im Vergleich zum GNSS-Signal sehr gering ist. Typischerweise werden dazu adaptive Filter eingesetzt. Im Fall von gepulsten Jammern wird versucht im Zeitbereich das Störsignal herauszuschneiden bzw. durch eine adaptierte Quantisierung den Einfluss zu minimie-

ren. Dies gelingt jedoch nur, wenn die Pulsdauer und die Wiederholrate nicht zu hoch sind. In modernen Mehr-Frequenz-Empfängern sind solche Verfahren auf Grund der auftretenden Interferenz mit terrestrischen Radionavigationssystemen (z.B. DME, TACAN) schon implementiert. Eine weitere Methode wäre die Verwendung von mehreren Antennen mit der Möglichkeit, ein Beamforming zu machen. Dabei werden die einzelnen Antennen miteinander verbunden und mittels Signalverarbeitung die Empfangsrichtung des Störsignals bestimmt. Damit ist es möglich, die Verstärkung der Antenne in dieser Richtung soweit zu reduzieren, dass kein Störsignal mehr empfangen wird.

Im Zuge der GIDAS-Entwicklung und der Tests wurden mehrere Messkampagnen in Österreich und in der Ukraine durchgeführt. Während der Kampagnen in Österreich wurden in der Nähe von Graz und Wien entlang von Autobahnen und in der Umgebung des Flughafens Graz binnen weniger Stunden zahlreiche Jammer detektiert, klassifiziert und auch lokalisiert [19]. Im Rahmen des aktuellen Forschungsprojekts PRSAustria werden derzeit die Auswirkungen von Störsignalen und mögliche Gegenmaßnahmen unter Verwendung unterschiedlicher Jammer von TeleConsult Austria in Kooperation mit Brimatech Services und dem Bundesministerium für Landesverteidigung und Sport untersucht. Ziel des Projekts ist es, den Mehrwert von Galileo Public Regulated Service (PRS) aufzuzeigen und anhand von konkreten PRS-Anwendungsszenarien zu testen.

Abbildung 3 zeigt den totalen Ausfall der GNSS-gestützten Positionierung im Falle eines zivilen Jammers.

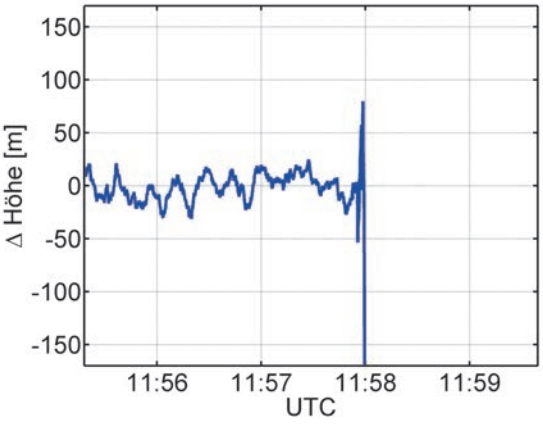

Abb. 3: Totaler Ausfall der Positionslösung

Sowohl die Lage- als auch die Höhenabweichungen stiegen binnen weniger Sekunden an und kurz darauf kam es zu einem totalen Ausfall der satellitengestützten Positionierung. Erst als das Jamming wieder deaktiviert wurde, konnte eine Position berechnet werden.

3.2 GNSS Spoofing

Spoofing bedeutet so viel wie Manipulation, Verschleierung oder Vertauschen. Ziel von Spoofing ist es, durch gezielt manipulierte Signale einen Empfänger auf eine falsche Position zu setzen oder das Zeitsignal gezielt zu manipulieren. Meaconing kann als einfachste Form von Spoofing angesehen werden. Dabei werden vom Angreifer echte GNSS-Signale aufgezeichnet und mit einer geringen zeitlichen Verzögerung und mit etwas höherer Leistung im Vergleich zum ursprünglichen Signal wieder abgestrahlt. Dies führt dazu, dass der attackierte Empfänger die zeitlich verzögerten Signale anstelle der echten prozessiert und somit eine falsche Positionslösung, nämlich jene, an der die Signale aufgezeichnet wurden, berechnet. Der Unterschied zu Spoofing ist, dass ein Spoofer GNSS-Signale, die zu einer zuvor vorgegebenen Empfängerposition passen, generiert und diese, mit etwas höherer Leistung, aussendet.

