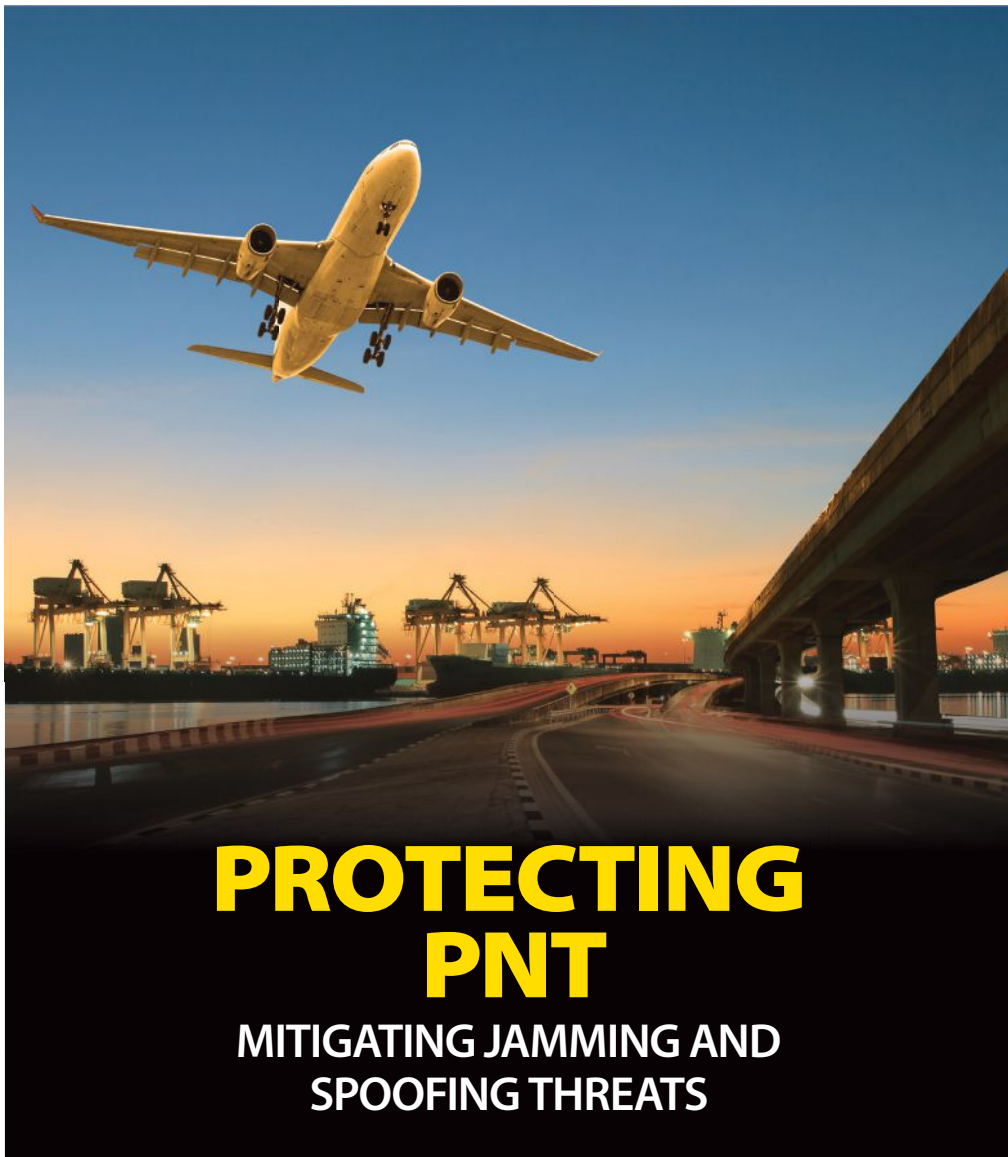


# InsideGNSS

Published by **Autonomous Media**

GPS | GALILEO | GLONASS | BEIDOU



## PROTECTING PNT

MITIGATING JAMMING AND  
SPOOFING THREATS

- SPOOFING DETECTION** | Decomposing the CCAF of GNSS signals during attacks
- WORKING PAPERS** | GNSS authentication via an embedded navigation testbed
- WARDING OFF ATTACKS** | Verifying spoofing countermeasures based on sparse signal processing

# CAST TRUTH

REAL WORLD GNSS/INS  
SIMULATION SOLUTIONS

Aerial\_Jammer\_1



Aerial\_Jammer\_2

CAST Navigation's Jammer sub-systems allow you to add exceptional accuracy and repeatability to your GNSS phased array antenna system testing solution where interference modeling is required. Our proprietary FPGA technology supplies up to 16-phase coherent and independently controlled interference signals per antenna element, and as many as 8 antenna elements per Jammer sub-system.

**CAST**  
NAVIGATION  
[www.castnav.com](http://www.castnav.com)

# AI BASED NAVIGATION SOLUTIONS

RTK GNSS / INS

Y: 183.78 ° P: - 4.91 °  
R: - 0.12 ° Alt: 1281 m  
Lat: -33.862687 - 151.208860

Power Consumption (typical) 29 W



## CERTUS EVO – RTK GNSS/INS

Accurate positioning in the most demanding conditions

- 0.05° Heading  
0.03° Roll & Pitch
- 0.2° /hr  
MEMS gyroscope
- 1000 Hz  
Update Rate
- 10 mm  
RTK Positioning



ADVANCED  
NAVIGATION



# CONTENTS

SEPTEMBER/OCTOBER 2022 VOLUME 17 NUMBER 5

Published by **Autonomous Media**



**ON THE COVER**

## 46 Mitigating the Threat of Jamming and Spoofing to Aeronautics

Sascha Bartl, Manuel Kadletz, Philipp Berglez, Tomáš Duša

This article highlights a multiscale interference monitoring approach using various detectors, and details findings from an airport monitoring campaign.

### Table of Contents BY THE NUMBERS

**EDITORIAL**

**10** Protecting PNT

**ARTICLES**

**34** Thwarting GPS Spoofing Attacks

**42** Kodiak Robotics Relies on Lightweight Mapping for Autonomous Truck PNT

**46** Cover Story: Mitigating the Threat of Jamming and Spoofing to Aeronautics

**60** Working Papers: Nautilus, an Embedded Navigation Authentication Testbed

**66** Detecting GNSS Spoofing

**DEPARTMENTS**

**14** News

**16** Washington View

**22** The Inertialist

**30** Brussels View

**74** Advertisers Index

**74** GNSS Timeline

## 34 Thwarting GNSS Spoofing Attacks

**Verifying spoofing countermeasures based on sparse signal processing.**

Junhwan Lee, Erick Schmidt, Nikolaos Gatsis, David Akopian

A look at a technique developed to mitigate joint spoofing against time and a single position coordinate in stationary GPS receivers.



## 60 Working Papers

**Nautilus: An Embedded Navigation Authentication Testbed**

Cillian O'Driscoll, Gianluca Caparra

This lightweight, low-cost platform can be configured for various applications and test scenarios, including GNSS authentication.



# Next level precision

Increase your reliability with seamless,  
global network coverage.



**Topnet Live** is a real-time GNSS correction service that delivers high-quality data to GNSS receivers around the globe. Sold through aftermarket, system integrators and OEM channels, the service can be used in a variety of applications including survey, construction, GIS, mapping, and agriculture.

CONTINUOUS ACCURACY | ALWAYS ON | FLEXIBLE SUBSCRIPTIONS

Learn more at [topconpositioning.com/topnetlive](https://topconpositioning.com/topnetlive)

COLUMNS

16



**Washington View**

Welcome to the Space Jam

By Dawn Zoldi

22



**The Inertialist**

INS-Centric Sensor Fusion

By Andrey Soloviev

30



**Brussels View**

ESA ESTEC Gets Smart City Treatment

By Peter Gutierrez



**66 Detecting GNSS Spoofing**

Decomposing the Complex Cross Ambiguity Function of GNSS signals during malicious spoofing attacks.

Sahil Ahmed, Samer Khanafseh, Boris Pervan

This method is applicable to spoofing scenarios that are difficult to detect by other means, including previously proposed methods that rely on observation of the magnitude of the CCAF alone.

EDITORIAL

**10 The Time and the Place**  
Protecting PNT

DEPARTMENTS

**14 News**

**74 Advertisers Index**

**74 GNSS Timeline**  
Calendar of Events

CUSTOM CONTENT

**56 Up Against It**  
VTOL and air-launched UAVs require sophisticated navigation systems, and VectorNav is taking the lead in integrating them into these platforms.

**GNSSA-DCP<sup>®</sup>**

**Active Dual Circularly Polarized geodetic-grade GNSS Antenna**



Receive RHCP and LHCP signals simultaneously. Cover all GNSS frequencies in L band.



**Available now:  
a lightweight, UAV-ready dual circularly polarized antenna**

Technology licensed by Fraunhofer IIS  
<https://teleorbit.eu>



orolia

# BACK TO SCHOOL TRADESHOWS

## **ADAS Automotive Testing Show 2022**

September 4-6, 2022  
San Jose, CA

## **UNVEX 2022**

September 14-16, 2022  
Sevilla, Spain

## **IAC 2022**

September 18-22, 2022  
Paris, France

## **ION GNSS+ 2022**

September 19-23, 2022  
Hyatt Regency Denver at Colorado  
Convention Center  
Denver, Colorado

## **The Trading Show Chicago 2022**

September, 28-29 2022  
Chicago, IL

## **Low Level RF Workshop 2022**

October 9-13, 2022  
Windisch, Switzerland

## **AUSA 2022**

October 10-12, 2022  
Washington, DC

## **MRO EUROPE 2022**

October 18-20, 2022  
London, UK

## **Euronaval 2022**

October 18-20, 2022  
Le Bourget, France

## **STAC New York Fall 2022**

October 19, 2022  
New York, NY

## **ITC 2022**

October 24-27, 2022  
Glendale, AZ

## **ITSF 2022**

November 7-10, 2022  
Düsseldorf, Germany

## **Space Tech Expo Europe 2022**

November 15-17, 2022  
Bremen, Germany

Where can you meet  
Orolia this year?



# InsideGNSS

GPS | GALILEO | GLONASS | BEIDOU

ENGINEERING SOLUTIONS FROM THE GLOBAL NAVIGATION SATELLITE SYSTEM COMMUNITY

September/October 2022 Volume 17/Number 5

Published by **Autonomous Media**

## EDITORIAL

Editor-in-Chief **Alan Cameron** alan@insidengnss.com

Editor Emeritus **Glen Gibbons** glen@insidengnss.com

Editor **Renee Knight** renee@insidengnss.com

Creative Director **Christine Waring**

Contributing Editor for "Working Papers"

**Günter Hein** Günter.Hein@unibw-muenchen.de

Contributing Editor for "GNSS Solutions"

**Sam Pullen** spullen@stanford.edu

Contributing Editor for "Washington View"

**Dawn K. Zoldi**

Contributing Editor for "Brussels View"

**Peter Gutierrez** peter@insidengnss.com

Contributing Editor for "The Inertialist"

**Andrey Soloviev** Andrey@insidengnss.com

Advisory Editor **Abe Peck** abe@insideunmanned.com

Contributing Editor for "GNSS & the Law"

**Ingo Baumann** ingo.baumann@bho-legal.com

Technical Editor **Fiona Walter**

Circulation Director **Jan Edwards-Pullen**

## ADVERTISING SALES AND BUSINESS DEVELOPMENT

Publisher **Richard Fischer** richard@insidengnss.com

Mobile: 609-240-1590, Office: 732-741-1964

Ad Services **Gina McGuinness** gina@insidengnss.com, Mobile: 732-456-4911

Published by **Autonomous Media**

157 Broad Street, Suite 307, Red Bank, New Jersey 07701 USA

Telephone: 732-741-1964



Follow us on Twitter @insidengnss

Copyright 2022 Inside GNSS Media & Research LLC. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical (including by Internet, photocopy, recording, or information storage and retrieval), without written permission. Authorization is granted to photocopy items, with attribution, for internal/educational or personal non-commercial use. For all other uses, contact Richard Fischer.

**INSIDE GNSS** (ISSN 1559-503X) is published bimonthly by Autonomous Media, LLC, 157 Broad Street, Suite 307, Red Bank, NJ 07701. Periodicals Postage Paid at Red Bank, NJ and at additional mailing offices. POSTMASTER: Send address changes to Inside GNSS, 157 Broad Street, Suite 307, Red Bank, NJ 07701. Print subscriptions are free to qualified USA subscribers. **Inside GNSS** is a registered trademark of Autonomous Media. **INSIDE GNSS** does not verify any claims or other information in any of the advertisements or technical articles contained in the publication and cannot take responsibility for any losses or other damages incurred by readers in reliance on such content.

## Subscribe Online

**FREE ONE-YEAR SUBSCRIPTIONS** to the print and/or digital versions are available to qualified readers who work in GNSS-related companies, organizations, research institutes, government agencies, and the military services.

You may also change your address, renew, or unsubscribe online:

[WWW.INSIDENGSS.COM/SUBSCRIPTIONSERVICES](http://WWW.INSIDENGSS.COM/SUBSCRIPTIONSERVICES)

## Editorial Advisory Council

### VIDAL ASHKENAZI

Nottingham Scientific Ltd., Nottingham, **United Kingdom**

### JOHN BETZ

MITRE Corporation, Bedford, Massachusetts, **USA**

### PASCAL CAMPAGNE

France Développement Conseil, Vincennes, **France**

### MARIO CAPORALE

Italian Institute of Navigation, Rome, **Italy**

### MARCO FALCONE

European Space Agency, Noordwijk, **The Netherlands**

### SERGIO GRECO

Thales Alenia Space, Rome, **Italy**

### JEAN-LUC ISSLER

CNES, Toulouse, **France**

### CHANGDON KEE

Seoul National University, Seoul, **Korea**

### MIKHAIL KRASILSHCHIKOV

Moscow Aviation Institute, Moscow, **Russia**

### SANG JEONG LEE

Chungnam National University, Daejeon, **Korea**

### MARCO LISI

ESA, **Belgium**

### JULES MCNEFF

Overlook Systems Technologies, Inc., Vienna, Virginia, **USA**

### PRATAP MISRA

Tufts University, Medford, Massachusetts, **USA**

### BRAD PARKINSON

Stanford University, Palo Alto, California, **USA**

### TONY PRATT

Professor and Consultant, **United Kingdom**

### SERGEY G. REVNIVYKH

ISS Reshetnev, Zheleznogorsk, **Russian Federation**

### MARTIN RIPPLE

Frequentis AG, **Australia**

### CHRIS RIZOS

University of New South Wales, Sydney, **Australia**

### TOM STANSELL

Stansell Consulting, Rancho Palos Verdes, California, **USA**

### JACK TAYLOR

The Boeing Company, Colorado Springs, Colorado **USA**

### JÖRN TJADEN

European Space Agency, Noordwijk, **The Netherlands**

### A.J. VAN DIERENDONCK

AJ Systems, Los Altos, California, **USA**

### FRANTISEK VEJRAZKA

Czech Technical University, Prague, **Czech Republic**

### PHIL WARD

Navward Consulting, Garland, Texas, **USA**

### CHRISTOPHER K. WILSON

Vehicle data and technology consultant, California, **USA**

### LINYUAN XIA

Sun Yat-Sen University, Guangzhou, **China**

### AKIO YASUDA

Tokyo University of Marine Science and Technology, Tokyo, **Japan**



# Keep the lights on!

**Protect Critical Infrastructure  
if GPS is disrupted or manipulated**

**Introducing the PNT-6220 Assured Reference – the only product combining Low Earth Orbit (LEO), GNSS, terrestrial, wireline, and atomic clock services in one small solution, specifically designed for Critical Infrastructure applications.**

The PNT-6220 is the first reference that can seamlessly combine concurrent L1, L2, L3, and L5 GNSS reception with a secure STL (LEO-based) timing receiver, terrestrial receivers, and full PTP/IEEE-1588 Edge-Grandmaster (EGM) and PTP/IEEE-1588-slave capability.

Whether you are looking for an Assured PNT reference for Critical Infrastructure applications in response to the directives of the recent Presidential Executive Order 13905, a timing reference for 5G equipment, an ePRTC-capable reference, or just a high-performance disciplined reference that supports PTP/IEEE-1588, LEO-based Satellite Time and Location (STL), RF distribution, and multi-frequency GNSS capability – the PNT-6220 can do it.

**Now available with M-CODE**



**Let us configure a version for your  
state-of-the-art application.**

# Protecting PNT



**RENEE KNIGHT**  
EDITOR

Jamming and spoofing remain a growing threat to the resiliency and accuracy of PNT. Incidents are becoming more common and signal disruption easier to achieve, putting our safety critical infrastructure at risk. But, of course, there's no shortage of work and research being done to determine how best to mitigate such potentially harmful attacks, and progress is being made.

The threat of spoofing and jamming to PNT is always top of mind, and an ongoing theme in many of the articles you'll find in *Inside GNSS*. In this issue, we make a point of highlighting efforts being made to lower the risk and protect PNT from nefarious acts.

One such article comes out of the University of Texas at San Antonio. Junhwan Lee and co-authors detail a technique to mitigate joint spoofing against time and a single position coordinate in stationary GPS receivers. Expanding on previous work, they present a linearization of the GPS measurement equation as well as review sparsity characteristics of the attacks.

during malicious spoofing attacks. The algorithm was tested in several challenging scenarios with promising results.


In this issue's Working Papers, we learn about Nautilus, an embedded navigation authentication testbed. The platform is both low cost and lightweight and can be easily configured for GNSS authentication. It also can be used in other scenarios, such as for signal quality monitoring or recording snapshots of GNSS signal events, including jamming.

Washington View looks at another threat to PNT: space debris. Currently, there are more than 2,500 defunct satellites in orbit that have the potential to do harm. Columnist Dawn Zoldi breaks down just how big a threat space debris is to PNT, and outlines the FCC's recently released plans to regulate its removal.

Moving a bit away from the jamming and spoofing focus, we also cover self-driving trucks and smart cities in this issue. Kevin Jost, editor of our sister publication *Inside Autonomous Vehicles*, highlights Kodiak Robotics and its fourth-generation autonomous trucks. CEO Don Burnette provides insight into the company's unique approach to PNT.

In Brussels View, columnist Peter Gutierrez takes us inside a smart city infrastructure at The European Space Agency's ESTEC facility. The large campus is set up like an urban environment with the most common GNSS hazards, including obscured view and multipath, making it a perfect place to test new technologies. Rokubun, a company that develops high-accuracy navigation solutions for mass-market devices, leads the HANSEL project.

Finally, The Intertialist columnist Andrey Soloviev covers INS-centric sensor fusion. He outlines the three main integration modes, loose, tight and deep coupling, and the pros and cons of all three.

We cover a lot in this issue, and I'd love to hear what you think. You can contact me at [renee@insidegnss.com](mailto:renee@insidegnss.com) to share your thoughts and story ideas. 

## THE THREAT OF JAMMING AND SPOOFING TO PNT

IS ALWAYS TOP OF MIND, AND AN ONGOING THEME IN MANY OF THE ARTICLES YOU'LL FIND IN *INSIDE GNSS*.

Reliable PNT is of particular importance in aeronautics, especially during approach and landing. RAIM provides limited protection against intentional interference, making it critical to develop dedicated interference monitoring algorithms that target jamming and spoofing. Sascha Bartl of OHB Digital Solutions and co-authors outline a multiscale interference monitoring approach using several different detectors. The article also presents findings from a signal monitoring campaign conducted at airport Brno in Europe.

Sahil Ahmed and co-authors from the Illinois Institute of Technology look into a new method to detect GNSS spoofing. The approach detailed makes it possible to decompose the Complex Cross Ambiguity Function of GNSS signals



# UNPRECEDENTED PERFORMANCE AT YOUR FINGERTIPS

Introducing the all new Tactical Embedded line.  
The best just got smaller.



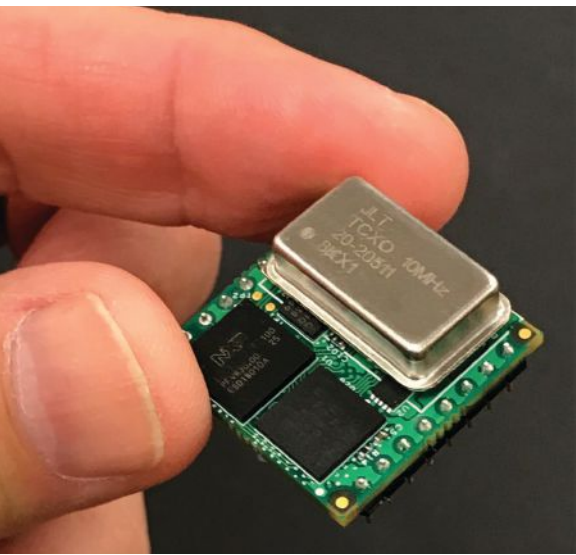
Tactical-Grade IMU  
Heading:  $0.05^{\circ}$ - $0.1^{\circ}$   
Pitch/Roll:  $0.015^{\circ}$   
GNSS: L1/L2/E1/E5  
with RTK/PPK



[vectornav.com](http://vectornav.com)  
**+1.512.772.3615**

# 360 DEGREES

News from the  
world of GNSS



12-channel, 1x1 inch, full-constellation, real-time GPS Simulator/Micro-Transcoder.

Photos courtesy of Jackson Labs.

## See Additional News Stories

at [www.insidegnss.com/news](http://www.insidegnss.com/news)

- In Memory of Industry Leader Patricia Doherty, Past ION President and Current Satellite Division Chair
- New Timing Antenna Now Part of Tallysman's GNSS Product Line
- Xona Secures Investment from First Spark Ventures and Lockheed Martin to Accelerate LEO GPS Alternative
- Upcoming Military Exercises to Focus on Detecting GNSS Disruption

Las Vegas

## Jackson Labs: Providing Resilient Solutions

As GNSS evolves, legacy equipment will continually need to be replaced with emerging technologies that offer advanced capabilities—a time consuming, costly process.

Instead of ripping out and replacing receivers, Jackson Labs Technologies has another solution. With the company's Transcoder, which generates a GPS RF signal locally from any source the user would like to integrate, both military and commercial users can keep their existing GNSS equipment.

The technology, for example, is being integrated into U.S. Army Strykers, reducing the crypty-keying time of the up to 12 SAASM receivers in each military vehicle. And instead of soldiers having to key all 12 SAASM receivers individually, the Transcoder allows using a single M-Code receiver paired to the vehicles' anti-jam (AJ) antenna. This provides a secure PNT solution to all the vehicles' SAASM and commercial GPS receivers through the existing antenna distribution infrastructure.

The Transcoder makes it possible to put the most modern technology—even technology that hasn't been thought of yet—into these and other vehicles from multiple vendors, Jackson Labs Founder and President Gregor Said Jackson said, and have it communicate with the existing infrastructure inside the vehicle.

"You can retrofit the vehicle just by plugging the Transcoder in," Jackson said. "And it will rebroadcast inside the vehicle, so soldiers sitting in the vehicles who have their jammers, their dismantled backpacks, are all receiving their RF signal from the updated Resilient-PNT source in the vehicle. And the second they step outside the vehicle, they're still synchronized to UTC, even in a completely jammed, denied environment, because the vehicle can have an atomic clock in it that acts like a GPS satellite

constellation even in fully denied environments. So they maintain their communications capability."

The Transcoders also have been integrated into U.S. Air Force aircraft, which can have as many as eight or nine different GPS receivers, to address issues with jamming, Jackson said. The Transcoder takes the output of the inertial navigation system (INS) they fly, which is typically fused with other navigation and timing sources, and transmits this PNT solution into the aircraft through the existing antenna wiring.

"To feed the INS positioning into the aircraft systems, you take the output of that INS, you feed it into the Transcoder as a NMEA baseband signal and out comes an RF signal that you can splice into the existing antenna feed of the vehicle," Jackson said.

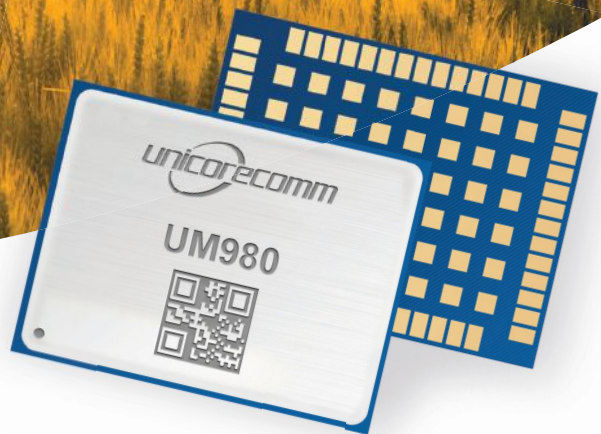
Because the INS is re-calibrated through Vision Based Navigation (VBN), Laser Ranging and other positioning sources, pilots no longer need to rely on GPS to complete their missions—so jamming becomes a non-issue.

"If they're flying in the Middle East, they might get jammed immediately as they take off and would have to find their way back following roads, rivers and train tracks," Jackson said. "They don't have to do that anymore. And they can extend their missions as long as they have fuel and food on board. It allows them to fly missions they could never fly before."

The vehicles being retrofitted have AJ antennas, Jackson said. Pilots can either take the GPS feed from the output from the inertials and feed that into the GNSS receivers on board or they can take the live sky AJ signal. They can switch back and forth between the two in a matter of minutes.

And similar to the M-Code/CSAC retrofit of the Strykers, this solution allows them to maintain legacy equipment that's maybe 10, 15 years old and can no longer be replaced.

*Continued on p. 14*



# Well positioned

With local inventory, dedicated sales and support expertise, and a highly regarded GNSS brand, **Rx Networks** is very well positioned to supply **Unicore Communications** high precision RTK chips, modules and boards to North American product managers, developers and distributors.

For more information on Equivalent RTK high precision and heading performance GNSS products visit [unicore.rxnetworks.com](http://unicore.rxnetworks.com) or contact [unicore@rxnetworks.com](mailto:unicore@rxnetworks.com)

Continues from p. 12

The 1x1 inch small Micro-Transcoder is used successfully in several hand-held anti-drone weapons in a GPS simulator mode to spoof the drones to either land or crash. This is significantly more effective than drone-jamming, as late model drones have built in anti-jamming countermeasures such as INS modules.

The technology also can be used commercially, with the telecom industry a prime example. The Transcoder retrofits small cell sites without any hardware or software changes. This makes it easier to update units to comply with regulations as they change, and will save companies money in the long run.

### STL Integration

Jackson Labs also offers devices that can receive Satellite Time and Location (STL) from Satellites as an alternative to GPS. The signal is 1,000 times stronger than GPS, Jackson said, making indoor reception possible, a benefit for cell phone companies that need to demonstrate capabilities inside mall and storefront walls.

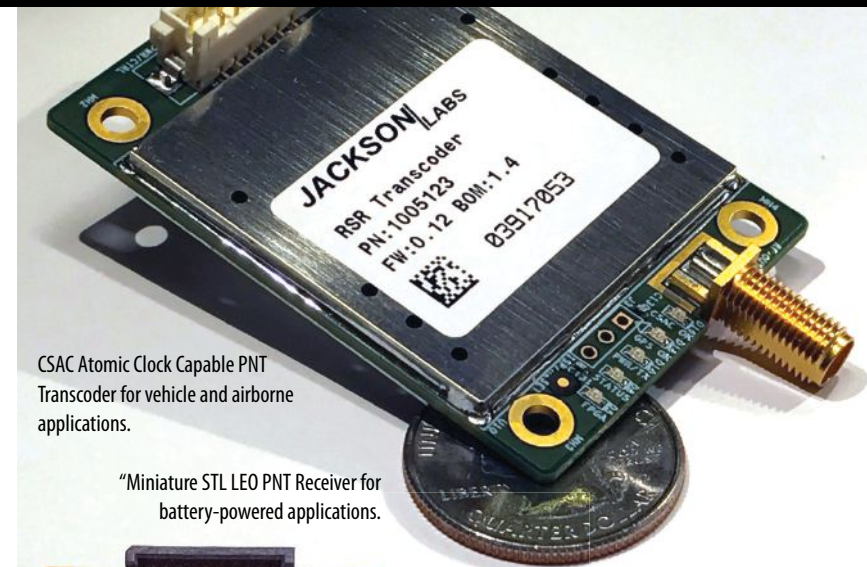
“Companies are finding they can’t get the GPS signal in urban canyons or inside metal buildings, and have to pay up to \$10,000 or more in rental costs to the building owner and operator to put a GPS antenna on the roof,” he said. “With the STL signal, they can get that signal through a local antenna. So it alleviates the need to pay the rental costs for the GPS. That’s a huge, huge advantage for them.”

Regulations will soon require telecom companies to have a backup to GNSS, Jackson said, making this unit even more attractive to the industry.

“We’re the only fully GNSS-independent alternative solution that doesn’t require you to dig trenches to lay fiber optic cable to all the cell sites,” Jackson said. “From a technology perspective, I can deploy this today at any cell site in the world. And we do not need GNSS-dependent Grandmaster servers distributed around the country such as wired or terrestrial solutions require.”

The military can also benefit from this type of technology and is actively pursuing redundant GPS backup solutions.

“Telecom operators, power-generation, communication and broadcast operators world wide are looking for alternatives to



CSAC Atomic Clock Capable PNT Transcoder for vehicle and airborne applications.

“Miniature STL LEO PNT Receiver for battery-powered applications.



GPS, especially since the Ukrainian invasion. Active jamming goes on there. China and Russia have postured that they can be a threat to our GPS system.” Jackson said. “China demonstrated they can grab a satellite and throw it out of orbit. If they make a decision to attack us, we have no GPS backup right now. This is a GPS backup solution. I would compare it to about a gen two or gen three GPS receiver in terms of capabilities, but it’s really much better than that.”

The Time to First Fix (TTFF) including accurate Leapsecond offsets can be as low as 36 seconds with a good constellation and view of the sky, Jackson said, compared to the 10 to 15 minutes it sometimes takes to download the GPS Almanac and get an accurate Leapsecond offset with a GPS receiver. The units are completely software defined and made with commercial, off-the-shelf components. There’s no custom hardware; the software can be integrated into any GNSS receiver. They’re designed to be mass market products with high volume


capability.

“In terms of timing performance, we’re looking at somewhere around 50 nanoseconds standard deviation,” he said. “We’re a timing and frequency company, so we designed this receiver as a timing and frequency receiver from the ground up rather than creating a positioning receiver, and then trying to coax timing out of it. So that’s why our timing performance is so good. We have our GPS disciplined oscillator patented algorithms built into it.”

### Bringing it All Together

JLT provides a comprehensive solution in its PNT-6xxx product line that combines front-end, oscillator holdover, and back end RF distribution capabilities in a small 19” half-width rackmount enclosure. With the boxes, customers can pick and choose what they want based on their needs, with the transcoder and STL integration among the options that distinguish them in the market.

As a company, Jackson Labs focuses on three different product areas: the receivers, timing and holdover capabilities, and the transcoder and output capabilities. They offer options that solve problems for military and commercial customers that depend on reliable GNSS, allowing them to achieve the desired position accuracy through both GNSS and GNSS alternatives, while maintaining legacy equipment and eliminating the costs and headaches associated with upgrades.

“If you combine those areas together,” Jackson said, “magic happens.” 



# Live Remote GNSS Training with Real-Time Engagement

## UPCOMING GNSS COURSES

**November 15-16, 2022**

**Course 122:** GPS Fundamentals and Enhancements

**Instructor:** Dr. Chris Hegarty, MITRE

**November 15-18, 2022**

**Course 346:** GPS/GNSS Operation for Engineers and Technical Professionals

**Instructor:** Dr. Chris Hegarty, MITRE

**December 12-16, 2022**

**Course 557:** Inertial Systems, Kalman filtering and GPS/INS Integration

**Instructors:** Dr. Alan Pue (Retired) APL/JHU and Michael Vaujin, Consultant

All courses available for private group training, remotely or on-site. See <https://www.navtechgps.com/gps-gnss-training/courses/>

“

The video quality was excellent. I don't feel as though going through the course remotely had any negative impact. It was still very personal, easy to ask questions, and I enjoyed the banter over coffee in the morning even if we were all scattered across the world. This was such a great experience.”

—Shealyn Greer, Trident Research

Visit us at  
**Booth 107**  
at ION GNSS+



GNSS products, solutions, and training

QUESTIONS? Contact Trevor Boynton • [tboynton@navtechgps.com](mailto:tboynton@navtechgps.com) • 800-628-0882 • +1-703-256-8900



**T**he resilience of the Global Navigation and Satellite System (GNSS) that enables mission and life-critical position, navigation and timing (PNT) remains a topic of interest around the world. Threats to PNT continue to increase exponentially. Space-based threats rank high among them, including space debris.

Recently, the Federal Communications Commission (FCC) caused a bit of a stir by indicating it plans to issue regulations governing activities in space that currently fall between jurisdictional policy lines, including on the controversial matter of debris removal. Will there be clarity on this issue for the PNT industry soon despite the clutter among the stars and in the halls of government?

American Iridium 33 communications satellite. The impact blew both satellites apart. The ESA estimates more than 630 of the currently defunct satellites in orbit may be involved in similar events.

Add this to an environment already littered with hunks of other dangerous junk. The space surveillance networks regularly catalog and track 36,500 objects of debris larger than 4 inches across. But not all objects are tracked. Based on statistical models, ESA estimates there are 1 million chunks of space debris from 0.4 inches to 4 inches and 130 million from .04 to 0.4 inches. The total mass of this space garbage is estimated to weigh in at more than 10,000 tons.

The problem will continue to get worse. Computer simulations project that space trash between 4 and 8 inches may multiply 3.2 times over the

next 200 years. These same models predict debris less than 4 inches will increase even more, by a factor of 13 to 20.

This raises serious concerns for PNT resilience. While the danger of satellite-to-satellite impacts may be

obvious, even a tiny fragment of debris in space can cause catastrophic damage to satellites. These objects often travel faster than a speeding bullet, at speeds of more than 22,300 miles per hour. This can lead to satellite destruction and result in fragmentation.

Growing orbital congestion also increases the risk of unintentional radio frequency interference.

For these reasons, the costs of mitigating space debris continue to add up. In addition to costs associated with tracking it, companies and governments pay a hefty price for design measures, dodging space debris in orbit or scrubbing missions entirely. Considering a GPS III satellite costs \$400 million or more to build, an ounce of prevention may be worth the potential financial losses of a collision.

**2,500+**

The number of defunct satellites in orbit. Of those, more than 630 may be involved in a collision.

Source: ESA

## Welcome to the Space Jam

Space debris poses a danger to PNT. Here's a look at the threat and how the FCC plans to regulate its removal.

DAWN M.K. ZOLDI (COLONEL USAF, RET.)



**Dawn M.K. Zoldi**  
(Colonel, USAF, Retired)  
is a licensed attorney  
and a 25-year Air  
Force veteran. She

is an internationally recognized expert on advanced technology law and policy, a recipient of the Woman to Watch in UAS (Leadership) Award 2019, and the CEO of P3 Tech Consulting LLC.

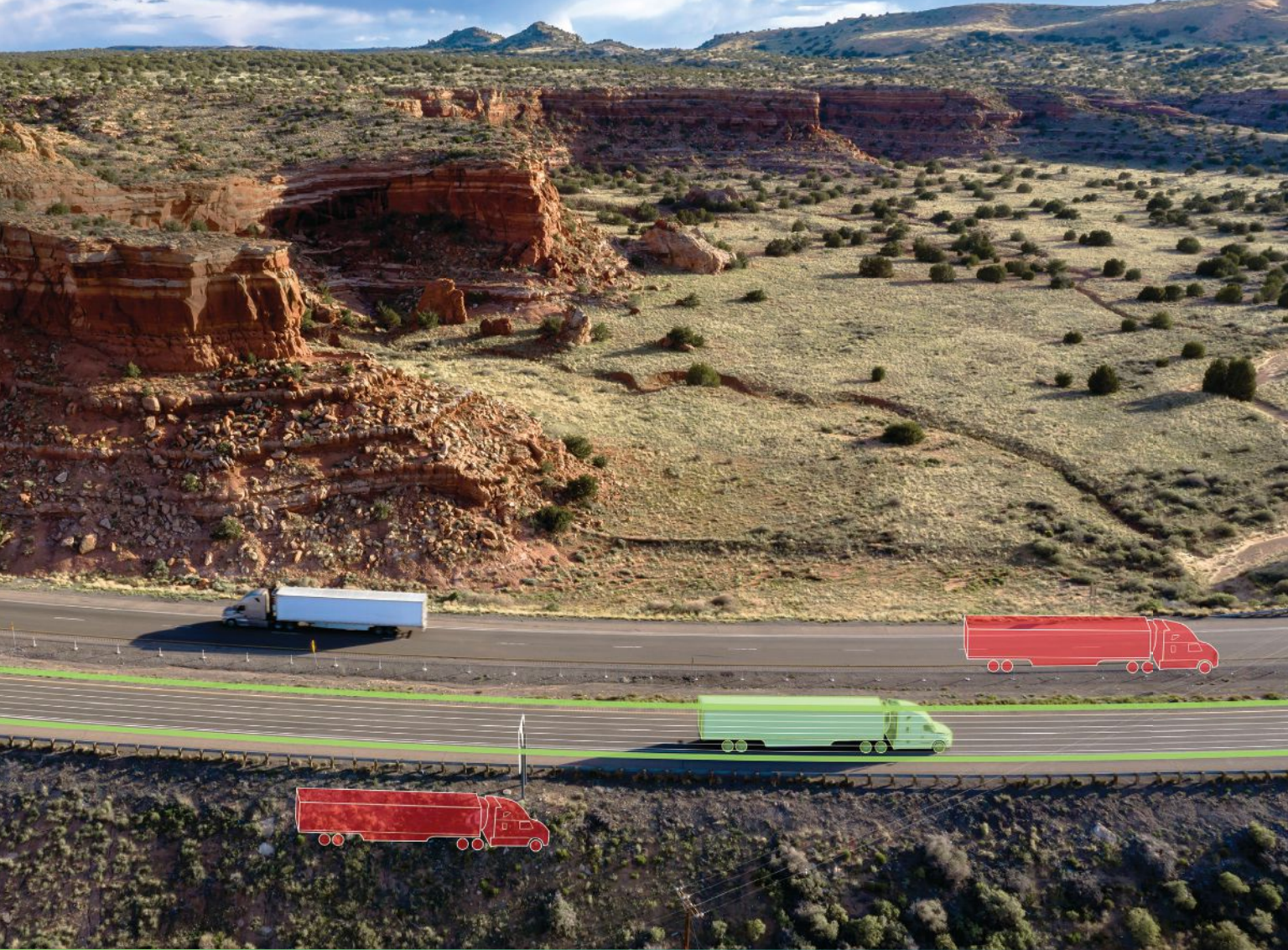
### The Threat Spectrum

Earth's orbit, home to GNSS satellite constellations, continues to grow increasingly crowded. According to the most recent statistics from the European Space Agency (ESA), humankind has launched about 13,630 satellites into Earth's orbit since 1957, the beginning of the Space Age. Of those, almost 9,000 still remain.

While the majority are functional, more than 2,500 defunct satellites also continue to zip around in orbit. They have become nothing more than very large pieces of debris, which may break up, explode, collide or be involved in an event that results in fragmentation.

Such mayhem has already occurred. The first documented case of the destruction of an operational satellite after a collision with a defunct satellite happened in early 2009. In that case, an inactive Russian military communications satellite destroyed an





# Try to spoof us. But fool us? Not a chance.

GNSS Resilience and Integrity Technology (GRIT) is a firmware suite of detection and protection technology developed for our OEM7 receivers to guard your position, navigation and timing. GRIT can detect spoofing and keep you on track, and the GNSS Interference Toolkit (ITK) identifies interference frequencies in your area, protecting you from unintentional or malicious interference. When you've got GRIT for OEM7, your position is true.

Autonomy & Positioning – Assured | [novatel.com/grit](https://novatel.com/grit)



## Other Space-Related Topics

You can track the FCC's other proposed rulemaking on space-related issues in its most recent bi-annual Unified Agenda in the Federal Register at [govinfo.gov/content/pkg/FR-2022-08-08/html/2022-14618.htm](https://govinfo.gov/content/pkg/FR-2022-08-08/html/2022-14618.htm). The complete Unified Agenda will be published in a searchable format at [reginfo.gov](https://reginfo.gov).

Here's a breakdown of what's ahead:

Sequence number	Title	Regulation Identifier No.
301	Update to Parts 2 and 25 Concerning NonGeostationary, Fixed-Satellite Service Systems, and Related Matters: IB Docket No. 16-408.	3060-AK59
302	Amendment of Parts 2 and 25 of the FCC Rules to Facilitate the Use of Earth Stations in Motion Communicating With Geostationary Orbit Space Stations in FSS Bands: IB Docket No. 17-95.	3060-AK84
303	Further Streamlining Part 25 Rules Governing Satellite Services: IB Docket No. 18-314.	3060-AK87
304	Facilitating the Communications of Earth Stations in Motion With Non-Geostationary Orbit Space Stations: IB Docket No. 18-315.	3060-AK89
308	Revising Spectrum Sharing Rules for Non-Geostationary Orbit, Fixed-Satellite Service Systems: IB Docket No. 21-456.	3060-AL41

### A Big Cluster

From a policy standpoint, space debris remains an unsolved global issue. Space law consists primarily of international agreements, treaties, conventions, and United Nations General Assembly resolutions and rules and regulations of international organizations. None of these explicitly forbid the production of space debris. They also don't indicate who is responsible for removing it.

For example, the 1967 Outer Space Treaty imposes general responsibilities on member states for national activities to ensure they are conducted in conformity with the treaty (with the premise of freedom for exploration by all), to authorize and continually supervise its activities, and to share international responsibility for activities in which the state is a participant. Article VIII provides that a state "shall retain jurisdiction" and control over its objects. Most interpret this as including debris. Thus, states and organizations make their own rules for dealing with debris.

In the United States, just this July, the White House Office of Science and Technology Policy released the National Orbital Debris Mitigation Plan to meet space sustainability priorities to mitigate, track and remediate debris. This

**"The first documented case of the destruction of an operational satellite after a collision with a defunct satellite happened in early 2009."**

new 14-page plan supports the overarching 2021 U.S. Space Priorities Framework and implements Space Policy Directive-3 (SPD-3).

Signed by former President Trump, SPD-3 was the nation's first National Space Traffic Management Policy. It outlined key roles and responsibilities. The directive assigned the administrator of NASA as lead for efforts to update the U.S.' Orbital Debris Mitigation Standard Practices and to establish new guidelines for satellite design and operation to mitigate the effect of orbital debris on space activities.

NASA, the directive indicated, must do this in coordination with the secretaries of state, defense, commerce and transportation, and the director of national intelligence. In contrast to this coordination requirement, according to the directive, the NASA administrator must consult with the FCC chairman.

SPD-3 requires the secretaries of

commerce and transportation to assess the suitability of incorporating these updated standards and best practices into their respective licensing processes—again, in consultation with the FCC chairman. In short, the FCC has an important, but consultative, role when it comes to space debris—at least for U.S. government agencies.

In 2019, NASA updated The United States Government (USG) Orbital Debris Mitigation Standard Practices (ODMSP), originally established in 2001 to address the increase in orbital debris in the near-Earth space environment. These updated standard practices for the feds included preferred disposal options for immediate removal of structures from the near-Earth space environment, a low-risk geosynchronous Earth orbit (GEO) transfer disposal option, a long-term reentry option, and improved move-away-and-stay-away storage options in medium Earth orbit (MEO) and above GEO.

But when it comes to commercial use of space, the FCC holds the keys to the kingdom in terms of licensing. Even so, generally speaking, agencies coordinate across the aisle when creating policies that could impact each other. Imagine the surprise when in August the FCC announced a proceeding on Space Innovation; Facilitating Capabilities for In-space Servicing, Assembly, and Manufacturing (ISAM).” As defined in this Notice of Inquiry (NOI), the FCC defines missions in its purview as those “which can include satellite refueling, inspecting and repairing in-orbit spacecraft, capturing and *removing debris* (emphasis added), and transforming materials through manufacturing while in space.”

### Playing Nice in the Space Box

An FCC NOI is a way to ask the public to comment on specific questions about an issue to help determine whether further action is warranted. NOIs are the precursor to the agency's Notice of Public Rulemaking (NPRM).

In this most recent NOI, the FCC specifically seeks comment on “space safety issues that may be implicated



## GNSS Performance Evaluation Integrity Assessment

### GNSS Simulator

- ✓ Multi-Constellation & Multi-Frequency
- ✓ Spatial, Aerial and Terrestrial Trajectories
- ✓ Jamming, Spoofing & 3D Multipath Simulation
- ✓ Low Latency HIL Simulation
- ✓ High Precision through SBAS, RTK

### GNSS Record & Replay

- ✓ All GNSS Bands and Signals
- ✓ Programmable Center Frequency and Bandwidth
- ✓ Single or Multi-Channel Simultaneous Records
- ✓ Up to 16 bits Quantization
- ✓ Configurable Event-based Controlled Record



by ISAM activities, including orbital debris considerations.”

This is not the commission’s first foray into space debris regulation. It has been reviewing the orbital debris mitigation plans of non-Federal satellites and systems for more than 20 years as part of its licensing and grants for space systems. The commission asserts its authority to regulate orbital debris derives from the Communications Act of 1934, as amended, which provides this authority to license radio frequency uses by satellites.

assign numerical values to collision risk, probability of successful post-mission disposal, and casualty risk associated with those satellites that will re-enter earth’s atmosphere.” Among other things, the rule changes also levied new disclosure requirements on satellite applicants related to protecting inhabitable spacecraft, maneuverability, use of deployment devices, release of persistent liquids, proximity operations, trackability and identification, and information sharing for situational awareness.

And yet, others in the interagency

or modifications to the commission’s licensing rules and processes that would facilitate ISAM capabilities.

**Satellite Servicing Missions:** Any additional licensing considerations unique to satellite servicing missions including servicing missions consisting of multiple spacecraft.

**Assembly, Manufacturing and Other**

**Activities:** Any special considerations in licensing of assembly and manufacturing missions.

**International Considerations:** Whether and how to take into account that ISAM missions also raise the possibility of interactions between operators under the jurisdiction of multiple nations in the commission’s licensing process.


**Orbital Debris Mitigation:** The implications of updated practices and approaches to stored energy and potential byproducts from in-space assembly.

**Orbital Debris Remediation:** Whether and how the commission should consider active debris removal as part of an operator’s orbital debris strategy.

**Activities Beyond Earth’s Orbit:** Any updates to the commission’s rules that might facilitate licensing ISAM missions beyond Earth’s orbit, including missions to the Moon and asteroids.