In Abhängigkeit des Aufwands wird Spoofing in einfache, erweiterte und anspruchsvolle Attacken klassifiziert [20]. Für eine einfache Spoofing-Attacke kann ein kommerzieller GNSS-Simulator zusammen mit einem RF (Radio Frequency) Verstärker und einer Antenne kombiniert werden. Mit Hilfe des Simulators werden GNSS-Signale für eine zuvor eingestellte Satellitenkonstellation und Empfängerposition generiert. Für den attackierten Empfänger sieht das generierte Spoofing-Signal zu Beginn der Attacke wie Rauschen aus. Der Empfänger muss, um auf das Spoofing-Signal zu reagieren, zuerst das Tracking der realen Signale verlieren. Dies kann entweder über ein sehr leistungsstarkes Spoofing-Signal erfolgen oder durch eine kurze Jammer-Attacke. Sobald der Empfänger nach der Jammer-Attacke versucht, die Signale wieder zu akquirieren, wird er das Spoofing-Signal nutzen. Solche Attacken sind relativ einfach zu erkennen, da das echte Signal und das Spoofing-Signal nicht synchronisiert sind und es zu signifikanten Sprüngen sowohl in der empfangenen Leistung als auch in den Tracking Loops, den Messungen und der Position kommt.

Bei einer erweiterten Spoofing-Attacke wird unter Verwendung eines GNSS-Empfängers ein zum

realen GNSS-Signal synchronisiertes Spoofing-Signal erzeugt und erst nach der erfolgreichen Übernahme des attackierten Empfängers durch den Spoofer die Position- und Zeitinformation verändert. Dies ist technisch sehr anspruchsvoll und erfordert neben einer aufwändigen Hardware auch sehr viel Wissen im Bereich GNSS-Algorithmik und Softwareentwicklung. Voraussetzung für diese Art von Spoofing ist, dass die aktuelle Position, Geschwindigkeit und Zeitinformation des zu spoofenden Empfängers mit einer hinreichenden Genauigkeit bekannt sind. Information über die aktuelle GNSS-Konstellation ist ebenfalls von Vorteil. Dadurch kann zu Beginn der Attacke ein im Vergleich zum echten GNSS-Signal im Sinne der Code- und Phasenverschiebung plausibles Signal im zu spoofenden Empfänger erzeugt werden. Dadurch fällt im Idealfall die Korrelationsfunktion des echten GNSS-Signals und des Spoofing-Signals mit dem lokalen Code im Empfänger zusammen. Diese Art von Spoofing ist schwerer zu detektieren und geeignete Gegenmaßnahmen erfordern erheblichen Aufwand. Da alle Spoofing-Signale von einer Antenne abgestrahlt werden ist es möglich die Empfangsrichtung der Signale mit Hilfe von Antennen-Arrays und Beamforming-Techniken zu bestimmen und gegebenenfalls ein Nullsteering (d.h. die Antenne wird in dieser Richtung „blind“ gemacht) durchzuführen und somit das Spoofing-Signal herauszufiltern. Dies wird bei der anspruchsvollen Art von Spoofing durch den Einsatz mehrerer Sendeantennen versucht nachzuahmen. Es erfordert aber einen erheblichen Mehraufwand an Technik und ermöglicht auch nur ein örtlich begrenztes Spoofing.