**Encouraging Innovation and Investments in ISAM:** Ways to facilitate development of and competition in ISAM activities, provide a diversity of on-orbit service options and promote innovation and investment in the ISAM field.

**Digital Equity and Inclusion:** How the topics discussed and any related proposals may promote or inhibit advances in diversity, equity, inclusion and accessibility, as well as the scope of the commission’s relevant legal authority.

Insofar as all commercial satellites may be affected by this proposal, the PNT community should engage. Will this latest FCC foray into potential space debris rulemaking protect, or lay waste to, the industry’s chances of reaching the space-high projected valuation of \$8,817.3 million by 2031? Only time..and space...will tell. 

## Interested in learning more about space debris?

Read these research reports, articles and the new U.S. implementation plan:

- [rand.org/content/dam/rand/pubs/research\\_reports/RR2900/RR2970/RAND\\_RR2970.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2970/RAND_RR2970.pdf)
- [space.com/kessler-syndrome-space-debris](https://space.com/kessler-syndrome-space-debris)
- [nationalgeographic.com/science/article/space-junk](https://nationalgeographic.com/science/article/space-junk)
- [whitehouse.gov/wp-content/uploads/2022/07/07-2022-NATIONAL-ORBITAL-DEBRIS-IMPLEMENTATION-PLAN.pdf](https://www.whitehouse.gov/wp-content/uploads/2022/07/07-2022-NATIONAL-ORBITAL-DEBRIS-IMPLEMENTATION-PLAN.pdf)

In 2000, for example, it adopted rules requiring disclosure of plans to mitigate orbital debris for licensees in the 2 GHz mobile-satellite service. Those were the basis for rules applicable to all services that were adopted shortly thereafter (Establishment of Policies and Service Rules for Mobile Satellite Service in the 2 GHz Band, Report and Order, 15 FCC Rcd 16127, 16187-88, paras. 135-138). In 2004, it adopted a comprehensive set of rules on orbital debris mitigation (2004 Orbital Debris Order, 19 FCC Rcd at 11575, para. 14).

Just two years ago, it held an orbital debris proceeding, Mitigation of Orbital Debris in the New Space Age. It sought public comment on a variety of areas for rule updates, including an “active debris removal” as a debris mitigation strategy for planned proximity operations. While it concluded more detailed regulations would be premature, the resultant report nevertheless updated the commission’s satellite rules on orbital debris mitigation for the first time in more than 15 years.

The 2020 FCC rule changes included “requiring that satellite applicants

balk at what some have referred to as the FCC’s continued stretching of its legal limits. The 2020 rule changes apparently stirred up considerable debate and controversy. Despite objections from the Department of Defense and other government agencies, the FCC pressed ahead.

### PNT Industry Impacts?

Fast forward to today. Comments on the FCC’s latest space-based regs focused on ISAM issues are due 45 days following publication in the Federal Register (August 5). Here is the list of topics for which the commission seeks comment. (Note the commission includes space debris as part of ISAM for purposes of this drill):

#### Spectrum Needs and Relevant Allocation:

The variety of radiofrequency communications links that could be involved in ISAM missions.

**Licensing Processes in General:** Any updates



**Read the FCC’s ISAM document:** [fcc.gov/document/fcc-opens-proceeding-servicing-assembly-manufacturing-space-0](https://www.fcc.gov/document/fcc-opens-proceeding-servicing-assembly-manufacturing-space-0)



0.02°  
RTK Roll/Pitch

0.06°  
RTK Heading

1 cm  
RTK/PPK Position

## QUANTA MICRO

### Outstanding Performance/ SWaP-C

- » Tactical grade IMU: 0.8°/h Gyro Bias Instability
- » Robust to Vibrating Environments
- » Post-processing with Q inertia PPK Software
- » Quad-Constellation Multi-Band RTK GNSS receiver



Single or Dual  
Antenna

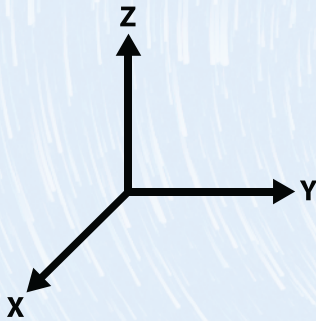


Highly Tested  
and Calibrated



Q inertia PPK  
Software





**THE INERTIALIST** is a regular feature in every issue of *Inside GNSS*. This expert-authored column explores operational principles and the state-of-the-art of this key navigation technology. It discusses main principles, current technological trends and system integration aspects of inertial navigation. These include:

- aspects of inertial navigation mechanization (system initialization, integration algorithms, non-inertial effects, compensation of coning and sculling);
- trends in sensor technologies (micro-electromechanical systems or MEMS, fiber optic and ring laser gyros, cold atom interferometry);
- fusion with other sensors (integration approaches and example implementations) and,
- system implementation aspects (time synchronization, bandwidth and vibration profiles, and the influence of latencies under high dynamics).

We welcome questions and suggested topics of specific interest from the readers of *Inside GNSS*. Please contact us at [Andrey@insidegnss.com](mailto:Andrey@insidegnss.com).

## INS-CENTRIC SENSOR FUSION

The main principals of fusing inertial navigation with other sensors.

As discussed in previous columns, inertial navigation systems (INS) enable a fully self-contained navigation capability. Yet, integration is a fundamental operation of INS mechanization. Input measurements of non-gravitational acceleration (also referred to as specific force) and angular rate vectors are integrated into attitude, velocity and position outputs. Measurement errors are integrated as well, which leads to the output drift over time. As a result, even the highest-quality inertial systems must be periodically adjusted.

To mitigate inertial drift, INS has been coupled with other navigation

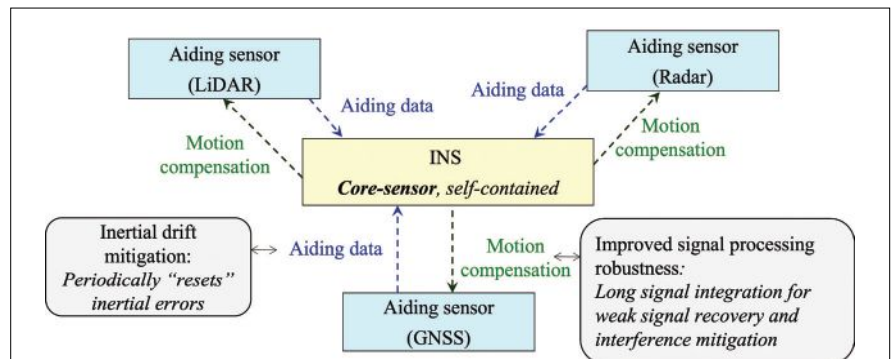
aids. GNSS is the most popular one, but numerous other aiding sources also have been applied such as electro optical (EO) sensors (vision and LiDAR), radars (including synthetic aperture radar), terrain data bases, magnetic maps, vehicle motion constrains, and radio frequency (RF) signals of opportunity (SOOP) to name a few. In this column, we consider the main principles of fusing inertial navigation with other sensors.

### Sensor Fusion Architecture

**Figure 1** illustrates the sensor-fusion approach.



**Andrey Soloviev**, author of *The Inertialist*, is a principal at QuNav. His research and development interests focus on sensor-fusion and signal-processing implementations for GNSS-degraded and GNSS-denied applications. He received his Ph.D. in electrical engineering from Ohio University, the Institute of Navigation (ION) Early Achievement Award and the RTCA William Jackson Award. He will occasionally bring in other subject matter experts to aid in the discussion.



**FIGURE 1** INS-centric sensor fusion.



# YOUR OWN INERTIAL TEST LAB

*Without Having To Own An Inertial Test Lab*

The Inertial Testing Lab (ITL) in Phoenix, Arizona, uses a high-performance 3-axis rate table with an integrated thermal chamber and a linear shaker to provide turnkey solutions for almost all types of inertial tests, including:

- Bias Over Temperature
- Scale Factor Error
- Misalignment
- Bias G-sensitivity
- Vibration Rectification
- Many Other Tests



[www.ideal-aeromsmith.com](http://www.ideal-aeromsmith.com) | 1.800.229.2451

INS is used as a core sensor. It is augmented by aiding navigation data sources (such as GNSS or LiDAR) to mitigate the drift in inertial navigation outputs. Aiding sources generally rely on external observations or signals that may or may not be available. Therefore, they are treated as secondary sensors.

When available, aiding measurements are applied to reduce the drift in inertial navigation outputs. In turn, inertial data can be used to improve the robustness of an aiding sensor's signal processing component, which is generally implemented in a form of motion compensation. For instance, INS-based motion compensation can be used to adjust replica signal parameters inside a GNSS receiver's tracking loops to increase the signal accumulation interval, thus recovering weak signals and mitigating interference (jamming, spoofing and multipath). Another example is compensation of motion-induced distortions in EO imagery.

To mitigate inertial drift, sensor fusion uses the complementary estimation approach, which is illustrated in **Figure 2**.

As shown in **Figure 2**, differences between INS and aiding observations ( $\hat{z}_{INS}$  and  $\hat{z}_{Aiding}$ ) are applied to estimate inertial error states instead of navigation states. Error state estimates are then subtracted from the INS solution, thus providing the overall navigation output. Specific structure of the observation vector  $z$  depends on the integration mode.

The complementary formulation estimates INS error states rather than estimating full navigation states. As compared to the full-state formulation, the main benefit of complementary estimation is a significantly simplified modeling of state transition. Inertial errors are propagated over time instead of propagating navigation states themselves. In this case, the process noise is completely defined by stability of INS sensor biases, as well as sensor noise characteristics. On the contrary, modeling of actual motion generally needs to accommodate different motion segments (such as a straight flight

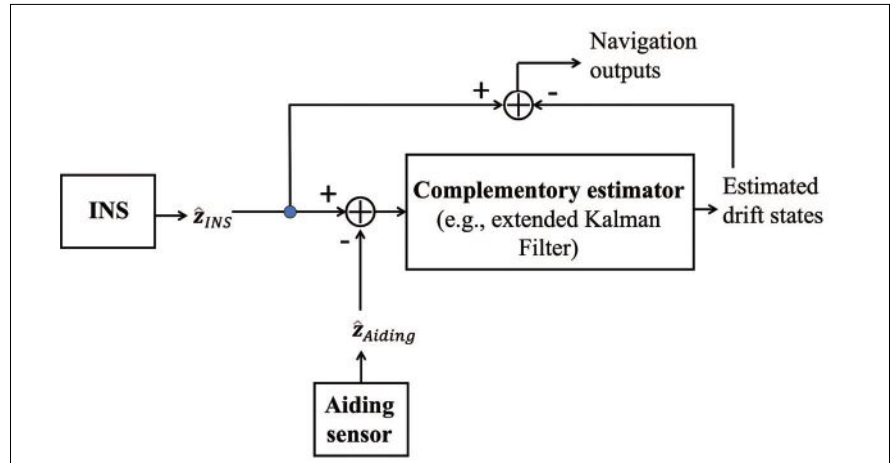


FIGURE 2 Complementary form of INS-centric sensor fusion.

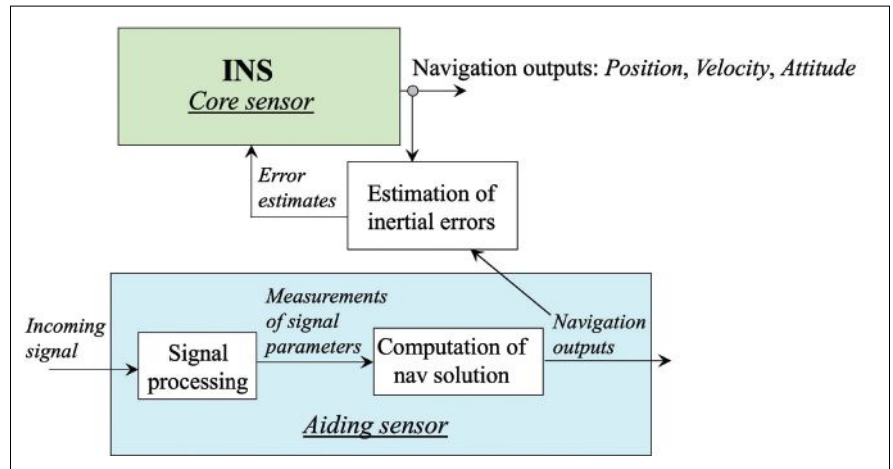


FIGURE 3 Loosely coupled sensor fusion.

versus a turn maneuver), which can require ad hoc tuning to optimize the performance. Moreover, propagation of navigation states through INS mechanization is a non-linear process.

In contrast, time propagation of inertial errors into navigation outputs can be efficiently linearized. As a result, complementary filters can generally rely on computationally efficient linear filtering techniques such as an extended Kalman filter (EKF) while reserving non-linear estimation approaches, such as particle filters and factor graphs, only to cases where aiding measurements are non-linear/non-Gaussian by nature, such as database aiding updates.

The integrated system operates recursively on the inertial update cycle. Every time a new measurement arrives from an inertial measurement unit (IMU), INS navigation computations

are performed followed by the prediction update of the complementary filter. If an aiding navigation output becomes available after the previous IMU update, it is used to compute complementary filter observables and apply them for the estimation update. Otherwise, error estimates are assigned their predicted values and computations proceed to the next inertial update.

**Integration Modes**

The three main sensor fusion modes include loose coupling, tight coupling and deep coupling. They perform sensor fusion at the navigation solution level, measurement level and signal processing level, respectively. Their key features are:

**Loose coupling**

**Figure 3** shows a high-level diagram of a loosely coupled system mechanization





# GPS NETWORKING

## GPS Rack Mount Amplified Splitter

Ideally suited for timing and testing applications where the GPS carrier signal is required by up to 32 devices simultaneously.

● Test Labs

● Cellular Markets

● Public Safety

● Timing



\* Available in 1x8 1x16 1x32  
2x16 and 2x32

\* Standard Splitter options available 1x2 1x4 and 1x8

Contact us for custom system design or more information  
at 800-463-3063 or email [salestech@gpsnetworking.com](mailto:salestech@gpsnetworking.com)

[WWW.GPSNETWORKING.COM](http://WWW.GPSNETWORKING.COM)

that fuses inertial and aiding data at the navigation solution level.

Aiding sensors generally include a signal processing part and a navigation solution part. The signal processing part receives navigation related signals and measures their parameters. For example, GNSS receiver tracking loops measure parameters (pseudoranges, Doppler frequency shift and carrier phase) of received GNSS signals. Another example is a LiDAR time-of-flight measurement that is directly related to the distance between the LiDAR and a reflecting object. Signal parameter measurements are then applied to compute the navigation solution. For example, GNSS pseudoranges are used to compute the GNSS receiver position. Changes in distances to reflecting stationary objects are exploited to compute the change in the LiDAR's position.

Note the navigation solution can only be computed if a sufficient number of signal measurements is available. For example, at least four pseudoranges must be available to compute the GNSS-based position. At least two non-collinear lines must be extracted from an image of a two-dimensional (2D) LiDAR image to compute a 2D position. Depending on the aiding sensor, the observation vectors,  $\hat{z}_{INS}$  and  $\hat{z}_{Aiding}$  can include, position, velocity, attitude and their combinations.

The loosely coupled approach operates at the navigation solution level and does not require any modifications to the aiding sensor. Yet, a key limitation

of loosely coupled fusion is it cannot estimate INS error states unless a complete aiding solution is available. For instance, loosely coupled GNSS/INS cannot update inertial drift terms in an urban canyon when the GNSS position cannot be computed even though limited satellite measurements may still be available. As a result, useful aiding information is inherently lost.

**Tight coupling**

Tight coupling applies measurements of aiding signal parameters for the INS drift mitigation. As compared to loose coupling, the main benefit of tightly coupled systems is the ability to (partially) update INS error states even when insufficient aiding data are available to compute a full navigation solution, such as when less than four GNSS satellites are visible.

For such cases, a GNSS only position solution cannot be calculated. As a result, loosely coupled systems experience a complete GNSS outage. In contrast, the tightly coupled method can use limited GNSS measurements, thus enabling (partial) mitigation of the INS error drift. Another example of tight coupling is an EO-aided INS where landmark features are extracted from imagery data and then applied for the INS drift mitigation. When limited landmarks are present, and the system cannot compute an EO-based position update, individual feature measurements still enable INS drift mitigation within the tightly coupled architecture.

**Figure 4** illustrates the tightly coupled approach.

For tight coupling, the INS error estimation generally has to be augmented with the estimation of aiding sensor errors. For example, GNSS receiver clock errors (bias and drift) are included into the system state vector for the GNSS/INS integration case. Image-aided inertial augments the system states with misalignment between INS and camera (or LiDAR) sensor frames.

Similarly to loose coupling, complementary estimation observables are formulated as differences between actual measurements and their INS-based estimates. To illustrate, for GNSS/INS, complementary pseudorange observations are formulated as differences between their INS estimates and GNSS measurements:

$$z_p^{(k)} = \hat{p}_{INS}^{(k)} - \hat{p}_{GNSS}^{(k)} \tag{1}$$

In **Equation 1**,  $\hat{r}_{INS}^{(k)}$  is the geometrical range to the  $k^{th}$  satellite. It is estimated using INS position solution,  $\hat{x}_{INS}$ , and satellite position vector,  $x_{SV}^{(k)}$ :

$$\hat{r}_{INS}^{(k)} = |\hat{x}_{INS} - x_{SV}^{(k)}| = |x + \delta x_{INS} - x_{SV}^{(k)}| \approx r^{(k)} - (e^{(k)}, \delta x_{INS}) \tag{2a}$$

where:

$$e^{(k)} = \frac{x_{SV}^{(k)} - \hat{x}_{INS}}{|x_{SV}^{(k)} - \hat{x}_{INS}|} \tag{2b}$$

In **Equation 2**,  $x$  is the true position,  $\delta x_{INS}$  is the INS position error,  $r^{(k)}$  is the true range between the receiver and satellite  $k$ ,  $(\cdot, \cdot)$  is the vector dot product, and  $|\cdot|$  is the Euclidian norm.

The GNSS pseudorange measurement model is:

$$\hat{p}_{GNSS}^{(k)} = r^{(k)} + c\delta t_{rcvr} + \epsilon \tag{3}$$

where  $c$  is the speed of light,  $\delta t_{rcvr}$  is the receiver clock bias, and  $\epsilon$  is the pseudorange measurement error that includes thermal noise, multipath, atmospheric delays, and orbital errors.

From **Equations 3 and 4**, the complementary observation is formulated as:

$$z_p^{(k)} = -(e^{(k)}, \delta x_{INS}) - c\delta t_{rcvr} - \epsilon \tag{4}$$

The EKF is commonly applied to estimate INS error states and GNSS receiver clock states.

As mentioned previously, the main benefit of tight coupling is the ability

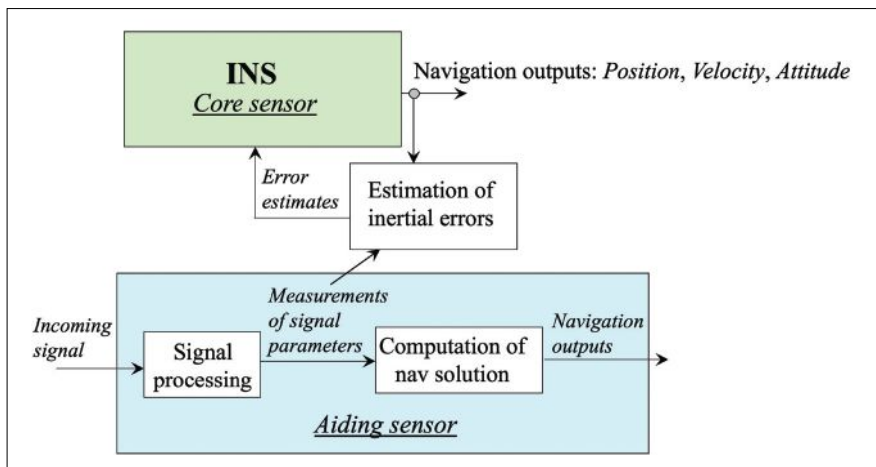


FIGURE 4 Tightly coupled sensor fusion.



A new era in fiber optic sensors  
has arrived



## Introducing KVH IMUs with PIC Inside™

With improved reliability and environmental survivability over competing technologies, KVH's new family of IMUs all feature exclusive photonic integrated chip (PIC) technology. This breakthrough technology reimagines fiber optic gyros by replacing individual fiber components with an integrated planar optic chip.

Already offering outstanding shock and vibration resistance, KVH has also upgraded its IMUs with high-performance accelerometers that further enhance system performance. The result is a series of robust inertial sensors designed to deliver the performance and reliability that autonomous platforms demand:

- Excellent Bias Stability
- High Bandwidth
- Low Noise
- Improved Orientation Stability



Learn more at: [www.kvh.com/pic](http://www.kvh.com/pic)

to implement estimation updates even when limited signal measurements are available. As a drawback, it may require a firmware modification of the aiding sensor to enable access of its signal measurements, which are also referred to as raw measurements.

**Deep coupling**

Deep coupling fuses inertial and aiding data at the signal processing stage. This approach keeps measurement-domain estimation of INS error states (as in tight coupling) and adds INS-based motion compensation to robustify the signal processing component of the aiding sensor. **Figure 5** shows a high-level block diagram of the deeply coupled approach.

For GNSS/INS, various deeply integrated implementations, which are also referred to as ultra-tight coupling, have

been reported in the literature. Both deep and ultra-tight systems are designed to improve the post-correlation signal to noise and interference ratio (SNIR). The distinction between deep and ultra-tight approaches can be somewhat vague. Ultra-tight coupled implementations generally maintain GNSS tracking loops and use inertial aiding to narrow their bandwidths. Deep integration operates directly with GNSS IQ samples. This is done by (i) processing IQ data with a combined pre-filter/Kalman filter scheme; or, (ii) explicitly accumulating IQ samples over an extended time interval (i.e. beyond the unaided receiver implementation).

Deep coupling maximizes the benefits of sensor fusion as it fuses inertial and aiding data at the earliest processing stage

possible, thus eliminating any inherent information losses. However, it generally requires modification of the aiding sensor signal processing component. Yet, in some cases, these modifications still can be implemented via a firmware upgrade, for example, by providing access to high-frequency (1 kHz or similar) IQ outputs of GNSS correlators.

**Example Benefits**

This section considers two example cases that illustrate benefits of INS-centric sensor fusion. The first example is the integration of GNSS and inertial for ground vehicle applications. **Figure 6** shows example test results that compare loosely and tightly coupled system mechanizations. The system integrates a consumer-grade GNSS chipset, consumer-grade MEMS INS and vehicular motion constraints.

Cumulative error distribution results shown in **Figure 6b** clearly demonstrate the benefits of tight coupling over the loosely coupled approach. For example, the 90% bound of the horizontal position error is reduced from 15 meters to 6.5 meters, while the 95% error bound is reduced from 40 meters to 7.5 meters.