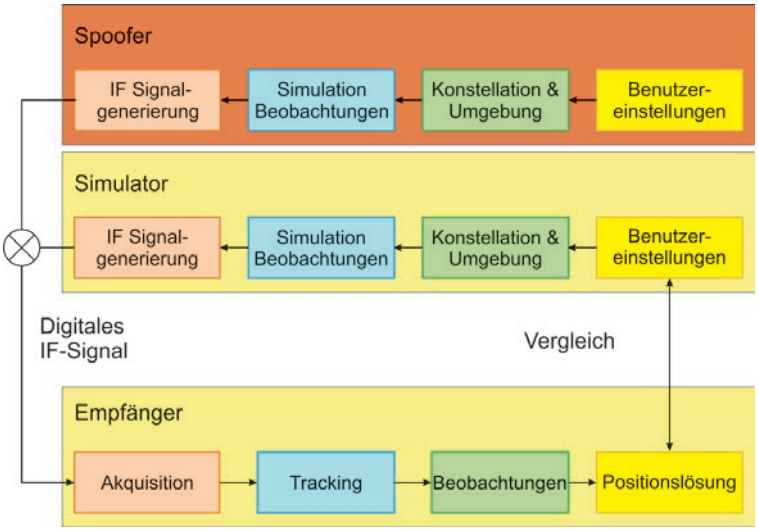

Abb. 4: Spoofing-Simulation Setup

3.3 Spoofing-Simulation

Im Rahmen des laufenden Forschungsprojekts DECODE werden, gemeinsam mit dem Institut Electronic Engineering der Fachhochschule Joanneum, aktuell die Auswirkungen von Spoofing untersucht sowie Detektionsstrategien und Gegenmaßnahmen hinsichtlich Spoofing anhand von Spoofing-Simulationen, basierend auf digitalen GNSS-Signalen, entwickelt. Für die Simulation wird der von TeleConsult Austria entwickelte GNSS-Simulator (GIPSIE – GNSS multi-system performance simulation environment) verwendet. Der Simulator dient einerseits zur Simulation von realen GNSS-Signalen und andererseits zur Simulation der Spoofing-Signale. Bei den Signalen handelt es sich um digitale Intermediate-Frequency (IF) Signale, die in den software-basierten GNSS-Empfänger eingespielt werden. Abbildung 4 zeigt die Simulationsumgebung bestehend aus einem SDR (dem zu spoofenden Empfänger) und zwei Simulatoren, wovon einer die Realität simuliert und der zweite den Spoofer darstellt.

Als Ziel der simulierten Spoofing-Attacke wurde das Bürogebäude der TeleConsult Austria (TCA) in Graz ausgewählt. TCA verfügt über zwei Dachantennen für GNSS-Referenzmessungen. Ziel

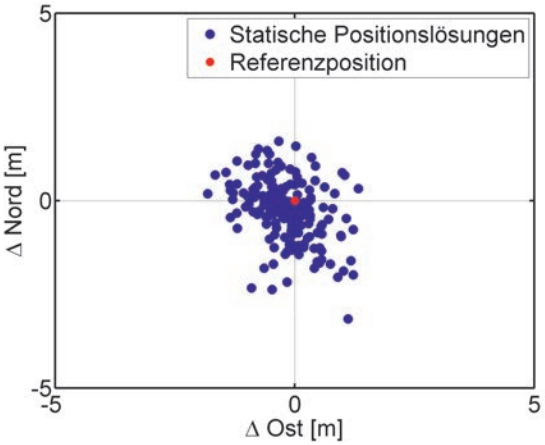

Abb. 5: Statische Positionslösungen der Dachantenne

der Attacke ist es einen Empfänger, der an einer der statischen Dachantennen angeschlossen ist, zu einem bewegten Empfänger zu machen. Dazu wurde in einem ersten Schritt das statische Szenario simuliert und mit dem SDR prozessiert. Abbildung 5 zeigt die Abweichungen der statischen horizontalen Positionslösung von der Referenzposition.

Der Empfänger soll nun durch Spoofing von dieser statischen Position wegbewegt werden. Dazu wurde eine Trajektorie, wie in Abbildung 6 dargestellt, vorab bestimmt, diese in den Spoofer eingegeben und die Simulation gestartet. Die Startposition wurde mit einer Genauigkeit von ±20 m angenommen. Das Spoofing-Signal wurde wiederum mit dem Simulator generiert und mit dem zuvor generierten „realen" Signal überlagert, wobei die Leistung des Spoofers gegenüber der vorherigen Simulation um 3 dB angehoben wurde.

Anschließend wurde das kombinierte digitale Signal mit dem SDR prozessiert und die Ergebnisse analysiert. Abbildung 7 zeigt den doch signifikanten Anstieg der empfangenen Signalleistung während der Spoofing-Attacke. Wie in Abbildung 8 zu sehen ist, reagiert der Empfänger auf das Spoofing-Signal sofort und die Positionslösungen (rot) entsprechend der simulierten Trajektorie (gelb). Das nicht-gespoofte Soll-Resultat entspricht der statischen Lösung (blau). Es sind jedoch Lücken und Ausreißer erkennbar.

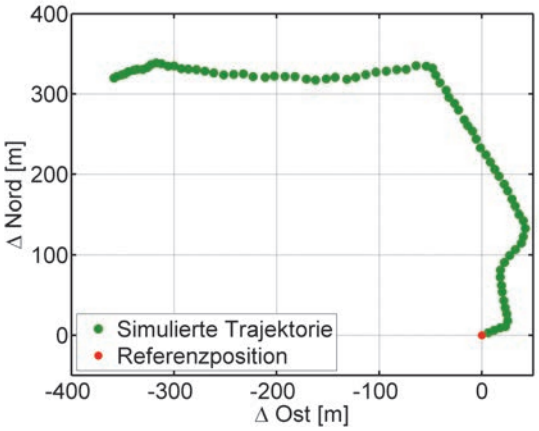

Abb. 6: Spoofing-Trajektorie

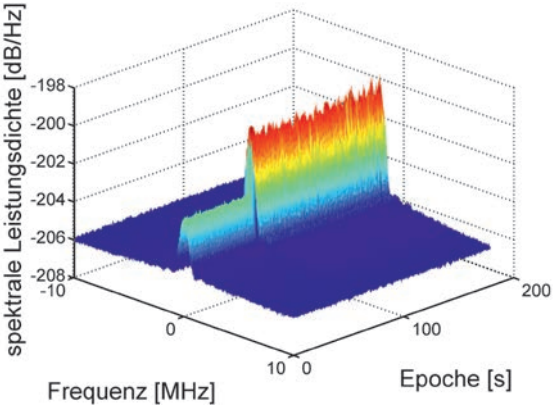

Abb. 7: Empfangene Signalleistung während der simulierten Spoofing-Attacke

Abb. 8: Positionslösungen der Spoofing-Attacke überlagert mit Google Earth

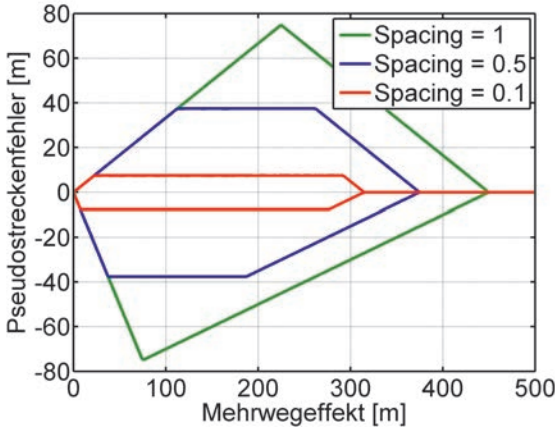

Abb. 9: Abschätzung des Pseudostreckenfehlers in Abhängigkeit vom Mehrweg und dem Korrelator-Spacing