The second example illustrates the benefits of deep integration. Deep coupling for GNSS/INS (including weak signal recovery and interference mitigation) has been discussed by various research papers (including the first issue of The Inertialist column where we illustrated applications of deep integration for jamming and

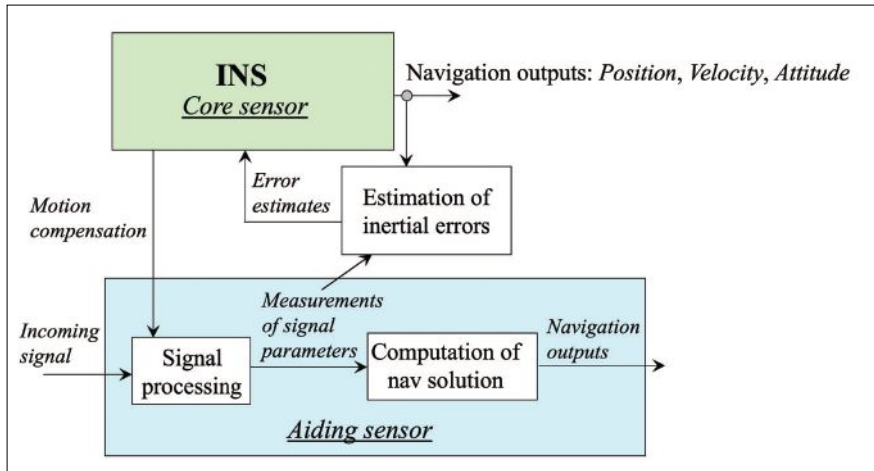


FIGURE 5 Deeply coupled sensor fusion.

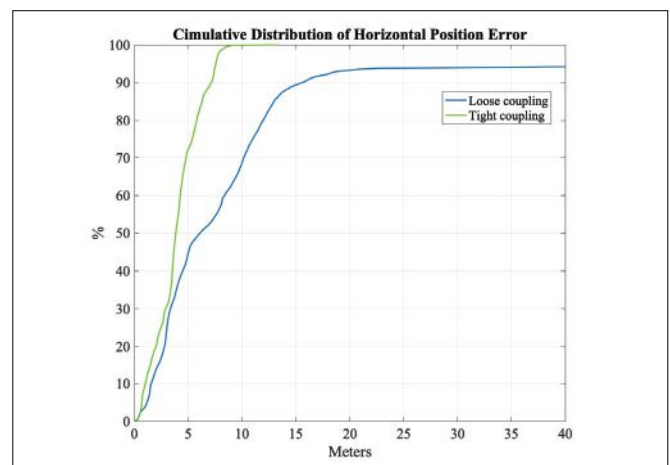
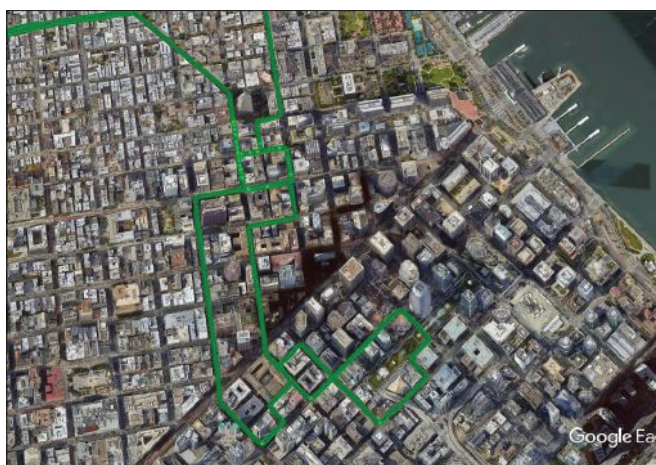


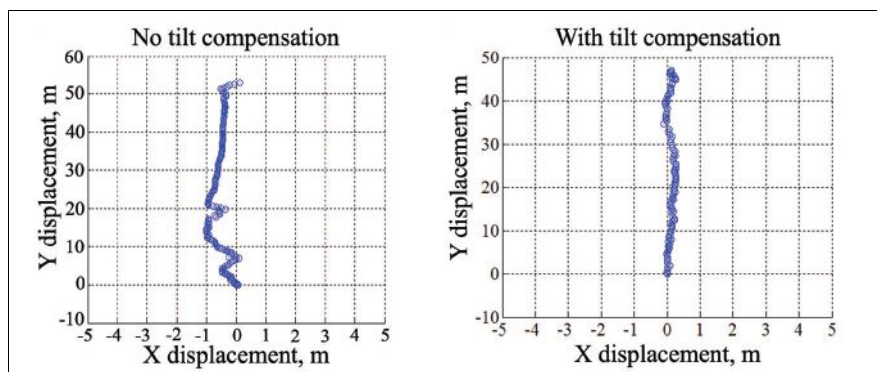
FIGURE 6 Example performance in dense urban environments: Integration of consumer-grade GNSS, consumer-grade MEMS INS and motion constraints for ground vehicle applications.

spoofing mitigation). In this section, example benefits are extended to non-GNSS aiding of inertial navigation.

**Figure 7** shows example test results for a LiDAR-aided inertial. In this case, inertial data is fused with measurements of line features that are extracted from images of a 2D scanning LiDAR. The tightly coupled implementation assumes the LiDAR scanning plane remains horizontal, which leads to distortions in the cross-track direction as shown in the left-hand plot. Deep coupling applies inertial data to adjust LiDAR images for tilting, thus improving the cross-track performance as shown in the right-hand plot of **Figure 7**.

### Conclusion


INS-centric sensor fusion uses self-contained inertial navigation as its core sensors and applies aiding data from other navigation aids to reduce drift in inertial navigation outputs. The complementary fusion enables seamless addition



**FIGURE 7** Example benefit of deep coupling for LiDAR/INS integration. Ground vehicle test example where the vehicle was driven in a straight line. The INS is used to compensate tilting of the 2D LiDAR, which improves the cross-track positioning performance.

of aiding data (when and if available); PNT continuity in various environments; and robust, resilient state estimation with outlier mitigation (e.g., non-line-of-sight GNSS and SOOP multipath in urban environments) via INS-based statistical gating of aiding measurements.

The three main fusion strategies include loose, tight and deep coupling that

subsequently increase the level of interaction between inertial and aiding sensors' navigation and signal processing components. Progressing from loose to deep coupling improves the navigation accuracy and robustness. It may require modifications on the aiding sensor side, which in many cases can be accomplished via firmware upgrades. 

Tallymatics integrates Tallysman antennas, a u-blox F9x GNSS receiver and the PointPerfect augmentation service into the **TW5390** multi-constellation and multi-band smart GNSS antenna.



**Accutenna® technology**

- Multi-constellation and multi-signal support*
- Mitigates out-of-band interference*
- Excellent multipath rejection*
- IP69K waterproofing*



WOW!



*F9x receiver family*

*Supports SPARTN L-Band corrections*

*PointPerfect + PPP-RTK and RTK augmentation*

*Dead reckoning (IMU)*

Join us at **INTERGEO 2022** in Essen, Germany - Hall 1 B1.020

 **TALLYMATICS®** A GALIAN® COMPANY

**tallymatics.com**



Rokubun, leading the HANSEL initiative, has set up an intelligent and flexible ‘smart city’ infrastructure at The European Space Agency’s sprawling ESTEC facility in Noordwijk. The innovative system establishes the basis for future living space control and monitoring networks that will deliver key position-based services and other benefits for both citizen inhabitants and urban authorities.

## ESA ESTEC gets smart city treatment



Photo courtesy of ESA.



### PETER GUTIERREZ

*Inside GNSS's* European correspondent, is a senior reporter and editor based in Brussels, Belgium, who has written about Europe's GNSS programs for many years. He received his bachelor's degree from the University of Texas at Austin and a M.S.

degree from the University of Massachusetts at Amherst.

The smart city scenario has become a familiar one to followers of high-tech. Picture here, if you will, living spaces where lights and information and entertainment systems switch on and off automatically as you move from room to room and from building to building, urban factories and warehouses staffed by autonomous robots operating without human intervention, transport systems where driverless taxis pull up to the curb right when you need them and where drones and other unmanned delivery vehicles place goods into your hands within minutes, wherever you may be.

Such spaces, first imagined by science fiction writers, are no longer a promise of the distant future, but are, slowly but surely, becoming a present-day reality.

“A smart city is an urban environment that exploits information and communication technology to improve the operational efficiency of the services delivered there,” said Miquel

Garcia-Fernandez, CTO and co-founder of Barcelona-based Rokubun, a company that develops high-accuracy navigation solutions for mass-market devices. Rokubun leads the HANSEL project, demonstrating how to design and implement smart city infrastructure, using for its testbed the European Space Agency’s (ESA) European Space Research and Technology Centre (ESTEC) in Noordwijk, the Netherlands. The largest of several ESA facilities spread across Europe, ESTEC is known to visitors from around the world as the home of ESA’s renowned Space Expo. It also houses one of the world’s most advanced navigation laboratories, the aptly named ESTEC Navigation Laboratory.

“ESTEC is not a city,” Garcia-Fernandez said, “but it is a large campus, with buildings, vehicles and streets, and it does resemble the urban environment. As such, it features the most common GNSS hazards that occur in a city, such as obscured

view, multipath, and so on, making it the perfect setup to test and validate new technologies.”

Applications and services associated with smart cities are, by all accounts, likely to depend on well-conceived, seamless positioning, navigation and timing (PNT) infrastructure. ESTEC Radio Navigation Engineer Rui Sarnadas, ESA’s onsite project officer for HANSEL, said, “The prime goal of the HANSEL testbed demonstrator is to integrate various technologies in the field of positioning and navigation. What we have at ESTEC is a delimited geographic and administrative area in which different types of electronic data collection sensors can request, provide and exchange information among themselves within a managed network.”

A fundamental aspect of HANSEL, and one of the things that make it so innovative when compared to other smart city initiatives, is the network exchanges are performed via a centralized server, the brain of the smart city, so to speak, and not in a direct peer-to-peer fashion. This allows for the execution of monitoring and control activities, as well as ad-hoc deployments, test campaigns and data collection for analysis.

### GNSS plus

“Besides the cornerstone GNSS applications,” Sarnadas said, “the testbed deploys sensors and services leveraging on Wi-Fi and cellular infrastructure, with the objective of exploring and characterizing different PNT techniques such as GNSS+Wi-Fi hybridization, GNSS+cellular snapshot positioning, RTK and GNSS cooperative positioning.”

The target, he said, is to demonstrate the concept of connected infrastructure that enables users to take advantage of the different technologies readily available in an urban context, for example via network connectivity and Android applications.

“With the HANSEL project, we’re providing more accurate and robust positioning capabilities,” Garcia-Fernandez said. “The main components of the testbed revolve mostly around satellite

navigation systems and include collaborative positioning technology of user terminals, GNSS snapshot receivers to monitor interference and jamming, and the deployment of Wi-Fi access points and terminals that are compliant with the 802.11mc protocol.”

Under HANSEL, GNSS and Wi-Fi are hybridized in a tight coupling strategy, at the ranging level. Compliance with the 802.11mc, specifying the set of media access control and physical layer protocols for implementing Wi-Fi communication, enables precise measurement of the travel

**“WITH THE HANSEL PROJECT, WE’RE PROVIDING MORE ACCURATE AND ROBUST POSITIONING CAPABILITIES. THE MAIN COMPONENTS OF THE TESTBED REVOLVE MOSTLY AROUND SATELLITE NAVIGATION SYSTEMS AND INCLUDE COLLABORATIVE POSITIONING TECHNOLOGY OF USER TERMINALS, GNSS SNAPSHOT RECEIVERS TO MONITOR INTERFERENCE AND JAMMING, AND THE DEPLOYMENT OF WI-FI ACCESS POINTS AND TERMINALS THAT ARE COMPLIANT WITH THE 802.11MC PROTOCOL.”**

Miquel Garcia-Fernandez,  
CTO and co-founder, Rokubun

time, i.e. ranges instead of signal strength, between terminals and access points. This creates a seamless indoor/outdoor positioning system, a firm foundation into which other ranging-based systems can be integrated, such as ultra-wideband [UWB] or 5G. “With an affordable reference GNSS receiver used with our testbed,” Garcia-Fernandez said, “we can achieve accurate positioning in a smart city scenario by means of RTK.”

“Of course, we’re working at a smaller scale than an actual city,” Sarnadas said, “but the system as implemented provides us a valuable means for deployments,

experimentations and tests in our controlled setting. Having roads, buildings, canopy and indoor environments similar to an open-sky and light urban settings, we gain the advantage of having end-to-end control over the deployment, meaning location and type of sensors, users, etcetera, and the testbed services themselves. Bringing together all of the available infrastructure—not only GNSS-related but also the Wi-Fi and cellular networks—we are able to exercise, generate and assess test scenarios for different applications.”

HANSEL has carried out a number of GNSS+Wi-Fi positioning experiments with a single smartphone, cooperative positioning using GNSS measurements with two smartphones, and snapshot positioning with GNSS+cellular SDR-based sensors and remote processing.

Sarnadas said HANSEL is delivering a number of real benefits: “One clear example is the expected increase in position solution availability and accuracy, when GNSS stand-alone solutions are impaired or simply not available. For this, the use of Wi-Fi RTT [Round-Trip-Time] measurements, of cooperative positioning, or of hybridization with cellular measurements, is fundamental.”

With the HANSEL system in place, where sensors, users and infrastructure can be mapped, supervised and maintained, additional benefits become evident. “To name a few,” Sarnadas said, “we can see energy saving by provision of a snapshot processing service, both for GNSS and cellular receivers, improved accuracy for GNSS users thanks to the availability of a controlled base station for RTK. We can deliver better hybrid positioning services by maintaining and disseminating accurate locations and timing for cellular base stations and Wi-Fi access points.”

Better quality of service (QoS) is assured using a network of sensors for spectrum monitoring and interference detection and localization. Safety and security are increased via protected communications for authorized users only, and data exchange over a dedicated, private, smart city network.

“Finally,” Sarnadas said, “we believe we can get more efficient resource usage using centralized asset tracking and monitoring, with potential for optimizations and real-time management of registered positioning measurements, for example traffic jams, emergency situations and ad hoc deployments.”

### Like clockwork

Rokubun is working with a number of key partners on the HANSEL project.

“The Links Foundation has provided the expertise in the design and requirement specifications of a navigation testbed that may be potentially used in a smart city context,” Garcia-Fernandez said, “while Politecnico di Torino, in Italy, has been responsible for the design and implementation of a collaborative positioning system based on GNSS for smartphones.”

The Universitat Autònoma de Barcelona designed and implemented the GNSS snapshot capabilities for interference and jamming monitoring and Spain’s Traffic Now is responsible for the testbed web interface design.

“At Rokubun, we have been the prime contractor and responsible for the design of the testbed architecture, deployment of the complete system, including the GNSS reference station, and also the definition and implementation of the GNSS + Wi-Fi hybridization technology,” Garcia-Fernandez said.

“We wanted to deploy a smart city initiative at ESTEC to enhance our infrastructure in support of multiple R&D and industrial activities,” Sarnadas said. “In this sense, we wanted the HANSEL testbed to give us more flexibility on the campus, effectively bringing ESTEC closer to a ‘smart campus.’”

ESA issued a call for tenders under its Technology Development Element (TDE) program, aimed at providing concepts and demonstrators, at lower technology readiness level (TRL), for key ESA technology objectives.

“In this framework,” Sarnadas said, “the activity ‘Navigation and GNSS in Smart Cities – Testbed Concept Definition,’ now known as HANSEL, was introduced to capture a set of positioning



Photo courtesy of Peter Gutierrez.

Visitors know ESTEC as the home of ESA’s Space Expo.

**“WE TOOK A STEP-BY-STEP APPROACH WITH THE HANSEL DEPLOYMENT. IT IS NOT ONLY A TESTBED BUT ALSO AN R&D TOOL IN ITSELF.”**

ESTEC Radio Navigation Engineer Rui Sarnadas,  
onsite project officer for HANSEL, ESA

and navigation technologies and techniques in a comprehensive and flexible testbed that allows real-world demonstration of the main concepts.”

Under ESA’s tender procedure, a number of excellent proposals were comprehensively evaluated.

“For ESA, the task is never straightforward,” Sarnadas said, “since we are fortunate enough to receive very good proposals from multiple European players, from industry to academia. In the end, the HANSEL proposal covered all the objectives and tasks that were called for and the consortium brought forward indispensable expertise in the relevant areas.”

“This was a competitive process,” Garcia-Fernandez said. “Once we were selected, the execution of the project ran through several phases—design, implementation and testing—all

closely monitored by ESA technical officers through regular reporting as well as in-depth technical meetings and reviews at the end of each phase.”

In the run-up to the deployment of HANSEL at the ESTEC site, the team carried out a series of key tests on a football field, where a reference station like the one to be used at ESTEC was employed to demonstrate precise positioning. The system successfully followed, with high accuracy, the trajectory of a GNSS receiver placed on a moving cart. Additional GNSS software receivers placed on the same cart were used to assess the testbed’s snapshot processing capabilities.

“We took a step-by-step approach with the HANSEL deployment,” Sarnadas said. “It is not only a testbed but also an R&D tool in itself. For example, although many services are exploited continuously, several sensors are not permanently fixed within the campus and can be moved around, configured and used in service of specific ad hoc campaigns. In this sense, as we are continuously developing and adapting our Navigation Laboratory facilities to support Europe’s navigation activities, HANSEL has become another building block in support of ESTEC’s infrastructure.

“The relationship with Rokubun and the entire consortium has been very good and extremely fruitful,” he said. “We had the chance to put together experts in the different technologies and applications, coming from a number of different backgrounds, and to get their full range of views on how to materialize the testbed. It should also be highlighted that HANSEL development partially coincided with the COVID-19 pandemic, especially during the field test campaigns, which of course was not without its challenges. But it also reinforced the importance of the good working relationship within the whole team during the project.”

### Next steps

One of the key requirements of the HANSEL testbed was that it be easily expandable to include additional capabilities and upgrades.

“HANSEL could be potentially used to control, for example, delivery robots



operating in a smart city,” Garcia-Fernandez said, “or to monitor certain receivers and incorporate new technologies for navigation such as UWB, Bluetooth, 5G and others, which will make GNSS more resilient against things like multipath, interference and/or spoofing.”

In terms of marketable applications, he said, “High-accuracy, indoor location through the hybridization of GNSS with other ranging technologies such as Wi-Fi, UWB or Bluetooth, would be of great use for indoor navigation and guidance in retail, trade fair and congress scenarios. And we also see potential for navigation systems based on vehicle-to-vehicle [V2V] communication protocols with immediate applicability to the automotive market.”

For Sarnadas, the project has clear implications for GNSS users: “We can think of proliferation of dual-frequency, mass-market receivers, authentication


and high-accuracy services on one hand, and on the other hand we can have dedicated deployments for low-energy, snapshot and internet-of-things [IoT] use cases. The nominal GNSS user will continue to have targeted stand-alone solutions, although the existing GNSS caveats still play a role, those being impairments, interference, jamming, multipath, indoor penetration, visibility, etcetera.”

In the smart city context, 5G NR and ongoing standardization efforts will further enhance the capabilities not only of data communication but also of positioning services. “Another example is on the vehicular side,” Sarnadas said, “where V2X [vehicle-to-everything connectivity] also opens new avenues for exploiting user networks, data exchanges and inter-user ranging.”

However, there remain legitimate concerns about the security and privacy of these applications, especially where user data is exchanged. “In fact,” Sarnadas

said, “although the concept of smart-city-as-a-service does look like an interesting approach in many aspects, it should be leveraged against the target deployment objectives and core services to be provided.”

Ultimately, Sarnadas said, “the deployment and management of infrastructure and networks in a controlled way, leveraging proven technologies and standardization efforts, in combination with the privacy and security that such a dedicated deployment can be designed to achieve, will be key differentiators as smart cities become a reality.”

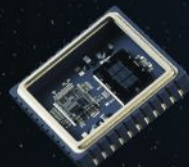
In all, the HANSEL system hosted at the ESTEC Navigation Laboratory, with its variety of linked sensors, has provided valuable insights into the kind of collective networking and computing needed to get a range of intelligent elements to mesh seamlessly together, essentially a blueprint for the ‘brain’ of a future smart city. 



Physical Logic

## MEMS: ALL THE RIGHT MOVES

Advanced MEMS accelerometers for multiple applications:  
taking accuracy to the next level



Inertial  
Navigation

Long Distance  
Application

North Finding  
& Target Location

Oil  
Drilling

Package Delivery  
Systems

Preventive  
Maintenance



# Thwarting GPS Spoofing Attacks

Verifying spoofing countermeasures based on sparse signal processing.

JUNHWAN LEE, ERICK SCHMIDT, NIKOLAOS GATSIS, DAVID AKOPIAN  
UNIVERSITY OF TEXAS AT SAN ANTONIO

**G**lobal Navigation Satellite Systems (GNSS) offer an irreplaceable service on providing Position, Velocity and Time (PVT) references for various applications. The growing reliance on GNSS has generated increased interest on its authentication, validity and security, which is undeniably challenging due to external interference. Inherently, the GNSS receiver is susceptible to experiencing a range of disturbances during long-distance satellite-to-receiver communication. The GNSS receiver can thus become a victim of a harmful third-party hacker, a situation the relevant literature shows is applicable and plausible [1],[2].

Major cybersecurity attacks against GNSS receivers include jamming and spoofing. While blocking one or more satellite channels, jamming attacks force the receiver tracking loop to be locked on a false high-powered correlation peak. Spoofing, often referred to as a smart attack, hijacks tracking correlation peaks with matched-power noise to create deviations in PVT solutions. Carefully

designed spoofing attacks can bypass basic Receiver Autonomous Integrity Monitoring (RAIM) detection mechanisms. This article outlines a framework that defines various types of spoofing attacks based on their sparsity characteristics and leverages the aforementioned properties toward showcasing and verifying spoofing countermeasures.

Smart grid, an infrastructure that has significant reliance on timing synchronization via GPS, is a vulnerable target for malicious spoofing actors. In the work of [3], scenarios where time synchronization attacks (TSAs) lead to failures in power system state estimation are illustrated, which may eventually cause failure to take a corrective action. Another significant application that has attracted prominent research and heavily hinges upon the position and velocity estimations of GNSS receivers is unmanned autonomous vehicle (UAV) navigation. The spatial spoofing research is rich in analyzing attack mechanisms, whose effects are chiefly showcased on UAVs or other vehicles [2],[4].

As much as the dangers of spoofing are manifested through research work, a plethora of publications attempt to introduce promising antispoofing countermeasures [5],[6]. In general, antispoofing countermeasures may offer two fundamental features. Initially, the algorithm captures abnormal behavior discovered during either baseband or signal-level search. The aforementioned process is commonly referred to as detection. Several mechanisms halt their mission once spoofing detection is attained. Mitigation goes beyond detection in that it rejects the attack signal and produces accurate PVT estimates.

Among the methodologies available in the literature, several target the baseband domain and strive to capture unpredictable or abnormal behaviors of any sort. More specifically, the relevant research often uses the observable changes on correlator peaks [7],[8], vector tracking loops [9] or power and automatic gain control [10],[11]. Such research sometimes requires supplementary circuitry to be included in off-the-shelf receivers or has to rely on one or more sophisticated receivers.