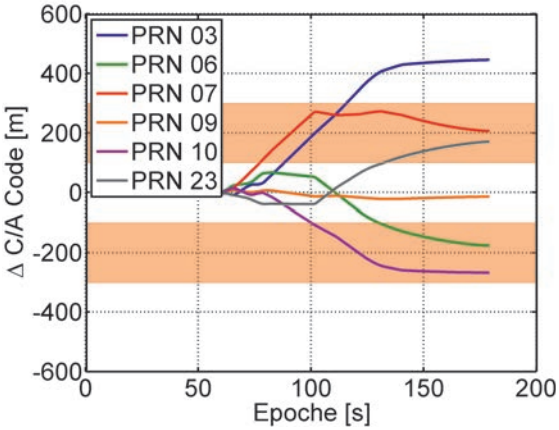

Abb. 10: Pseudostreckendifferenzen zwischen „realem" und Spoofing Szenario

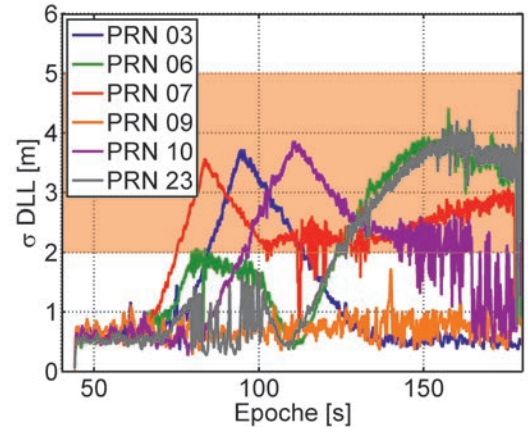

Abb. 11: Tracking-Genauigkeit der Pseudostreckenmessungen

Diese Ausreißer hängen damit zusammen, dass sich Spoofing ähnlich verhält wie der Mehrwegeffekt. In beiden Fällen handelt es sich um die zeitlich versetzte Überlagerung von ein und demselben Signal. Während beim Mehrwegeffekt das zeitlich versetzte Signal auf Grund der Reflexion schwächer wird, wird es beim Spoofer auf Grund der höheren Sendeleistung des Spoofers stärker. Jenes Signal, das im Empfänger verarbeitet wird, ist die Summe der beiden Signale. Durch die Überlagerung kommt es zu einer Deformation der Korrelationsfunktion und dies wiederum bewirkt eine fehlerhafte Messung der Signallaufzeit.

In beiden Fällen führt dies zu einem Fehler in der Distanzmessung und damit verbunden zu einem Fehler in der Positionslösung. Im Falle des Mehrwegeffekts lässt sich ein Zusammenhang zwischen dem Fehler in der Distanzmessung und dem zeitlichen Versatz der Signale herstellen. Dieser ist abhängig vom auftretenden Mehrwegeffekt und den Tracking-Eigenschaften, im Speziellen vom Korrelator-Spacing des Empfängers. Abbildung 9 zeigt den Zusammenhang zwischen dem Mehrweg und dem Pseudostreckenfehler für unterschiedliche Korrelatorabstände (0.1 Chips, 0.5 Chips, 1 Chip). Der größte Fehler bei der Pseudostreckenmessung tritt bei einem Mehrweg von ca. 200 Metern auf.

Betrachtet man nun im Falle der Spoofing-Attacke die Differenz zwischen der tatsächlichen Distanz zwischen Satellit und Empfänger und der Spoofing-Trajektorie und den Satelliten, so sieht man, dass hier die Differenzen im Bereich von ±500 Metern liegen. Wie beim Mehrwegeffekt tritt die größte Ungenauigkeit im Tracking bei einem Versatz von ±200 Metern auf (Abbildung 10).

Ein Vergleich der Pseudostreckendifferenzen mit der geschätzten Tracking-Genauigkeit (Abbildung 11) zeigt, dass diese korrelieren. Da die Tracking Loop nur das gesamte empfangene Signal verarbeitet, ist es nicht möglich zwischen Mehrwegeffekt und Spoofing zu unterscheiden. Dies bedeutet aber auch, dass damit ein Ansatz zur Detektion bzw. für Gegenmaßnahmen gefunden werden kann.