On the other hand, certain antispoofing techniques focus on the signal-level layer of the GPS receiver. These



# SERVO ACTUATORS FOR UNMANNED SYSTEMS

◀ Scan For DroneCAN / CAN Parameters List

## SG SERIES



Case Size:  
Product:

50mm  
SG50BL

33mm  
SG33BLT

15mm  
SG15BL

10mm  
SG10BL

### SERIES FEATURES

9.0~15.0V  
18.0~32.0V  
WIDE OPERATING  
VOLTAGES

IP68\*  
WATERPROOF  
CASE RATING

Circular /  
Gland Cable  
TWO CONNECTOR  
OPTIONS

\*SG10BL Excluded



9001:2015  
14001:2015  
CERTIFIED



MULTIPLE COMMAND PROTOCOLS AVAILABLE:



DroneCAN



## MD SERIES



Case Size:  
Product:

20mm  
MD950TW

16.8mm  
MD245MW

15mm  
MD250MW

13mm  
MD89MW  
MD85MG

11.6mm  
MD70MH  
MD65MG

10mm  
MD1455W  
MD1415H

### SERIES FEATURES

4.8~7.4V  
OPERATING  
VOLTAGE RANGE

SAME  
DIMENSIONS AS  
PWM  
COMMAND  
PROTOCOL

4-PIN  
CONNECTOR  
OPTION



Hitec Commercial Solutions proudly combines decades of aviation experience and in-house engineering talent, with formidable manufacturing, distribution, and support capabilities. Our talented team of professionals research, design and develop the latest in servo actuator and commercial drone technologies, and bring it all to life in our United States, South Korea, and Philippines manufacturing and testing offices.

techniques strive to detect anomalies in observable sequences such as carrier-to-noise ratio [12], and navigational drift [13],[14]. This article falls in the latter category and exploits common GPS observables, that is, pseudorange and pseudorange rate as a pair, to protect the receiver against malicious spoofing. Moreover, the presented algorithm is cost-effective; it can run on a single rudimentary receiver assisted with software routines such as the freely deployed Android software.

This article presents the basics of an algorithm that is capable of autonomous spoofing detection and mitigation of joint attacks against time and position. Specifically, the present work focuses on stationary receivers and, with respect to the position attack, it provides an effective method to capture and reject an attack against a single position coordinate. The developed model expands on our previous work [15] that deals with TSAs only.

**GPS Observable Pair**

The fundamental GPS observables we used to contrive the antispoofing mechanism are the pseudorange and pseudorange rate pair. These data are typically accessible in mobile phones, for example, with certain applications installed as well as off-the-shelf commercial receivers. This section briefly discusses the observable pair and how the PVT excursion is arranged.

Pseudorange ( $\rho_n$ ) refers to the computed satellite-to-receiver distance. The satellite and user position are respectively denoted by  $\mathbf{p}_n = [x_n \ y_n \ z_n]^T$  and user position  $\mathbf{p}_u = [x_u \ y_u \ z_u]^T$  where  $n = 1, 2, \dots, N$  refers to the total number of tracking satellites represented in Earth-Centered Earth-Fixed (ECEF) coordinates. The 3-dimensional Euclidean norm based on the difference in satellite-to-receiver positions can generate the true range of the user, which, however, differs from observed pseudorange reported by the receiver due to the induced clock biases at the satellite and user ends, respectively denoted by  $b_n$  and  $b_u$ .

$$\rho_n[k] = \|\mathbf{p}_n[k] - \mathbf{p}_u[k]\|_2 + c(b_u[k] - b_n[k]) + \epsilon_{\rho_n}[k] \tag{1}$$

where  $c$  represents the speed of light, and any Gaussian white noise is captured in  $\epsilon_{\rho_n}$ .

A complementary component in the measurement pair is Doppler rate, or alternatively referred to as the pseudorange rate. Caused by the effect of Doppler shift that is generated between maneuvering satellites and the receiver, the pseudorange rate must satisfy the following consistency requirement:

$$\dot{\rho}_n[k] \cong \frac{\rho[k] - \rho[k-1]}{\Delta k} \tag{2}$$

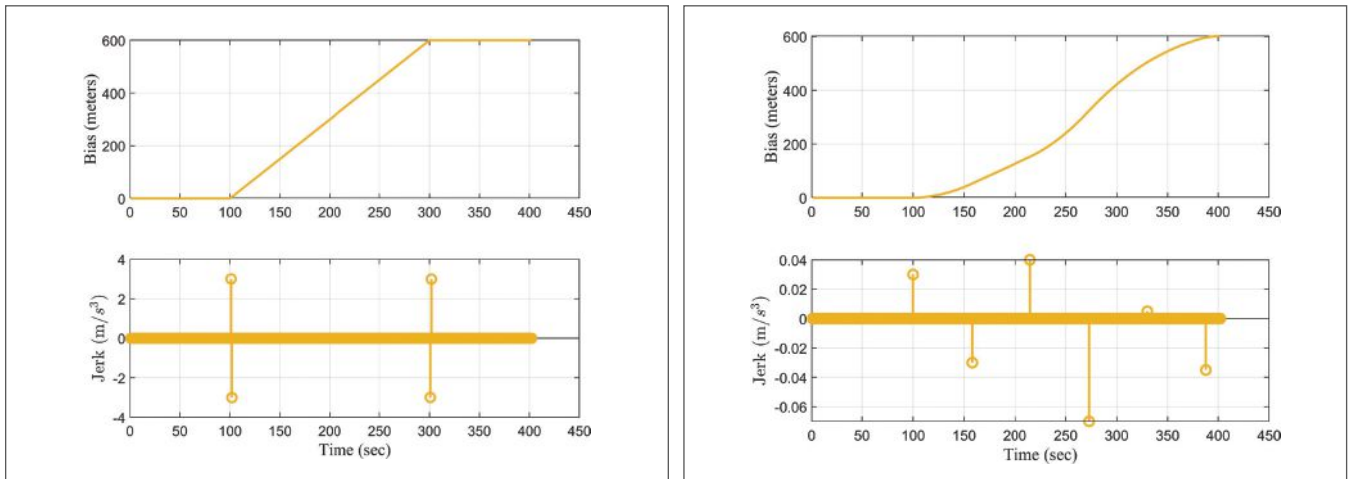
where satellite  $n$ 's velocity is referred to as  $\mathbf{v}_n = [\dot{x}_n \ \dot{y}_n \ \dot{z}_n]^T$  and the velocity of the receiver as  $\mathbf{v}_u = [\dot{x}_u \ \dot{y}_u \ \dot{z}_u]^T$ . During satellite-to-receiver data communication, the user readily obtains information in regard to all the visible satellites such as position ( $\mathbf{p}_n$ ), velocity ( $\mathbf{v}_n$ ), and clock

offset and bias ( $b_n$  and  $\dot{b}_n$ ), which in turn leaves user PVT variables ( $\mathbf{p}_u$ ,  $\mathbf{v}_u$ ,  $b_u$ , and  $\dot{b}_u$ ) as unknown.

Once measurement data was fully captured on the receiver, we performed a sanity check examination using Equation 2 to attain the validity of acquired data. The pair of pseudorange and pseudorange rate equations needs to be linearized for two reasons. The user position  $\mathbf{p}_u$  in Equation 1 is under the Euclidean norm, which is a nonlinear function. Also, considering pseudorange rate equation, though not stated in this article, includes the user velocity under the Euclidean norm as well.

Although general-purpose nonlinear programming (NLP) solvers are available, a linearized model can leverage the computational advantages of convex optimization solvers, namely rapidly calculating PVT solutions, without losing accuracy. The linearization is performed using Taylor series expansion. Because the present work is concerned with stationary receivers, the observed pair are linearized with respect to a fixed known user position reference,  $\mathbf{p}_{u,ref}$  and zero velocity reference  $\mathbf{v}_u = 0$ . See [17] for a detailed derivation of the linearization. To clarify the observed model versus linearized pair, we refer to linearized pseudorange and pseudorange rate as  $z_{\rho_n}$  and  $z_{\dot{\rho}_n}$ .

In the presence of spoofing, injected attacks are modeled as additive to the measurement pair. The following equations manifest the representation of



**FIGURE 1** Second and third orders bias attacks and their derivatives in acceleration and jerk domains, respectively. They depict sparsity in higher domains according to the attack order types.

spoofed pseudorange and pseudorange rate:

$$\begin{cases} z_{n,s} = z_{\rho_n} + s_{\rho_n} \\ \dot{z}_{n,s} = \dot{z}_{\rho_n} + \dot{s}_{\rho_n} \end{cases} \quad (3)$$

where  $S_{\rho_n}$  and  $\dot{S}_{\rho_n}$  represent spoofing signals injected on pseudorange and pseudorange rate, respectively. The attacked pseudoranges and pseudorange rates are conventionally provided as inputs to traditional algorithms such as Weighted Least Squares (WLS) or extended Kalman Filter (EKF), which output the PVT solutions to the end user. Thus, the abnormal behavior captured in pseudoranges is transferred on the PVT solutions.

### Spoofing Attack Order

In our previous work [15], we specifically consider TSAs and examine whether higher-order discrete-time derivatives of the spoofing signal are sparse, that is, exhibit spike-like behavior. This article extends the premise to attacks against a single position coordinate, and we specifically focus on the z coordinate in ECEF domain. Following [15], we analyze the smallest order derivative where the attack exhibits evident spikes and define the attack accordingly. For instance, a so-called Type I attack in [13] can be re-identified as a first order attack for the sparsity occurs in velocity domain, or equivalently in the first derivative of position.

Considering the bias domain, we define second order and third order attacks with examples depicted in **Figure 1**. The second order attack with increasing trend is shown in **Figure 1a**, whose second derivative (the acceleration) features two spikes at 100 and 300 seconds. **Figure 1b** depicts subtle gradual changes akin to third order attack where the sparsity is achieved on the third derivative (jerk domain). The chief advantage in defining spoofing profiles to benefit the development of antispoofing models is the fact that sparsity appears on the jerk domain for the majority of attacks reported in the literature.

### Spoofing Consistency

Attack consistency is inspired by the

measurement integrity in **Equation 2**. Applying the rationale to the spoofing signal, a consistent attack is required to satisfy the following condition:

$$s_{\rho}[k] = \frac{s_{\rho}[k] - s_{\rho}[k-1]}{\Delta k} \quad (4)$$

If the attacks fail to satisfy (4), it can be referred to as a non-consistent attack. An example of a consistent attack is TSA [13]. While fulfilling measurement integrity,

deviating signals on pseudorange and pseudorange rate are explicitly manifested on clock bias and drift. Particular applications vulnerable to TSAs are electric power grid operations that are driven by Phasor Measurement Unit (PMU) readings. PMUs are equipped with (stationary) GPS receivers, whose timing errors translate into voltage and current phase angle deviations. These

Visit us at  
ION GNSS+  
BOOTH 106

INTERGEO  
BOOTH  
F3.023

# MOTION SENSING ON ANY TERRAIN

DMU41  
P/N: 0300-00-0100  
P/N: 0300-00-0100

TOUGH, PRECISE INERTIAL SENSING FOR  
ULTRA-RELIABLE PERFORMANCE IN  
REAL-WORLD ENVIRONMENTS

Precision MEMS technology    Ultra-compact, easily integrated    Inertial sensors for all performance requirements



[siliconensing.com](http://siliconensing.com)

**SILICON SENSING**

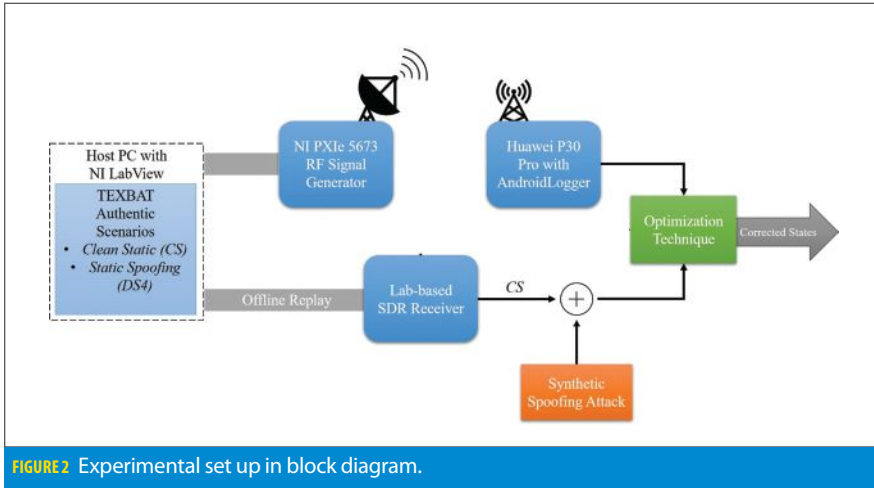


FIGURE 2 Experimental set up in block diagram.

can subsequently lead to erroneous state estimation for the power grid [20]. The authentic spoofing database TEXTBAT corroborates the aforementioned TSA characteristics, which also can be incited with baseband spikes.

In case of spatial spoofing, the attack may be defined as consistent or non-consistent depending on the targeted domain. If the spoofer aims to solely vary a position estimate and leaves the velocity domain intact, that would be an example of a non-consistent attack. Consistent spatial attacks result in modification on position and velocity domains.

This article considers attacks against two domains: TSA (clock bias  $b$ ) and single-coordinate position (coordinate  $z$ ), whereby time and spatial solutions are simultaneously affected. This condition is called a joint attack. In practical applications, such complicated spoofing can be achieved by having the receiver hacked by different data sources [21]. For joint attack simulation, we only examine consistent attack because TSA must be applied with the spoofing integrity.

### GPS Dynamic Equations

The GPS receiver is described by a dynamical system that follows the random walk model [16]:

$$\mathbf{x}_k = \mathbf{F}_k \mathbf{x}_{k-1} + \mathbf{w}_k \quad (5)$$

where  $\mathbf{x}_k$  stands for state variable vector,  $\mathbf{F}_k$  is the state transition matrix, and  $\mathbf{w}_k$  refers to the state transition noise. Although in a stationary environment, the position does not vary and the

velocities in  $x, y, z$  remain zero, Equation 5 is adopted in the present work because  $\mathbf{x}_k$  may contain deviating signals, and specifically, attacks that modify the solution in the  $b$  or  $z$  domains. Including the unknown  $\mathbf{x}_k$  as an optimization variable may be beneficial toward recovering the authentic PVT solution. Further, as mentioned earlier, the spoofing signal variables are appended for the system to delineate authentic PVT solutions with inflicting signals, with linearized measurement vectors  $\mathbf{z}_k = [z_\rho \ z_\beta]^T$ , which can be expressed as the following:

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{G}_k \mathbf{s}_k + \boldsymbol{\epsilon}_k \quad (6)$$

in which  $\mathbf{s}_k$  place-holds captured deviating signals introduced on  $z$ -position ( $s_z$ ), velocity, ( $s_v$ ), clock bias ( $s_b$ ) and drift ( $s_\beta$ ). Such formulation aims to capture the attack introduced onto the clock timing and  $z$ -domain. Lastly,  $\boldsymbol{\epsilon}_k$  represents the zero mean Gaussian measurement noise with covariance matrix  $\mathbf{R}_k = \text{diag}(\sigma_{\rho_1}^2, \sigma_{\rho_2}^2, \dots, \sigma_{\rho_N}^2, \sigma_{\beta_1}^2, \sigma_{\beta_2}^2, \dots, \sigma_{\beta_N}^2)$  that can determine uncertainties of observed measurements.

### Proposed Anti-Spoofing Technique

The proposed anti-spoofing technique is based on a minimization formulation that lends robustness against the spoofing attacks described earlier. The following minimization is performed as solver estimates  $\hat{\mathbf{x}} = [\hat{x}_1, \dots, \hat{x}_K]$ ,  $\hat{\mathbf{s}} = [\hat{s}_1, \dots, \hat{s}_K]$ :

$$(\hat{\mathbf{x}}, \hat{\mathbf{s}}) = \underset{\mathbf{x}, \mathbf{s}}{\text{argmin}} \left\{ \sum_{k=1}^N \|\mathbf{z}_k - \mathbf{H}_k \mathbf{x}_k - \mathbf{G}_k \mathbf{s}_k\|_{\mathbf{R}_k}^2 + \frac{1}{2} \sum_{k=1}^N \left( \|\mathbf{x}_k - \mathbf{F}_k \mathbf{x}_{k-1}\|_{\mathbf{Q}_k}^2 + \lambda_z \|\mathbf{D}_{s_z}\|_1 + \lambda_b \|\mathbf{D}_{s_b}\|_1 \right) \right\} \quad (7)$$

Equation 7 consists of four objectives that serve the anti-spoofing scheme. The first summation term is derived from the measurement in Equation 6. The second term examines the PVT behaviors in relation to the random walk model. The third and fourth terms, nominally referred to as penalization functions, each represent the higher-order domain where sparse spikes are likely to be displayed in position and clock aspects, respectively. The first and second terms jointly encourage PVT solutions that satisfy measurement integrity. With the help of penalization terms, the technique is capable of filtering accurate PVT estimations against attacks. The matrix  $\mathbf{D}$  constructs the third-order derivative of the respective sequences and is defined as follows:

$$\mathbf{D} = \begin{bmatrix} -1 & 3 & -3 & 1 & \dots & 0 \\ 0 & -1 & 3 & -3 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 3 & -3 & 1 \end{bmatrix} \quad (8)$$

The selection hinges upon the observation that realistic spoofing typically exhibits sparsity in the third-order derivative domain (jerk).

The performance of the technique depends on the selection of the factors  $\lambda_z$  and  $\lambda_b$ . These must be selected for each receiver. The proper values of  $\lambda_z$  and  $\lambda_b$  can tune the level of sparsity that emerges as solution from (7), as well as the relative emphasis that is placed among the four objectives in Equation 9. Proper tuning based on realistic attacks and in representative environments is therefore recommended.

Another parameter that affects the quality of the solution is the state noise covariance matrix. This must be set up with appropriate values corresponding to the static receiver. Overall, the optimization problem in (9) is a convex quadratic program that can be solved with relatively small computational effort.

### Simulation Methodology

To simulate and visualize the malignant effect of various spoofing types, we use a GPS receiver testbed that incorporates the wired and wireless signal transmission and reception simulations. We transmit a pre-recorded GPS signal via

signal generator, namely Clean Static (CS) scenario from TEXBAT database [1]. Interfaced with LabView developed software along with PCIe, the GPS signal transmitter uses a NI PXIe-1075 Chassis with a PXIe 5673 RF Signal Generator broadcasting via Vert 900 antenna.

Once transmitter setup is complete, the user has two choices as per the simulation. The unprocessed data is directly fed into the wired Software Defined Radio (SDR) developed in our lab [22], which rapidly processes the raw data into precise and comprehensible GPS information for the user. On the other hand, users can opt to deliver the signal over-the-air (OTA) via the connected antenna, in which the Huawei receiver, located about 5 to 6 meters away from the transmitter, captures and processes the signal with the GNSSLogger application [23].

The wireless route inherently contains more noise and consequently has higher uncertainties than the wired method. Thus, wired SDR empowers the PVT processing algorithms such as WLS and EKF to deliver more accurate position and time estimation. In this article, we exploit synthetically fabricated spoofing attacks while targeting a single position and time domain, namely z-domain in ECEF coordinate and clock bias estimation.

The attacks described next are synthetically added to the output of the TEXBAT CS scenario after it is replayed

over the SDR and the Huawei receiver. We initially confirm our algorithm attains robustness against TSA in various spoofing profiles as our previous works do [15], then simulation manifests the algorithm also can detect and mitigate the disturbance that aims to inflict 1) sole z-domain and 2) z-domain and clock bias simultaneously.

Each spoofing scenario is comprised of first, second and third order types of attacks while maintaining a minimum of 600 meters of deviation. The routines processing raw measurements that are reported from two receiver test beds, as well as PVT acquisition algorithms, namely, WLS, EKF and our algorithm, are all written in MATLAB. The MATLAB-friendly convex optimization modeling software, cvx, is used to solve the quadratic program in the novel algorithm, and is employed in the effort to estimate the correct PVT solution and the spoofing attack.

### Numerical Results

This section reports and examines the output of synthetic attack simulations. Both the SDR and the Huawei commercial receiver accumulate the TEXBAT clean static data, and we added the tailored spoofing scenarios onto the processed pseudorange pair. Multiple figures depict the outstanding performance of our algorithm, numerically compared by using Root-Mean-Square-Error (RMSE) values against the estimation produced by EKF. The following

equation defines the RMSE for the z-coordinate:

$$RMSE = \sqrt{\frac{1}{K} \sum_{k=1}^K (\hat{x}_{estimated,i}[k] - \hat{x}_{ground\ truth,i}[k])^2} \quad (9)$$

### Scenario 1: TSA

Figure 3 shows the result of sole TSA spoofing on the SDR receiver. A total of 600 meter magnitude deviation is applied to the clock bias; the drift changes accordingly. The third order spoofing profile has the smoothest shape that can have numerous sparse spikes on the jerk domain. Based on the consistency characteristic of TSA, the deviating shape and magnitude applied on clock bias are exactly identical to modifying signals on pseudoranges. Though the spoofing setting is identical to the experience executed in the work of [15], the algorithm based on the minimization of (7) differs from the approach shown in aforementioned paper.

The primary task of third component in (7) is to filter the estimated attack from the correct PVT solution,  $\mathbf{x}_k$ . We select  $\lambda_p = 10$ . The optimization problem acknowledges the abnormal behavior on the bias domain, also by expecting subtle sparse peaks on jerk. Figure 3a shows the clean (WLS output), attacked (EKF output) and corrected (optimization output) of z position, velocity, clock bias and drift estimations. As Figure 3a suggests, the corrected solutions all maintained to be less than absolute 20 meters. Further, the RMSE error on z coordinate is reduced from 389.22

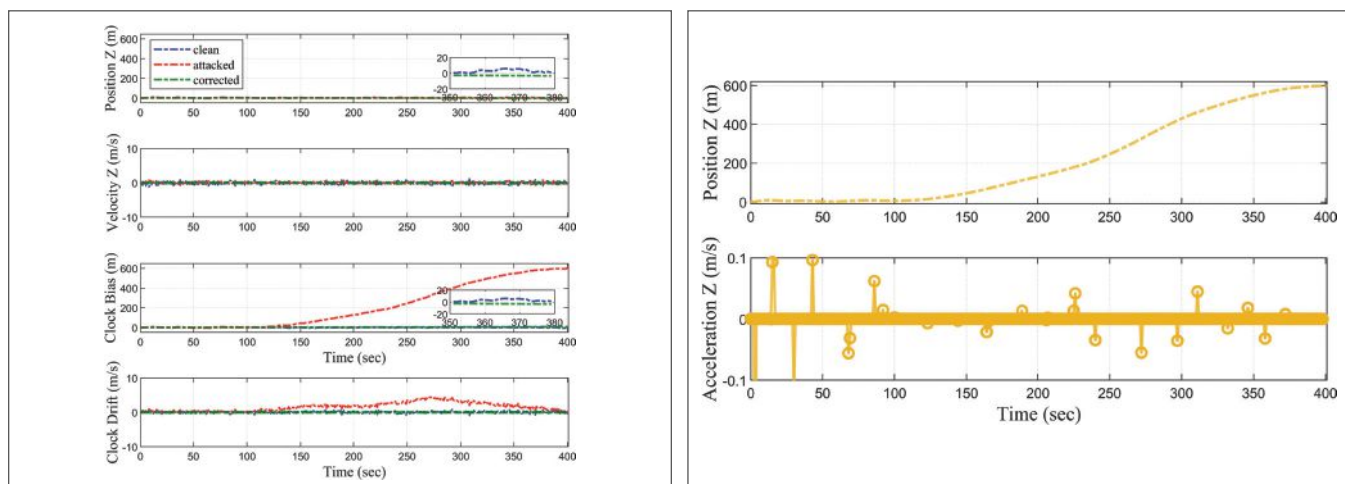
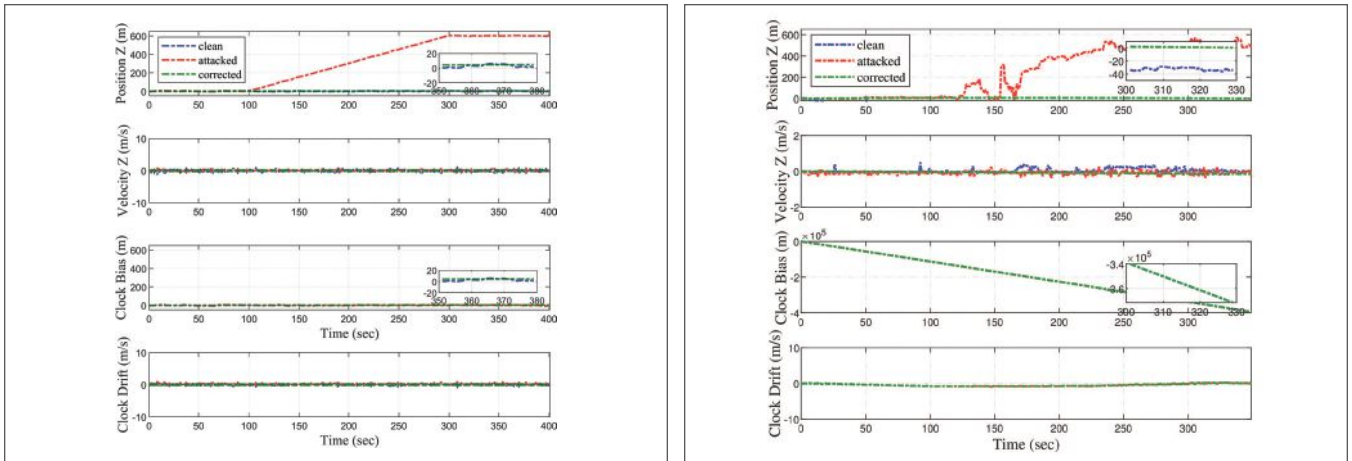


FIGURE 3 Response of Consistent TSA third order attack applied on CS data. Figure 3a (left) indicates estimated state on position and velocity z as well as lock bias and drift. Figure 3b (right) depicts estimated attack on clock bias and its third derivative.



**FIGURE 4** These figures depict the result of the optimization under z-domain non-consistent spatial spoofing. The synthetic attack is applied on the TEXBAT CS scenario, after it is replayed over the SDR [left] or the Huawei receiver [right]. Due to the evident second order attack in Figure 4a, sparsity in jerk domain is guaranteed and captured by the optimization problem.

meters to 2.25 meters. **Figure 3b** depicts the estimated attack, which turns out to be similar to the applied attack.

**Scenario 2: Spatial Spoofing**

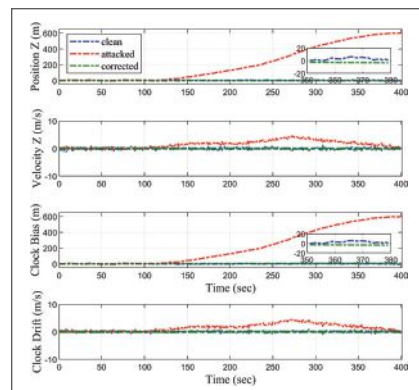
The second scenario explores the second order spatial spoofing where only the position estimate is affected by the pseudorange deviation. The deviating magnitude gradually increases from 100 to 300 seconds with ultimate amplitude of 600 meters. The second order spoofing profile expects to show peaks in acceleration and jerk domains. The major improvement made with respect to our previous approach [15] is attaining robustness against spatial spoofing. Due to measurement linearization, our algorithm has the capability to search more than clock domain.

The plots in **Figure 3** express the result of sole spatial spoofing in z-domain, namely the result of the optimization after applying the synthetic attack to the replayed CS scenario over the SDR and the Huawei receiver. Even though the Huawei recordings in **Figure 4b** have more noise than the SDR recordings shown in **Figure 4a**, both cases successfully captured and mitigated the attack using a tuning parameter of  $\lambda_z=10$ . Further, the RMSE value for the z domain in the SDR case reduced from 389.22 meters to 6.03 meters; and the corresponding one for the Huawei receiver decreased from 357.37 meters to 32.77 meters. Other variables produced by the optimization such as z-velocity,

clock bias, and drift, are estimated very closely to the ground truth.

**Scenario 3: Joint Attack**

The third spoofing scenario for a stationary receiver is the joint TSA and spatial attack. Because TSA is supposed to be a consistent attack, we simulate an overall consistent joint attack with 600 meters maximum magnitude and third-order profile. The joint spoofing was only able to be rejected upon tuning of the penalization terms. **Figure 5** indicates the algorithm successfully mitigates the attack on any domains of search. The RMSE value also has been reduced similarly to **Scenarios 1 and 2**. This manifests that the developed algorithm can deny any type of spoofing attack whether it targets singular or multiple domains.



**FIGURES** The result of third order consistent joint attack against z-domain and clock timings.

**Conclusion and Summary**

This article develops a technique to mitigate joint spoofing against time and a single position coordinate in stationary GPS receivers. To this end, a suitable linearization of the GPS measurement equation is presented and sparsity characteristics of attacks are reviewed. The technique relies on minimization of a multi-criterion objective that includes penalization giving rise to sparse solutions. Three synthetic spoofing scenarios are successfully mitigated. The resulting RMSE values in each scenario are reduced significantly versus the EKF estimations, meanwhile the absolute error is small as well. Our current work [17] focuses on expanding the model to receivers with slow dynamics, successful mitigation of joint attacks an all PVT domains analyzing the effects of different attack orders and degrees of consistency, and validation with authentic spoofed signals from the TEXBAT database, as opposed to synthetic attacks only.

**Acknowledgements**

This article is based on material presented in a technical paper at ION GNSS+ 2021, available at [ion.org/publications/order-publications.cfm](http://ion.org/publications/order-publications.cfm).

This material is based upon work supported by the National Science Foundation under Grant No. 171904.

**References**

References available online.



## Authors



**Junhwan Lee** received his B.S. degree in electrical engineering from the University of Texas at San Antonio (UTSA) in 2017. He is currently a Ph.D. candidate in the Department of Electrical and Computer Engineering at UTSA. His research interests include GNSS interference mitigation technique, state estimation in optimization and control theory.



**Erick Schmidt** received his B.S. degree in electrical engineering from Monterrey Institute of Technology and Higher Education, Monterrey, Mexico, in 2011 and both his M.S. and Ph.D. degrees in electrical engineering from The University of Texas at San Antonio (UTSA) in 2015 and 2020 respectively. His research interests include base-band processing in software-defined radio platforms for fast prototyping, WLAN indoor localization systems, and interference mitigation techniques for GNSS. He is a graduate student member of IEEE and ION.



**Nikolaos Gatsis** received a Diploma degree (Hons.) in electrical and computer engineering from the University of Patras, Patras, Greece, in 2005 and a M.Sc. degree in electrical engineering in 2010 and a Ph.D. in electrical engineering with a minor in mathematics in 2012 from the University of Minnesota. He is currently an Associate Professor with the Department of Electrical and Computer Engineering at the University of Texas at San Antonio. He was a Lucher Brown Professorship Endowed Fellow for the academic year 2020–2021. His research focuses on optimal and secure operation of smart power grids and other critical infrastructures, including water distribution networks and the Global Positioning System. Dr. Gatsis is a recipient of the NSF CAREER award and the UTSA President's Award for Research Achievement.



**David Akopian** is a Professor at the University of Texas at San Antonio (UTSA) and Associate Dean of Research for the College of Engineering. Before joining UTSA, he was a Senior Research Engineer and Specialist with Nokia Corporation from 1999 to 2003. From 1993 to 1999, he was a researcher, instructor and assistant director of a center at the Tampere University of Technology, Finland, where he received his Ph.D. degree in 1997. Dr. Akopian's current research interests include algorithms for communication and navigation receivers, including fast acquisition and massive correlators, spoofing mitigation on different levels of processing chain, and the general area of mobile applications. Also, he contributed positioning algorithms for Assisted-GPS and Labview platform concepts for software-defined radio GPS receivers. Recent efforts include automated human-machine interfaces. He has authored and co-authored more than 35 patents and 170 publications. He has been a Fellow of the National Academy of Inventors since 2016. His research has been supported by the National Science Foundation, National Institutes of Health, USAF, the U.S. Navy, and Texas foundations.

NavtechGPS brings you ...

# VectorNav Inertial

Available now!

Powerful, dual GNSS aided INS in a small, embedded unit

VectorNav VN-310E



High performance in a reliable, ruggedized enclosure

VectorNav VN-310



IMU/AHRS only, for highly SWaP-C constrained applications

VectorNav VN-110E



NavtechGPS sells hundreds of GNSS products, including receivers, antennas, inertial systems, GPS jammer detectors, and more!  
Contact us today.

NavtechGPS®

+1-703-256-8900 • 800-628-0885  
www.NavtechGPS.com

Your ONE source for GNSS products and solutions

# Kodiak Robotics relies on lightweight mapping for autonomous truck PNT



Kodiak Robotics' fourth-generation autonomous truck.

All photos courtesy of Kodiak Robotics.

*Inside GNSS* recently spoke with CEO Don Burnette in an exclusive interview about the company's fourth-generation platform, an autonomous truck that's taking a different approach to PNT.

KEVIN JOST

## "We do it differently.

We have a very sparse mapping solution that only includes the road network—the lane connectivity information."

Don Burnette, CEO, Kodiak Robotics

**K**odiak Robotics, Inc. has been on a bit of a roll lately, developing automated solutions for long-haul truck routes in the southern parts of the U.S.

The self-driving trucking company made a big announcement on that front in August, unveiling a partnership with Pilot Company, the largest travel center operator in North America, to develop autonomous truck services at Pilot and Flying J travel centers.

The companies are creating an autonomous truck port in the Atlanta area to evaluate potential service offerings and explore scalable solutions. The possibilities include spaces to pick up and drop off autonomous trucking loads; conducting inspections; maintaining and refueling

trucks; and the ability to transfer data for feature development and mapping.

The partnership is significant for both Kodiak and the industry. It establishes players like Pilot and its travel centers as premier locations to facilitate the various services autonomous trucks will need when they're in production and deployed commercially, Kodiak CEO Don Burnette said. In addition, the Pilot centers will be access points for transferring data.

The Pilot partnership is just the latest development in Kodiak's accelerating growth phase in 2022, with significant expansion coming in its service footprint and partner network as well.

In July, the company announced a partnership with 10 Roads Express, a provider of time sensitive surface transportation for the U.S. Postal Service, expanding the company's service to Florida. And earlier this year, Kodiak announced a new route between Dallas and Oklahoma City with CEVA Logistics and a route between Dallas and Atlanta with U.S. Xpress.

## A Fourth-Generation Autonomous Truck

This commercial success is being driven in part by the leading-edge technology in Kodiak's fourth-generation autonomous truck. The new generation is designed for improved autonomous system robustness, with greater fleet uptime, manufacturing and serviceability in mind—all of which are critical to scaling the technology quickly, safely and efficiently, according to the company.

"Complex and bulky systems that require an engineer to hand-build and hand-tune are expensive, unreliable and difficult to debug," said Burnette, who co-founded the Mountain View, CA-based Kodiak Robotics with COO Paz Eshel. "We believe that reliability and scalability flow from simplicity, and the best hardware modifications should be barely visible. Our fourth-generation

# GNSS Expertise providing Resilient PNT Solutions



Flash this code & learn more about Resilient PNT Solutions



**Tests & Measurements**



**GNSS Receivers**



**GPS/GNSS Coverage Extension**

For more information:

Visit our website:  
[syntony-gnss.com](http://syntony-gnss.com)

Contact us:  
[contact@syntony-gnss.com](mailto:contact@syntony-gnss.com)

Follow us:





Kodiak Robotics was co-founded by (l-to-r) CEO Don Burnette and COO Paz Eshel.

platform is designed for simple, scaled production, which means easy calibration, troubleshooting and maintenance for our partners.”

The truck features a modular and more discreet sensor suite in three locations—a slim-profile “center pod” on the front roof above the windshield and pods integrated into both sideview mirrors. This better-integrated sensor placement is said to vastly simplify sensor installation and maintenance while also increasing safety.

The autonomous driving system features Luminar’s Iris LiDAR, Hesai’s 360-degree scanning LiDARs for side and rear-view detection, ZF’s Full Range Radar, and the Nvidia Drive platform for the AI brains.

The Kodiak Vision perception system considers every sensor—including LiDAR, camera and radar—as primary, according to the company. All three sensors are purpose-built to meet the needs of autonomous trucks, which must “see” long-range in a variety of weather conditions to safely operate at highway speeds.

The system fuses information from the sensors and considers the relative strengths and weaknesses of each type. It incorporates extra redundancies and cross-validates data, adding another layer of safety to the self-driving system.

The patent-pending mirror pods—which will start with one Hesai LiDAR, two long-range 4D radars and three cameras—don’t require specialized sensor calibration. Rather than replacing a sensor in need of maintenance, a mechanic can

replace the mirror pod in minutes. This single point of integration will allow for maintenance and serviceability at scale.

To make sense of all the data, the trucks will feature Nvidia Drive Orin,

**“Our positioning is**

very high fidelity in a lateral sense, but it’s not as high fidelity in a longitudinal sense. It just doesn’t matter if we’re one foot farther or one foot back on the road. As long as we’re close enough to be within the vicinity, we can identify key markers to tell us where we need to take our exits and where to expect other vehicles to be.”

Don Burnette, CEO, Kodiak Robotics

once available, as the supercomputing platform. With more than 250 TOPS (trillion operations per second) of compute performance, the platform is architected for safety and addresses systematic safety standards such as ISO 26262 ASIL-D (Automotive Safety Integrity Level-D). In the interim, Kodiak will use the current-generation Nvidia Drive AGX Pegasus to process data from cameras.

**The Importance of PNT**

When it comes to positioning, navigation and timing (PNT), Burnette said it “is definitely an area where we feel like Kodiak is really innovating within the space.”

Within a mapping and localization framework, he said “ultimately the robot needs to answer the question, ‘Where am I?’ And once it knows where it is, then it needs to ask the question, ‘How do I drive from here?’ And then you just repeat those questions.”

Historically, most companies have implemented high-definition (HD) maps of the environment using vehicle sensors to identify fine details like road texture surfaces, paint markings, tree trunks, buildings, sides of buildings, etc, Burnette said.

“You name it, they put it in the map, and then they use that map to position themselves very finely in the real world,” he said. “And then they use an IMU [inertial measurement unit] to interpolate between those position-based preferences.”

His company diverges from the industry in this respect.

“We do it differently,” he said. “We have a very sparse mapping solution that only includes the road network—the lane connectivity information.”

For instance, the Kodiak system and lightweight Sparse map keep track of the number of lanes and their relation to each other and know where the exits and cloverleafs are.

“From there, we localize based on what our sensors see relative to the lane markings that are relevant for driving, much the same way [that] humans do,” he said.

Kodiak engineers use an IMU to interpolate truck location as it moves down the road.

“Our positioning is very high fidelity in a lateral sense, but it’s not as high fidelity in a longitudinal sense,” Burnette said. “It just doesn’t matter if we’re one foot farther or one foot back on the road. As long as we’re close enough to be within the vicinity, we can identify key markers to tell us where we need to take our exits and where to expect other vehicles to be.”

That’s where GPS comes in.

“We have a very loose reliance on GPS just to bootstrap the system when

we're just getting started to kind of tell us where we are initially," he said, "but also then to pull us gradually along longitudinally to maintain that semi accuracy."

### Reliability is King

While performance and cost are important considerations for IMUs and GPS units—as well as the perception sensors—for autonomy, the key metric Kodiak developers are interested in is reliability.

"I think this is a bit of a surprise for most people, and it applies to all the sensors," Burnette said. "At this stage, we're not looking for improved performance. I think we have the performance we need from our sensors, compute and hardware that would be acceptable to launch


this product safely. Cost is somewhat important, but what we really care about is reliability."

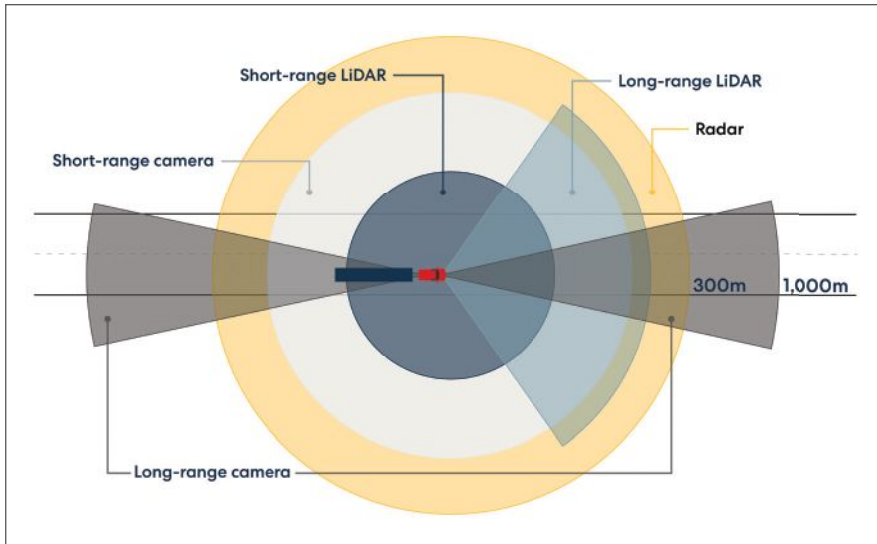
The company has not announced the sources for its IMU and GPS unit, but wants suppliers capable of building solutions that can withstand the harsh environment trucks face day in and day out without breaking.

"If you can build a unit that will go hundreds of thousands of miles on the highway without breaking, that's what we care about," he said. "We care about reliability much more than any kind of fancy gizmo."

The ability to withstand the typical shock/vibration is a top consideration, especially for IMUs, along with water ingress and temperature swings.

"We drive in the heat of a Texas summer where it can get extremely hot, and it also must be able to work in the bitter cold," he said. "So, temperature, shock and vibrate, water, ingress, reliability—just general wear and tear—those are the types of things that we evaluate."

Those evaluations continue as the company aims to integrate its self-driving software and hardware, the Kodiak Driver, into production customer trucks in early 2025. Kodiak Driver will operate self-driving fleets for a low per-mile subscription fee. 



Kodiak Driver sensors and their ranges.



Kodiak Vision raw sensor data.



Kodiak focuses on easy SensorPod maintenance.



# Mitigating the threat of jamming and spoofing to aeronautics

A look at a multiscale interference monitoring approach using several different detectors, as well as an overview of findings of an interference monitoring campaign conducted at a European airport.

**SASCHA BARTL, MANUEL KADLETZ**  
OH B DIGITAL SOLUTIONS GMBH

**PHILIPP BERGLEZ**  
GRAZ UNIVERSITY OF TECHNOLOGY

**TOMÁŠ DUŠA**  
GNSS CENTRE OF EXCELLENCE

**G**lobal navigation satellite systems (GNSS) have become increasingly important in many different fields of application, including the aeronautical domain. With the growing dependency on GNSS for various safety-critical applications, both the threat of intentional signal disturbances and the number of reported incidents of jamming are increasing. Even spoofing attacks, which were long thought of as a theoretical threat requiring high effort and knowledge, can today be conducted using relatively cheap software-defined radios (SDRs) and open-source software.

Aeronautics depends on GNSS in several ways, including in-flight navigation, ground-based augmentation systems (GBAS) and surveillance. Recent publications have shown vulnerabilities of GNSS systems against jamming and spoofing and demonstrated that receiver autonomous integrity monitoring (RAIM),

which is widely used in aviation, provides limited defense against intentional interference [1,2]. Therefore, there's a need for the development, evaluation and use of dedicated interference monitoring algorithms, targeting jamming and spoofing, that are applicable to the most vulnerable phases of flight (i.e. approach and landing).

While on-board interference detection and mitigation is considered important for the long-term evolution of GNSS in aviation, both commercial and general, the approach presented here uses a ground-based monitoring station to detect interference and issue a warning to the users. When deployed in the vicinity of an airport, such a system can secure GNSS during approach and landing, which is critical. The ground-based design can be mounted at a fixed location, can be more power consuming and is less restricted by long-term certification requirements for aviation equipment.

## Background

GNSS signals are susceptible to intentional interference without requiring

very high signal power or overly complex equipment. This has been widely reported in literature, gaining public interest in 2001 with the Volpe report [3], which assessed the dependencies of the transportation infrastructure on GPS and the vulnerabilities to signal interference. The two main factors contributing to the vulnerability of GNSS signals against interference are the low received signal power (below thermal noise) and the open and publicly known signal structure. Although modernized signals counter the vulnerabilities by employing more sophisticated modulation schemes like higher-order binary offset carrier (BOC) or authentication features, these countermeasures cannot provide perfect interference mitigation. Many systems also still rely on older signals.

### Signal Model

To counter the threat of intentional interference, it is important to understand GNSS signal structure. Therefore, a basic signal model used throughout the development of the detection algorithms is presented here. The equations are derived from [4].

According to [4], a radio frequency (RF) signal  $x_{RF}(t)$  can be written

$$x_{RF}(t) = \sqrt{2}x_I(t) \cos(2\pi f_c t) - \sqrt{2}x_Q(t) \sin(2\pi f_c t), \quad (1)$$

as a function of time  $t$  at a certain carrier frequency  $f_c$ , with the in-phase I and quadrature-phase Q components  $x_I(t)$  and  $x_Q(t)$ . These two components are orthogonal to each other and share the same power normalization factor of  $\sqrt{2}$ . The  $90^\circ$  phase delay of the quadrature component leads to the signals being right-handed circularly polarized (RHCP).

GNSS uses both the I and Q components of the baseband signal to transmit more than one navigational signal on the same carrier wave, which is generally known as quadrature phase shift keying (QPSK). In this modulation scheme, each component is spread across a certain bandwidth by using binary phase shift keying (BPSK) or BOC modulation. For actual transmission of information to the receiver, a navigation message  $D(t) \in [1, 1]$  (at signal level) is introduced in addition,

leading to a single signal component  $y(t)$  reading

$$y(t) = A(t)D(t)C(t) = \sqrt{P(t)}D(t)C(t), \quad (2)$$

where  $P(t)$  denotes the power of the signal component,  $A(t)$  is the amplitude and  $C(t)$  is the binary spreading sequence or pseudorandom noise (PRN) code. Inserting (2) into (1) yields

$$s(t) = \sqrt{2P_I(t)}D_I(t)C_I(t) \cos(2\pi f_c t) + \sqrt{2P_Q(t)}D_Q(t)C_Q(t) \sin(2\pi f_c t) \quad (3)$$

as generic model of a typical GNSS signal as transmitted by a satellite. The received signal of a single satellite on Earth can be expressed as

$$r_{RF}(t) = A_I(t)D_I(t)C_I(t) \cos\{2\pi[f_c + f_D(t)]t + \phi_0\} + A_Q(t)D_Q(t)C_Q(t) \sin\{2\pi[f_c + f_D(t)]t + \phi_0\}, \quad (4)$$

where  $\tau(t)$  denotes the code delay,  $\phi_0$  is the phase delay and  $f_D(t)$  denotes the Doppler frequency shift due to the relative motion between satellite and receiver. The overall signal received contains the signals of all satellites in view as well as thermal noise and can thus be expressed (using the trigonometric identity as shown in [4]) as

$$r(t) = \sum_{i=1}^N a_i(t) e^{j\phi_{0,i}} s_i[t - \tau_i(t)] + n(t), \quad (5)$$

with  $s_i$  being the signal from satellite  $i$  attenuated by  $a_i(t)$ ,  $N$  denoting the number of satellites in view and  $n(t)$  being additive white Gaussian noise (AWGN).