Dabei spielt natürlich die Intelligenz des Spoofers eine entscheidende Rolle. Derzeit ist diese noch recht einfach. Geeignete Verfahren zur Mehrwegunterdrückung wären also im Fall von Spoofing ein erster Ansatz. Um wirksame Gegenmaßnahmen einzuleiten ist es allerdings notwendig, sich der Gefahr bewusst zu sein und darauf

zu achten. Detektion und Klassifikation sind dabei die ersten Maßnahmen. Mögliche Gegenmaßnahmen konzentrieren sich derzeit sowohl auf den Zeit-, Orts- als auch Frequenzbereich und reichen von Filtern bis zur Verwendung von zusätzlichen Sensoren. Ganz interessant und vielversprechend, aber auch entsprechend teuer, sind Ansätze, die nicht nur eine Antenne beinhalten sondern ein ganzes Array von Antennen. Damit kann durch Differenzbildung der Signale der einzelnen Antennen die Signalquelle hinsichtlich Empfangsrichtung und Elevation bestimmt werden. Taucht nun ein Jammer auf, so kann die Richtung zum Störsender bestimmt werden und in weiterer Folge virtuell die Antenne in diesem Bereich abgeschaltet werden, so dass keine Störsignale mehr empfangen werden können.

4. Ausblick

Eine weitere Methode Spoofing zu erkennen und abzuwehren, welche in Zukunft von Galileo zur Verfügung gestellt wird, ist die Signalauthentifizierung. Bei dieser Methode werden spezielle Sicherheitssignaturen in das Signal bzw. in die Navigationsnachricht integriert. Dadurch ist es möglich, festzustellen, ob das Signal tatsächlich vom Satelliten ausgeschickt wurde oder nicht. Der Galileo Commercial Service und in Zukunft vielleicht auch der Open Service werden diese Möglichkeit zur Signalauthentifizierung implementiert haben. Am 15. Dezember 2016 wurde von der Europäischen Kommission die Initial Operational Capability (IOC) von Galileo bestätigt [1]. Mit dieser Bekanntgabe begann Galileo offiziell, die ersten drei Services (Open Service, Search and Rescue Service und Public Regulated Service) für Navigationszwecke zur Verfügung zu stellen. Man setzte sich mit dem öffentlich regulierten Dienst (PRS), der verschlüsselt und wesentlich resistenter gegenüber Störungen und Interferenz ist, zum Ziel, die Erfordernisse der öffentlichen Einrichtungen in den Bereichen Zivilschutz, der nationalen Sicherheit und der Wahrung des Rechts zu erfüllen und einen hohen Grad an Authentifizierung, Dienstkontinuität und Verfügbarkeit (in Bezug auf GNSS-gestützte Positionierung und Zeitinformation) zur Verfügung zu stellen. Der Grund für diese Resistenz liegt im speziellen Signaldesign. PRS verwendet ein extrem breites Signalspektrum und ist zusätzlich noch speziell verschlüsselt. Ein Vergleich der Performance des zivilen GPS-Signals mit der des Galileo Open Service und des Galileo PRS im Falle einer Störattacke zeigt, dass Galileo PRS der zukünftig stetig steigenden Bedrohung von absichtlichen GNSS-Störattacken gewachsen ist.

Laut [21] soll im Jahr 2020, wenn die ersten drei Galileo Services voll operationsfähig sind, der Galileo Commercial Service den Nutzern erste Dienste zur Verfügung stellen. Nutzer des Commercial Services werden von zwei unterschiedlichen Diensten profitieren. Neben einer gesteigerten Genauigkeit (High Accuracy Service) wird es auch die Möglichkeit einer Signalauthentifizierung geben. Der High Accuracy Service basiert auf der Übertragung von Precise Point Positioning (PPP) Informationen im Galileo E6-Band und soll Genauigkeiten unter einem Dezimeter weltweit bieten. Der Commercial Authentication Service, basierend auf der Verschlüsselung eines Signals, welches ebenfalls im E6-Band übertragen wird, soll die Robustheit professioneller Anwendungen steigern. Diese beiden Dienste des Commercial Services sollen in Zukunft gegen eine Servicegebühr nutzbar sein [21].