### Intentional Interference

GNSS interference can be unintentional (e.g., inter-system interference, multipath, etc.) or intentional. Unintentional interference generally can be better controlled and mitigated [5–7] and is not the primary focus of this work. Intentional interference is categorized into the two main categories, jamming and spoofing, which pose a significant risk to GNSS measurements. Jamming denotes the transmission of high-powered signals with the goal to shadow the GNSS signals so a receiver cannot acquire and track them. Typical jamming signals are chirp or noise signals with a bandwidth matching or exceeding the bandwidth of the respective GNSS bands they target.

A good overview of available civil jamming devices and their signal characteristics is presented in [8]. The signal model presented in (5) in case of jamming is extended as

$$r_{\text{jammed}}(t) = \sum_{i=1}^N a_i(t) e^{j\phi_{0,i}} s_i[t - \tau_i(t)] + s_j(t) + n(t), \quad (6)$$

with  $s_j(t)$  denoting the jamming signal. As mentioned, the actual waveform of this jamming signal is not primarily important. Any interference signal leads to a decrease in carrier-to-noise ratio ( $C/N_0$ ) of the received satellite signals, which, if the decrease is high enough, leads to the inability of acquisition and tracking.

Spoofing denotes the transmission of fake GNSS signals with the goal to falsify (spoo) the position, velocity and time (PVT) solution of the receiver under attack. For this, spoofing signals have to be modulated in the same way authentic satellites are modulated. The navigation messages also usually have to be mimicked for a spoofing attack to work well. Typical spoofing attacks rely on either a GNSS signal generator or a modified (usually software-defined) GNSS receiver [9]. The signal model in case of spoofing is extended to

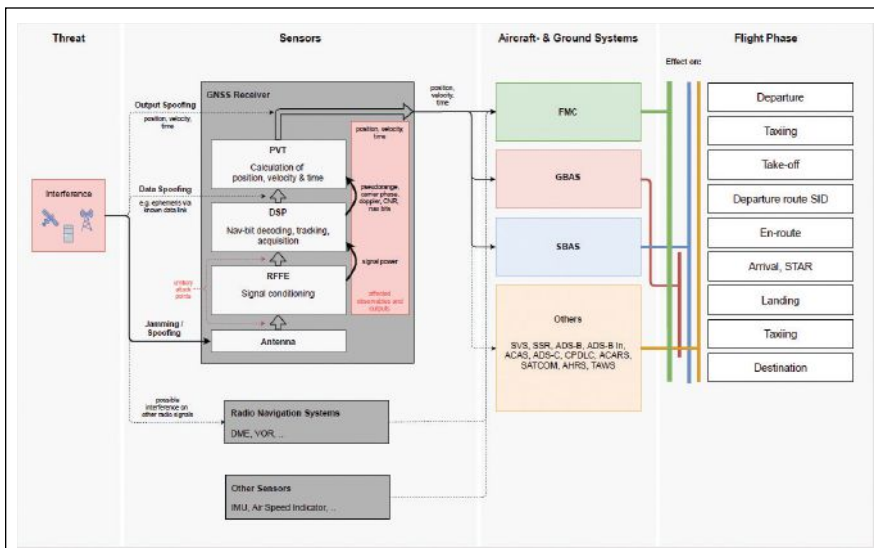
$$r_{\text{spoofed}}(t) = \sum_{i=1}^N a_i(t) e^{j\phi_{0,i}} s_i[t - \tau_i(t)] + \sum_{i=1}^{N^S} a_i^S(t) e^{j\phi_{0,i}^S} s_i^S[t - \tau_i^S(t)] + n(t), \quad (7)$$

where the superscript  $S$  denotes a spoofing signal. The spoofing signals' code delay  $\tau_i^S(t)$  as received not only depends on the actual and spoofed position but also on the spoofer's synchronization error. This contains the error in time synchronization relative to the GNSS time as well as the error in the estimation of the victim receivers' position, which is crucial for successful spoofing attacks.

### GNSS Interference in Aeronautics

Interference has multiple potential impacts on aircraft systems. The most common impact is the complete loss of GNSS reception, which results in loss of position, navigation and time (PNT). However, given the variety of systems operating, the impacts will not be homogenous across all fleets and equipment. In some cases, the GNSS signal could be degraded but not completely lost, resulting in decreased position accuracy.

The aircraft receiver is the main source of position information, which drives the aircraft navigation system supporting required navigation performance (RNP) operations and providing position input to different aircraft systems. Some business aircraft even use GNSS as a reference source for aircraft flight control and stability systems



**FIGURE 1** GNSS interference impact overview.

[10]. GNSS interference, either intentional or unintentional, introduces a threat to the navigation equipment via different vectors.

A wide variety of aircraft and ground systems rely on proper GNSS service and thus have to be assessed in terms of the effects of a malfunctioning service affecting different flight phases. **Figure 1** gives a holistic overview of the impacts of a jamming/spoofing attack.

**Development of a Multiscale Interference Monitoring Algorithm**

The effect of interference on a GNSS receiver can be recognized within various stages of the signal processing as indicated in **Figure 1**. Therefore, it is considered vital for reliable interference monitoring to also target all of these stages by combining different detectors within a multiscale approach. This ensures high reliability in terms of high detection probability and low false-alarm rates. During the development, special attention was also paid to the regulatory framework within aviation.

**The Regulatory Framework**

The FAA’s technical standard orders (TSOs) are used as a basis for qualifying aviation equipment. They are typically short documents that mostly rely on minimum operational performance standards (MOPS) as provided by the radio technical commission for aeronautics (RTCA), but in some cases deviate from those RTCA standards by adding, removing or changing the requirements.

A TSO-authorized part qualifies as an airworthy component. As such, a TSO is a minimum performance standard. When authorized to manufacture a receiver to a TSO standard, this is referred to as a TSO authorization. Current GNSS receivers are approved against one of the following TSOs:

- TSO-C129 (GPS as a supplemental means, last version found in RTCA DO208 [11])
- TSO-C145 (GPS+SBAS sensor feeding an FMS, last version found in RTCA DO229F [12])
- TSO-C146 (standalone GPS+SBAS, last version found in RTCA DO229F [12])
- TSO-C196 (GPS sensor feeding into an FMS, replacement of TSO-C129, last version found in RTCA DO316 [13])
- TSO-C161 (GPS+GBAS, last version found in RTCA DO253C [14])

**Jamming Detection**

Detecting GNSS jamming has been widely covered in literature [15–18]. In general, jamming detection can be performed pre-correlation or post-correlation, while the most suitable approach depends on the type and possibilities of the receiver in use. Because different detectors have different advantages and disadvantages, as pointed out, [15], an optimal jamming detector should be based on the combination of several detector values.

The approach presented in this article relies on monitoring the power spectral

density (PSD), total received power within the band and  $C/N_0$  of the tracked satellites. The combination of pre-correlation and post-correlation measures is considered advantageous for a low false-alarm rate, which is important for aviation. Furthermore, the chosen detectors are considered to be certifiable for aeronautics with a reasonable effort.

**The Jamming Detectors: PSD Detector**

The PSD detector is based on the recorded raw intermediate frequency (IF) signal without further preprocessing within the receiver. Transformation into the frequency domain is performed using Fourier transform as in

$$\hat{s}(f) = \mathcal{F}\{s(t)\} = \int_{-\infty}^{\infty} s(t) \cdot e^{-j2\pi ft} dt, \tag{8}$$

while the PSD can generally be computed as

$$PSD(f) = \frac{1}{f_s N} |\hat{s}(f)|^2, \tag{9}$$

with  $f_s$  denoting sampling frequency and a sample size  $N$ . In the presented approach, the PSD is computed using Welch’s method [19], which is considered optimal because of the smoothing effect. To accurately receive absolute power levels in the PSD, the actual gain of the RF components has to be known/calibrated. For jamming detection, the received PSD can be compared to the expected shape, which is mainly determined by the filter in the radio-frequency front-end (RFFE). The expected power spectrum can easily be estimated as thermal noise combined with the aforementioned filter, because the authentic GNSS signals are actually received below the noise floor.

For the detector presented here, two sets of thresholds above the expected spectrum are defined as follows:

**NARROWBAND THRESHOLD:** Single peaks within the received PSD are compared to a defined frequency-dependent threshold mask, which can be tailored to the respective filter characteristics or to exclude known tolerated interference signals based on their frequency. The narrowband threshold is considered optimal for detection of narrowband or continuous wave (CW) interference.



**WIDEBAND THRESHOLD:** The received PSD is averaged over defined frequency bins to form multiple sub-band power levels, which in turn are compared to a dedicated frequency-dependent threshold mask. The wideband threshold is considered optimal for detecting wideband interference. The wideband threshold can be set much lower compared to the narrowband without compromising on false alarm rate because the averaging provides an additional level of smoothing.

For use in aeronautics, these thresholds might be set to the values defined by ICAO as shown in **Figure 2**.

### Received Power Detector

The received power detector measures the absolute received signal power within the monitored frequency band. This is done by computing the power within the digitized signal  $s[n]$  and subtracting the actual RF gain  $\alpha(t)$  as

$$P(t) = 10 \log_{10} \left( \frac{1}{N} \sum_{k=tf_s}^{tf_s+N} s[k]^2 \right) - \alpha(t) \quad (10)$$

with  $N$  being the number of samples for averaging. Because the GNSS frequency bands are protected, the expected total received power within the band can simply be assumed the thermal noise floor given as

$$P_{\text{noise}} = k_B T_0 B \quad (11)$$

with the Boltzmann constant  $k_B$ , temperature  $T_0$  and bandwidth  $B$ . The detector is a simple threshold comparison, which indicates jamming in case the measured power exceeds the expected power plus the defined threshold.

### The C/N<sub>0</sub> Detector

The effective C/N<sub>0</sub> can be used for interference monitoring as post-correlation jamming detector by comparing the actually measured CN<sub>0</sub> with an expected value. In general, the effective C/N<sub>0</sub> can be written

$$\left( \frac{C}{N_0} \right)_{\text{eff}} = \frac{CL_S}{N_0 L_N + I_{\text{total}}} \quad (12)$$

the carrier power  $C$ , processing loss in the desired signal  $L_S$ , noise level  $N_0$ , processing loss in the noise  $L_N$  and the total level of interference  $I_{\text{total}}$ . The total interference level can be written

$$I_{\text{total}} = I_{\text{intra}} + I_{\text{inter}} + I_{\text{extern}} + I_{\text{jammer}}. \quad (13)$$

Neglecting the effect of external interference  $I_{\text{extern}}$  (which can be seen the same way as jamming signals for the sake of the detector), it can be seen the effect of inter- and intra-system interference should be considered to calculate the expected C/N<sub>0</sub>. Inter- and intra-system interference is caused by other GNSS signals (from the same or other constellations) in the same band and can be characterized

$$I_{\text{intra/inter}} = \sum_{k=1}^M C_k L_k \kappa_k, \quad (14)$$

for  $M$  signals present at the same time, where  $C_k$  denotes the signal power,  $L_k$  is the implementation loss for the interference signal and  $\kappa_k$  is the spectral separation coefficient (SSC). The SSC describes the level of interference caused by a certain signal/modulation and can be computed based on the frequency spectra of the respective signals [7].

Jamming detection based on the C/N<sub>0</sub> is performed threshold-based per satellite,

where the difference between each measured and expected C/N<sub>0</sub> is computed as

$$\delta_{C/N_0|j} = C/N_{0\text{expected}} - C/N_{0\text{measured}} \quad (15)$$

and compared to a pre-defined threshold. This is done for each tracked signal, which leads to a certain percentage of signals indicating jamming. In case this percentage exceeds a defined threshold, a jamming detection is triggered. The approach to summarize the results of all satellites allows for a reasonably low false-alarm rate because an eventual degradation of the C/N<sub>0</sub> for a subset of signals (as for example caused by multipath or partial shadowing) is also expected in cases without jamming.

### Combination and Weighting

The three jamming detectors are combined to one final jamming detection decision, which is outlined in **Figure 3**. The detectors have different weightings, which is a result of an empirical optimization performed using simulations. The final score is either that no jamming can be detected, a warning or an alarm, which can easily be visualized to a user within an operational aviation scenario.

**Figure 3** shows the PSD detector has the highest weight followed by the C/N<sub>0</sub> and the received power mainly serves as supplementary measure. At least two detectors have to be triggered to issue an alarm. A warning is either triggered by the PSD, C/N<sub>0</sub> detector or the combined detection of received power and a second detector. This makes sense because the three detectors are complementary in terms of which signal types (or bandwidths) they

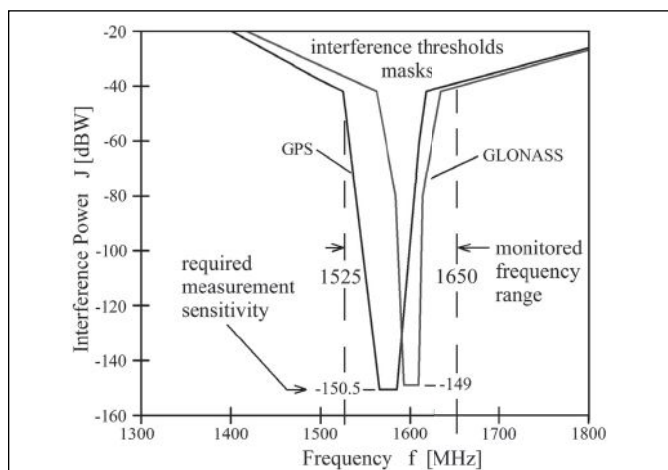


FIGURE 2 Threshold mask for interference monitoring (from [20]).

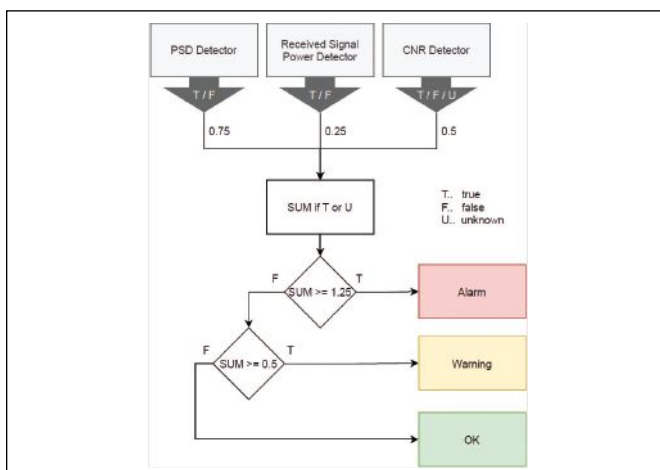


FIGURE 3 Jamming detection weighting.

can optimally detect. The inclusion (and high weighting) of the  $C/N_0$  detector also makes sense as it allows for detection of smart jamming/spectrum-matched jamming signals, which might be undetected by pre-correlation detectors.

**Spoofing Detection**

Detecting GNSS spoofing is more complex than jamming detection given the different nature of the attack, where a fine-tuned spoofing cannot necessarily be seen in the frequency spectrum. Nevertheless, several spoofing detection algorithms have been published in literature [21–24]. While some spoofing detection algorithms target multiple antennas or are only applicable with relative movement between spoofer and receiver, the approach presented here is suitable for a static single-antenna receiver, which is considered to facilitate eventual certification procedures due to the lower complexity of the overall system.

**The Spoofing Detectors:**

**$C/N_0$  Detector**

Spoofing detection based on  $C/N_0$  follows the same basic principles as in the jamming explanation. The only difference is the detection metric is inverse compared to the jamming detection as

$$\delta_{C/N_0|S} = C/N_{0\text{measured}} - C/N_{0\text{expected}} \tag{16}$$

This is because the expected  $C/N_0$  in case of a spoofing attack is higher than authentic, which is required for a successful takeover of the spoofing signal. For details on generation and prerequisites of spoofing attacks, read [25].

**Correlation Peak Detector**

From the spoofed signal model presented in (7) directly follows that the spoofing signals usually cannot remove the authentic GNSS signals from the received signal. Instead, the spoofing signals are added to the overall signal with a (slightly) higher power level. Because of this, the correlation function in case of a spoofing attack shows two correlation peaks instead of one, as is visualized in **Figure 4**.

The correlation peak detection method is twofold. It monitors for the existence of multiple correlation peaks within the complete code-Doppler search space and for distorted correlation peaks, which is the case when the authentic and spoofing signals partially overlap with each other. Multiple correlation peaks are easily found using a parallel code search FFT-based acquisition algorithm [26] while deliberately removing any already tracked correlation peaks. Monitoring for distorted correlation peaks is done using signal quality monitoring (SQM) metrics in code-delay domain as introduced in [27]. Note the detection of distorted correlation peaks is also common for multipath detection.

**Clock Detector**

The clock-based spoofing detector operates on the assumption of non-perfect synchronization of the spoofed signals with respect to their authentic counterparts. A GNSS receiver continually estimates its own clock bias relative to the system time within the PVT solution. After receiver initialization, large jumps in the estimated clock bias are typically

not expected due to the clock steering algorithm. In case of spoofing takeover, however, such a jump is expected (it is the combined effect of non-perfect time synchronization of the spoofer and non-perfect spoofer as well as victim receiver position estimation).

In an authentic case, the clock bias changes are mainly driven by the clock drift, which is a direct effect of the non-perfect frequency stability of the oscillator. Spoofing signals, however, are also generated using an oscillator as frequency standard, which might show a different clock drift. This results in a change of the observed clock drift after the start of a spoofing attack.

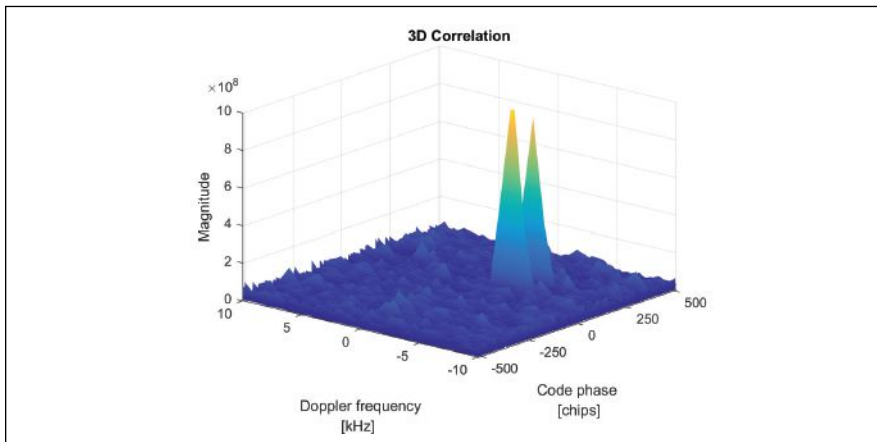
For spoofing detection, the clock bias  $\delta_r(t)$  and clock drift  $\dot{\delta}_r(t)$  at time  $t$  are both monitored by predicting the expected values for the next epoch ( $t + \Delta t$ ) as

$$\hat{\delta}_r(t + \Delta t) = \delta_r(t) + \Delta t \cdot \dot{\delta}_r(t), \hat{\dot{\delta}}_r(t + \Delta t) = \dot{\delta}_r(t) \tag{17}$$

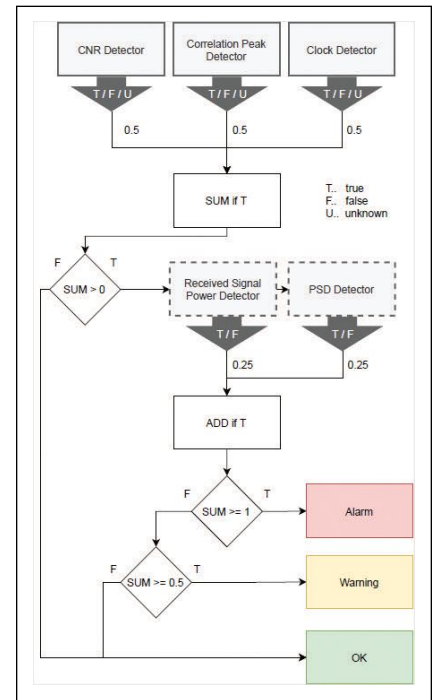
with an estimated variance model of

$$\sigma_{\hat{\delta}_r(t + \Delta t)}^2 = \sigma_{\delta_r(t)}^2 + \Delta t^2 \cdot \sigma_{\dot{\delta}_r(t)}^2 \tag{18}$$

following traditional variance propagation. For the detection, the measured bias and drift are compared with the expected values based on a standard student-t hypothesis test for the mean value, where the mean value is not a priori known.



**FIGURE 4** Two correlation peaks during spoofing attack.



**FIGURE 5** Spoofing detection weighting.

Note the clock-based detector can only show the beginning of a spoofing attack where the takeover happens. After takeover, the observed clock bias and drift will show the combined clock effect for spoofer and receiver but will again be consistent over time.

### Combination and Weighting

The combination of the three spoofing detectors is visualized in **Figure 5**. After the first stage of detection using the dedicated spoofing detectors, the jamming detectors based on PSD and received power are re-used as secondary spoofing detectors. In case these detectors show a detected jamming event, this is added to the spoofing detection score if at least one of the spoofing detectors was triggered before. Finally, the overall detection score is compared to thresholds again to distinguish between warning or alarm.

The three detectors are equally weighted for the first stage of detection because they are considered partially complementary to each other. In the case of a high-powered spoofing attack, the difference in signal level between spoofed and authentic signals is also high, which means the difference in  $C/N_0$  can be considered significant, while on the other hand the authentic correlation peaks might be drowned in the noise floor due to automatic gain control (AGC) and limited dynamic range. Vice versa, during a well-synchronized and rather low-powered spoofing attack, the effect on the  $C/N_0$  might not be significant at all, but multiple peaks or distortions of correlation are better detectable because

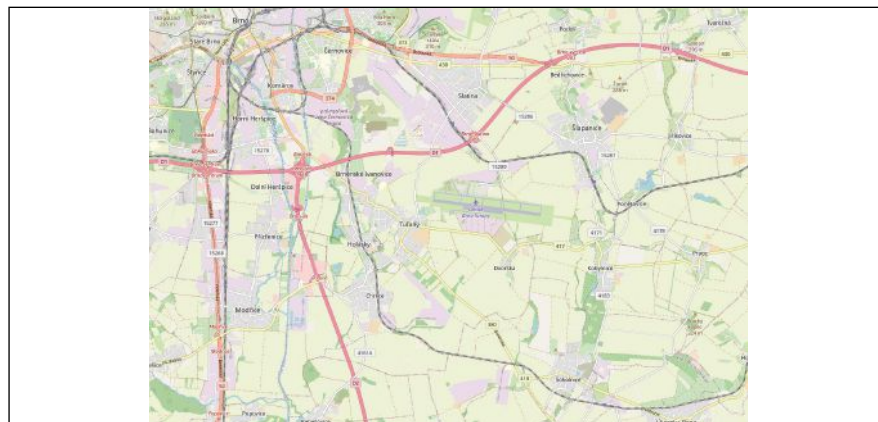


FIGURE 6 Installation location near airport Brno.

the power levels of both peaks are comparable. The clock detector can only detect the moment of takeover but works independent of the spoofing power levels (which is especially important for sophisticated spoofing attacks where artificial noise floor is transmitted together with the spoofing signals).