Geht es nach der Commercial Service Implementierungsentscheidung der Europäischen Kommission, sollen zivile Nutzer in Zukunft kostenlos die Möglichkeit zur Signalauthentifizierung bekommen. Durch die Verwendung der Galileo Open Service Navigation Message Authentication (OSNMA) im Galileo E1-Band können sich somit in Zukunft alle Galileo Nutzer vor Spoofing-Attacken schützen. [21] erwähnt ebenfalls, dass zumindest eine Signalkomponente des E6-Signals frei verfügbar sein soll, so dass Nutzer auch von einem Signal im E6-Band kostenlos profitieren würden. Diese frei verfügbare E6-Signalkomponente würde nochmals zur Steigerung der Positionsgenauigkeit, im Speziellen im geodätischen Bereich, beitragen.

Eine weitere Möglichkeit wird in Zukunft die Kombination von unterschiedlichsten Signalen zur Navigation sein. Mittels Software-Empfängern ist dies sehr leicht möglich; so können zum Beispiel UWB, WLAN oder GSM Signale zur Positionsberechnung herangezogen werden. Dieses Konzept lässt sich auch erweitern. Detektiert und lokalisiert man Störsender, so könnte deren Signale in Kombination mit dem Wissen über ihren Sendestandort zur Positionierung herangezogen werden. TeleConsult Austria untersucht derzeit gerade diese Möglichkeiten.

Danksagung

Die Projekte PRSAustria und DECODE werden durch das Bundesministerium für Verkehr, Innovation und Technolo-

gie (BMVIT) unter der Verantwortung der Österreichischen Forschungsförderungsgesellschaft (FFG) im Rahmen des Austrian Space Application Programms (ASAP) gefördert. Der Autor bedankt sich beim Fördergeber für die finanziellen Mittel, sowie bei der FFG für die professionelle Abwicklung. Allen Projektpartnern sei für die ausgezeichnete Zusammenarbeit ein Dank ausgesprochen. Ein großer Dank gilt auch dem hervorragenden Team der TeleConsult Austria GmbH, insbesondere Dipl.-Ing. Sascha Bartl, der maßgeblich an den Untersuchungen im Bereich Interferenz beteiligt ist.

Der Autor wurde für die hier beschriebene wissenschaftliche Arbeit, die im Rahmen des 7. Navigations-Get-Together präsentiert wurde [4], von der Österreichischen Geodätischen Kommission [22] mit dem Karl-Rinner Preis 2015 ausgezeichnet. Der Autor bedankt sich herzlich bei der Kommission für diese Ehre.

Die Navigations-Get-Together werden vom Österreichischen Verein für Navigation organisiert und finden zweimal jährlich abwechselnd an der Technischen Universität Graz und der Technischen Universität Wien statt und dienen dem Informationsaustausch auf den Gebieten Navigation, Positionierung, Globale Navigationssysteme und verwandter Themenbereiche.

Referenzen

[1] *European Global Navigation Satellite System Agency (2016)*: Galileo begins delivery of Initial Services. Pressemitteilung, 16. Dezember 2016. Online verfügbar unter: http://www.gsa.europa.eu.

[2] *TeleConsult Austria GmbH (2016)*: Detection, countermeasures and demonstration of GNSS spoofing (DECODE). Online verfügbar unter: www.tca.at/decode-4-de.

[3] *TeleConsult Austria GmbH (2016)*: Impacts and Countermeasures of Austrian PRS application scenarios in GNSS denied environments (PRSAustria). Online verfügbar unter: http://www.tca.at/prsaustria-4-de.

[4] *Österreichischer Verein für Navigation (2016)*: 7. Navigations-Get-Together - Aktuelle Projekte im Bereich Navigation. Online verfügbar unter: http://www.ovn.at.

[5] *European Global Navigation Satellite System Agency (2015)*: GNSS Market Report Issue 4. Online verfügbar unter: http://www.gsa.europa.eu/market/market-report.

[6] *European Global Navigation Satellite System Agency (2011)*: Why we need Galileo? Online verfügbar unter: http://www.gsa.europa.eu.

[7] *Hofmann-Wellenhof, B., Lichtenegger, H., Wasle, E. (2008)*: Global Navigation Satellite Systems – GPS, GLONASS, Galileo and more. Springer, Wien New York.

[8] *National Coordination Office for Space-Based Positioning, Navigation, and Timing (2015)*: GPS.gov: Applications: Timing. Online verfügbar unter: http://www.gps.gov/applications/timing/.

[9] *Volpe, John A. (2001)*: Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. National Transportation Systems Centre, Final Report, Department of Transportation, 29. August.

[10] *Jones, M. (2011)*: The Civilian Battlefield – protecting GNSS receivers from interference and jamming. Inside GNSS, März/April.

[11] *Berglez, P., Katzler-Fuchs, S. (2015)*: The PRS – Secure EU satellite navigation for government use. Eingeladener Vortrag bei der Informationsveranstaltung des Bundeskanzleramts, BMVIT, Wien, 12. Oktober.

[12] *Kemetinger, A., Hinteregger, S., Berglez, P. (2013)*: GNSS Interference Analysis Tool. In: Proceedings of the European Navigation Conference, ENC 2013, Wien, 23. – 25. April.

[13] *Betz, J., Titus, B. (2004)*: Intersystem and intrasystem interference with signal imperfections. In: Position Location and Navigation Symposium, Monterey, California, 26. – 29. April.

[14] *Wasle, E., Berglez, P., Seybold, J., Hofmann-Wellenhof, B. (2009)*: RNSS signal modelling for interference analysis. In: Proceedings of the 22nd International Meeting of the Satellite Division of The Institute of Navigation, ION GNSS 2009, Savannah, Georgia, 22. – 25. September.

[15] *Wallner, S., Hein, G., Pany, T., Avila-Rodriguez, J., Posafay, A. (2005)*: Interference computations between GPS and Galileo. In: Proceedings of the 18th International Meeting of the Satellite Division of The Institute of Navigation, ION 2005, Long Beach, California, 13. – 16-September.

[16] *Julien, O. (2005)*: Design of Galileo L1F Receiver Tracking Loops. PHD Thesis, Department of Geomatics Engineering, University of Calgary.

[17] *Bartl, S. (2015)*: Detektion und Lokalisierung von GNSS Störsendern zur Sicherung kritischer Infrastruktur im Alpenraum. In: AHORN 2015 – Der Alpenraum und seine Herausforderungen im Bereich Orientierung, Navigation und Informationsaustausch, Wildhaus, Schweiz, 26. – 27. November. Online verfügbar unter: http://www.ion-ch.ch/ahorn2015.

[18] *Bartl, S. (2014)*: GNSS Interference Monitoring - Detection and classification of GNSS jammers. Diplomarbeit, TU Graz, TeleConsult Austria GmbH; Betreuer: Hofmann-Wellenhof, B., Berglez, P., November 2014.

[19] *Hinteregger, S., Berglez, P. (2014)*: GNSS Airport Interference Monitoring System. In: Proceedings of the International Symposium on Certification of GNSS Systems & Services - CERGAL 2014, Dresden, Deutschland, 8. – 9. Juli.

[20] *Dovis, F. (2015)*: GNSS Interference Threats & Countermeasures. GNSS Technology and Applications, Artech House, Norwood.

[21] *European Global Navigation Satellite System Agency (2017)*: Galileo Commercial Service Implementing Decision enters into force. Pressemitteilung, 10. Februar 2017. Verfügbar unter: http://www.gsa.europa.eu.

[22] *Österreichische Geodätische Kommission (2016)*: Karl Rinner Preis 2015. Online verfügbar unter: http://www.oegk-geodesy.at

Anschrift des Autors

Dipl.-Ing. Dr.techn. Philipp Berglez, TeleConsult Austria GmbH, Rettenbacher Straße 22, A-8044 Graz.

E-Mail: pberglez@tca.at