The secondary detection stage is used only after at least one first stage detector was triggered and can increase the detection score. This is justified by the fact spoofing signals are usually more powerful than authentic ones and thus increase the received spectrum and power level.

### Monitoring Campaign

The authors had the unique opportunity to install an interference monitoring system for a three-month permanent monitoring campaign in direct vicinity of the airport Brno in Czech Republic. Some findings from this monitoring campaign are presented here.

### Installation

The installation of the monitoring system took place in November 2020 at the location in **Figure 6**. The monitoring station is near the airport Brno (LKTBrno) and close to a major highway (D1). The minimum distance between highway and monitoring station is 480m, which is considered small enough for successful detection of most commercial off-the-shelf (COTS) jammers on the highway and is also representative for the airport.

Installation was performed at an airport building, where the antenna could be mounted on a mast and the monitoring system was connected to it via RF cable and could be placed within a 19" server rack. **Figure 7** shows the installation on-site as well as the user interface of the monitoring system, which can be accessed remotely for monitoring purposes. Furthermore, the site has a direct fiber network connection to the airport's tower building, which was used for data transfer.



FIGURE 7 Installation of monitoring station (left: antenna mounting on mast; middle: RFFE and SDR in server rack; right: monitoring system user interface).

Parameter	Value
Monitoring duration	88 days
Total detected interference events	1,277
Average # events per day	14.5
Detected jamming events	1,275 (99.8 %)
Detected spoofing events	2 (probably false alarms)
Number of warnings	856 (67.0 %)
Number of alarms	421 (33.0 %)
Average (median) duration of events	6 seconds
Shortest event duration	2 seconds (minimum reported duration in system)
Longest event duration	249 seconds

**TABLE 1** Overview of monitoring results.

## Overview of Monitoring Results

The interference monitoring campaign was conducted September 24 to December 20, 2020, resulting in 88 days of signal monitoring. **Table 1** provides an overview of the detected interference events. As indicated in the table, the average number of detected events per day was 14.5, which is in line with the authors' expectations based on literature and monitoring system placement. The two spoofing detections were classified as false alarms and could not be verified using the recorded data (the most likely reason for this is the placement of the antenna beside a mast, which might lead to significant multipath for certain satellites).

Given the placement of the monitoring system relative to the highway, it is no surprise the majority of interference events were detected for a duration of roughly 6 seconds. We can assume the detection duration and number of detected events would be higher if placed directly beside the highway because the highway is considered the major source of interference at the installation location. Also the proportion of alarms compared to warnings would have been much higher because the effect of interference signals significantly decreases with increasing distance.

## Event Examples

The following are examples of recorded interference events to show the visible effect of interference on the monitoring system.

**EVENT NO. 30:** This event is an example of a wideband interference signal spread across the complete monitored spectrum in the L1/E1 frequency band (**Figure 8**). The

interference signal is clearly visible in the recorded spectrum and above the detection threshold. It also shows a recognizable degradation of  $C/N_0$  for all satellites.

### Event Parameters:

**START TIME:** 2020-09-24 05:31:13 (UTC), duration: 8 seconds

**SEVERITY:** alarm, classified type: SCW

**EVENT NO. 4015:** This event also shows a wideband interference signal across the complete bandwidth, but with fewer spikes compared to event No. 30 (**Figure 9**). The effect of interference on the GNSS is higher based on the  $C/N_0$  and the fact

there are actual tracking (and consequently PVT) losses during the event.

### Event Parameters:

**START TIME:** 2020-10-21 19:24:20 (UTC), duration: 43 seconds

**SEVERITY:** alarm, classified type: SCW

**EVENT NO. 4031:** This event shows a very interesting narrowband/CW interference signal, located directly on the L1/E1 carrier (**Figure 10**). Based on the authors' previous analyses of COTS jammers and their respective signal properties, this interference event is not assumed to be caused by a COTS jammer. Still, the effect of the interference is clearly visible as  $C/N_0$  degradation and thus the detection is justified.

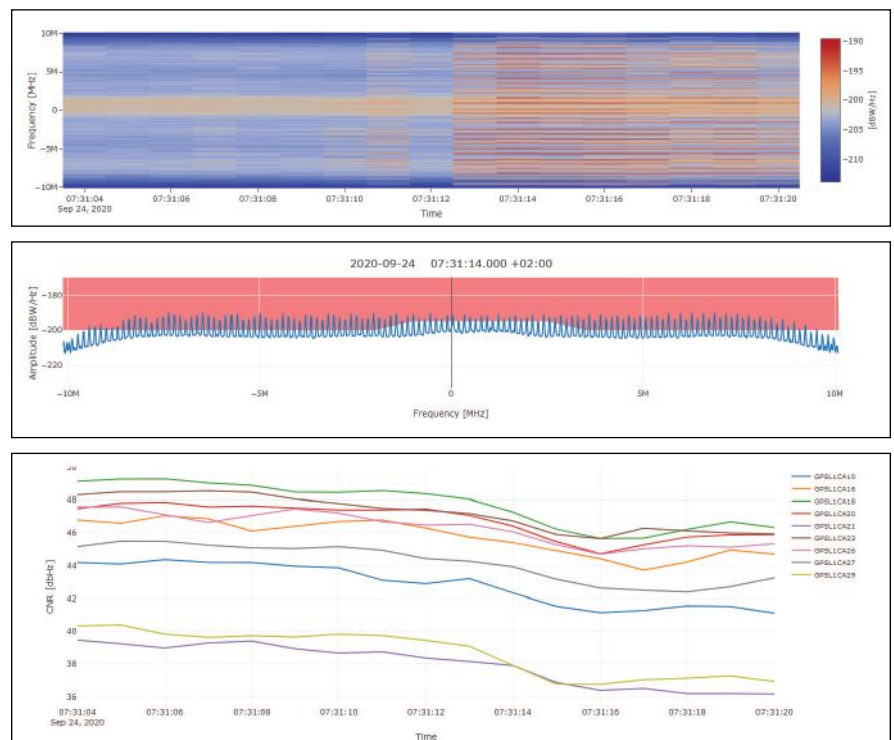
### Event Parameters:

**START TIME:** 2020-10-22 09:34:19 (UTC), duration: 59 seconds

**SEVERITY:** warning, classified type: CW/unknown

## Wide-Area Interference Event

Beside the expected local interference events, the monitoring campaign also showed an interesting series of events on December 10. They were detected not only in Brno but also simultaneously using



**FIGURE 8** Event No. 30 (top: waterfall diagram; middle: PSD at a single monitoring epoch; bottom: carrier-to-noise ratio).

a different detector (different type and manufacturer) in Prague with a matching spectrum. Thus, the interference had been spread over a significantly wider area, which leads to the assumption it might have been space-based.

### Event Parameters:

**START TIME:** 2020-12-10 07:45:06 (UTC), duration: 6 seconds (multiple times on this day)


**SEVERITY:** alarm

Figure 11 shows a short time Fourier transform (STFT) computed from the recorded signal snapshots during the event (before the start and during the event). The interference signal is rather narrowband within L1/E1. Further analysis of this specific event is considered of importance and interest, especially because there has been no notification on malfunctions by GNSS providers for this day.

### Conclusions and Outlook

This article reviewed the signal model for GNSS signals and intentional interference by means of jamming and spoofing. It presented a multiscale interference monitoring approach based on the combination of several different detectors. Findings of an interference monitoring campaign at the airport Brno also have been presented.

The number and severity of detected interference events clearly shows intentional interference by means of jamming is a major concern for aviation and other relevant applications. The authors see this as a clear indication for the necessity of permanently installed monitoring systems to secure safety critical applications relying on GNSS.

More research is needed regarding the interference event on December 10. We plan to conduct a second monitoring campaign where the monitoring system will be installed directly at a highway to see the increase of detections and severity. The developed monitoring approach will be extended toward non-stationary monitoring receivers and refined in accordance to aviation certification requirements. 

### Acknowledgment

The presented developments and monitoring campaign have been conducted in

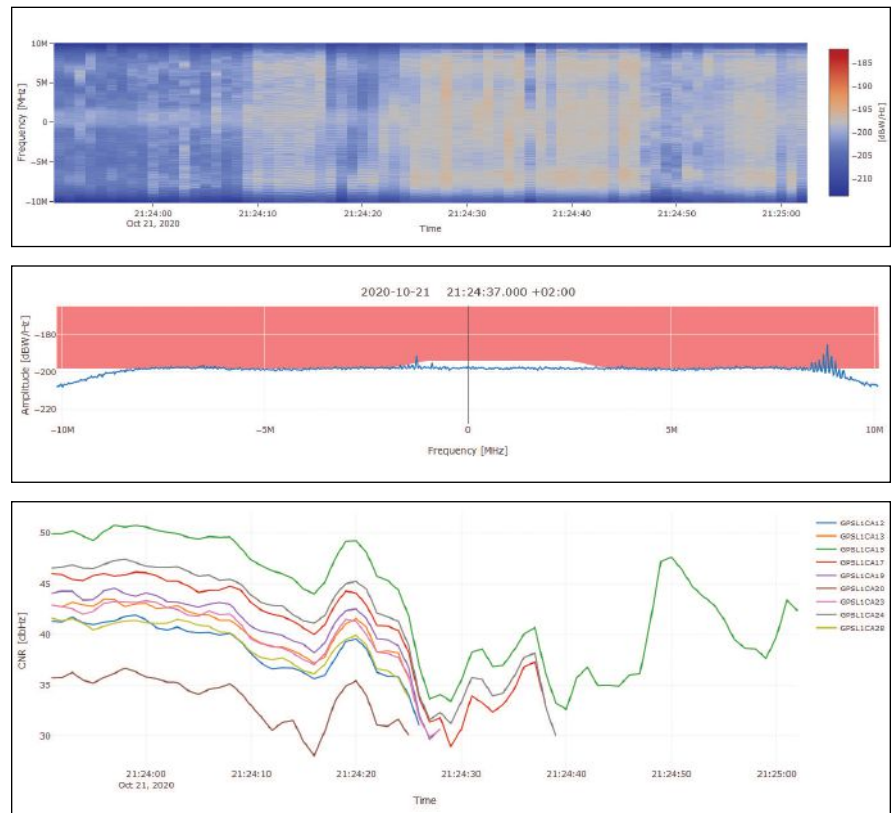


FIGURE 9 Event No. 4015 (top: waterfall diagram; middle: PSD at a single monitoring epoch; bottom: carrier-to-noise ratio).

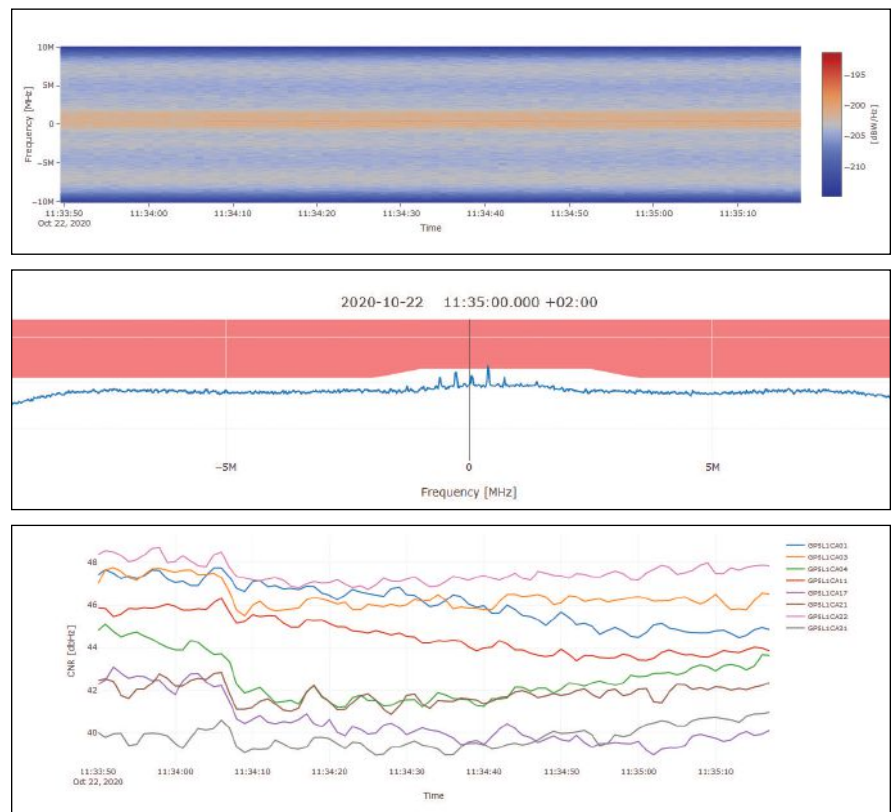
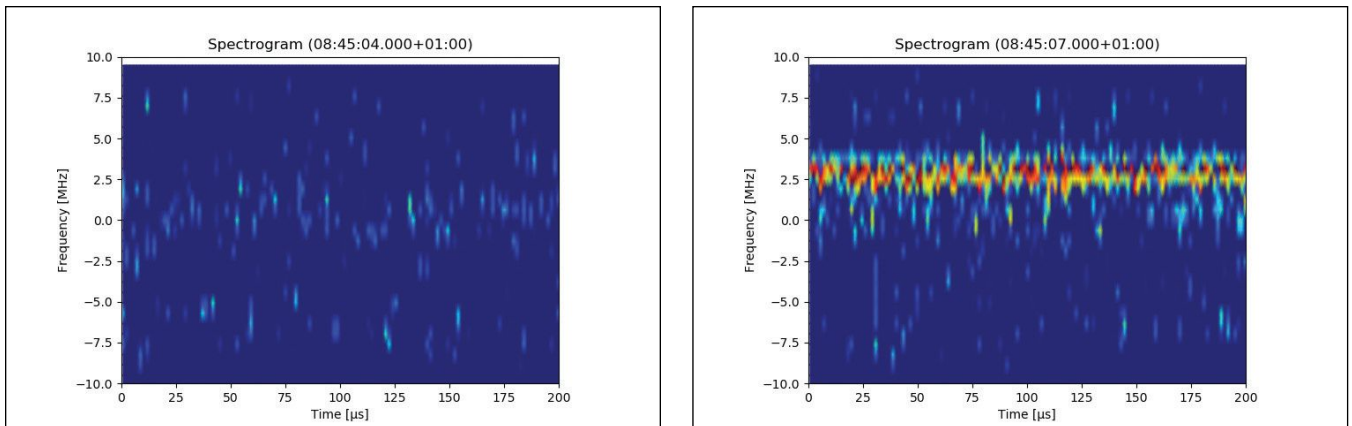


FIGURE 10 Event No. 4031 (top: waterfall diagram; middle: PSD at a single monitoring epoch; bottom: carrier-to-noise ratio).



**FIGURE 11** Short time Fourier transform of event No. 4815 (left: before start of the event; right: during the event).

the course of two research projects “GNSS Interference Detection & Analysis System (GIDAS)” and “GNSS Vulnerability and Mitigation in the Czech Republic” funded by the European Space Agency (ESA) within the NAVISP program.

This article is based on material presented in a technical paper at ION GNSS+ 2021, available at [ion.org/publications/order-publications.cfm](http://ion.org/publications/order-publications.cfm).

**REFERENCES**

(1) R. Morales-Ferre, P. Richter, E. Falletti, A. De La Fuente, and E. S. Lohan, “A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, 2020.

(2) A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS vulnerability to spoofing threats and a review of anti-spoofing techniques,” 2012.

(3) J. A. Volpe, “Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System,” U.S. Department of Transportation, p. 99, 2001.

(4) P. J. Teunissen and O. Montenbruck, Eds., *Springer Handbook of Global Navigation Satellite Systems*. Springer International Publishing, 2017.

(5) M. Wildemeersch, E. C. Pons, A. Rabbachin, and J. F. Guasch, “Impact Study of Unintentional Interference on GNSS Receivers,” Publications Office of the European Union, Tech. Rep., 2010. [Online]. Available: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/impact-study-unintentional-interference-gnss-receivers>

(6) X. Chen, F. DAVIS, S. Peng, and Y. Morton, “Comparative studies of GPS multipath mitigation methods performance,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 3, 2013.

(7) A. Kemetingler, S. Hinteregger, and P. Berglez, “GNSS Interference Analysis Tool,” *European Navigation Conference, (ENC-GNSS)*, 2013.

(8) R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O. Hanlon, J. a. Bhatti, and T. E. Humphreys, “Signal Characteristics of Civil GPS Jammers,” *Ion Gps* 2001, pp. 1907–1919, 2011.

(9) J. R. Van Der Merwe, X. Zubizarreta, I. Lukcin, A. Rügamer, and W. Felber, “Classification of Spoofing Attack Types,” *2018 European Navigation Conference, ENC 2018*, pp. 91–99, 2018.

(10) EUROCONTROL, “European GNSS Contingency/Reversion Handbook for PBN Operations, Scenarios and Options, PBN Handbook No. 6. Draft v0.3,” 2019.

(11) Radio Technical Commission for Aeronautics, “RTCA DO-208, Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS),” 1991.

(12) RTCA DO-229F, Minimum operational performance standards for global positioning system/wide area augmentation system airborne equipment,” 2020.

(13) RTCA DO-316, Minimum Operational Performance Standards (MOPS) for Global Positioning System/ Aircraft Based Augmentation System Airborne Equipment,” 2009.

(14) RTCA DO-253 Minimum Operational Performance Standards for GPS Local Area Augmentation

System Airborne Equipment,” 2017.

(15) S. Bartl, “GNSS Interference Monitoring - detection and classification of GNSS jammers,” Master Thesis, Graz University of Technology, 2014.

(16) O. Isoz, D. Akos, T. Lindgren, C.-C. Sun, and S.-S. Jan, “Assessment of GPS L1/Galileo E1 Interference Monitoring System for the Airport Environment,” in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, sep 2011, pp. 1920–1930. [Online]. Available: <http://www.ion.org/publications/abstract.cfm?jp=p{\&jarticleID=9741>

(17) S. Hinteregger and P. Berglez, “GNSS Airport Interference Monitoring System,” in *Proceedings of the International Symposium on Certification of GNSS Systems and Services (CERGA 2014)*, Dresden, Germany, 2014.

(18) D. Borio, F. DAVIS, H. Kuusniemi, and L. Lo Presti, “Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers,” *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1233–1245, 2016.

(19) P. D. Welch, “The Use of Fast Fourier Transform for the Estimation of Power Spectra: A Method Based on Time Averaging Over Short, Modified Periodograms,” *IEEE Transactions on Audio and Electroacoustics*, vol. AU-15, no. 2, 1967.

(20) F. Butsch, “A concept for gnss interference monitoring,” in *ION GPS ’99*, 1999, pp. 125–135.

(21) M. L. Psiaki and T. E. Humphreys, “GNSS Spoofing and Detection,” *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

(22) T. E. Humphreys, "Detection strategy for cryptographic gnss anti-spoofing," IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 2, pp. 1073–1090, 2013.

(23) A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in IEEE PLANS, Position Location and Navigation Symposium, Myrtle Beach, South Carolina, USA, 2012, pp. 479–487.

(24) Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System," IEEE Sensors Journal, vol. 19, no. 13, 2019.

(25) M. L. Psiaki and T. E. Humphreys, "GPS Lies," IEEE Spectrum, vol. 53, no. 8, pp. 26–53, 2016.

(26) K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach. Birkhäuser, Boston Basel Berlin, 2007.

(27) A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Two-Dimensional Signal Quality Monitoring For Spoofing Detection," NAVITEC 2016, no. 14-16 December, 2016.

### Authors



**Sascha Bartl** has a background in geodesy with a special focus on satellite navigation and detection of intentional interference. He has been involved in several

international research projects, developing jamming and spoofing monitoring solutions. Furthermore, he is currently working on his Ph.D. about spoofing detection at Graz University of Technology.



**Manuel Kadletz** is Product Manager for GNSS Quality Assurance at OHB Digital Solutions GmbH and has been with the company for 5 years. Since being at OHB Digital

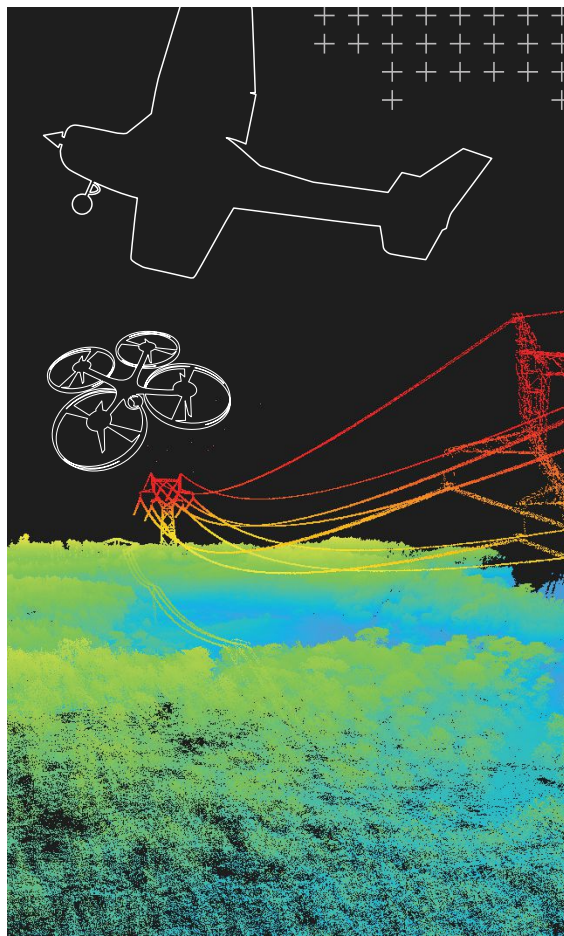
Solutions GmbH he has taken part in international research projects as a software developer and project manager.



**Philipp Berglez** is a professor at Graz University of Technology where he leads the working group navigation of the Institute of Geodesy. From 2010 till 2021 he worked as CTO of OHB Digital Solutions. He is focusing on positioning algorithms, GNSS signal and data processing and GNSS software-based receivers.



**Tomáš Duša** has a background in air traffic management and aviation in general. He has been involved in the space technology domain for more than a decade, focused primarily on GNSS not only in transport but in all markets. Since his Ph.D. research he has specialized in GNSS RFI detection and mitigation. He is active now as the director of the Czech GNSS Centre of Excellence.



## Save time and money with Applanix Direct Georeferencing

- ▶ Ditch Ground Control Points and reduce image overlap
- ▶ Speed up data processing with POSPac MMS/POSPac UAV software
- ▶ Survey hard-to-reach areas with ease

### Applanix User Group Meeting and Conference

September 20-22, 2022 | Fremont, CA, USA  
Register now at [info.applanix.com/ugm2022](http://info.applanix.com/ugm2022)

Applanix Corporation  
85 Leek Crescent, Richmond Hill, ON L4B 3B3 Canada  
T +1-905-709-4600, F +1-905-709-6027  
[info.applanix.com/airborne-video](http://info.applanix.com/airborne-video)  
[airborne@applanix.com](mailto:airborne@applanix.com)





Shield AI's V-BAT, a 135 lbs vertical takeoff and landing (VTOL) UAS capable of takeoff & landing with landing zones as small as 12' x 12'.

## Up Against It

### Advanced UAVs Overcome the Big Challenges of VTOL, Air Launch and Jamming

As tactical UAVs come of age, inertial technology's ability to endure GPS outages while providing reasonable accuracy at high update rates keeps it as the backbone of UAV sensor systems. Coupling inertial with M-code, anti-jam antennas and vision in the autonomous arsenal can make the sum of parts a very robust solution.

In defense applications, as military users look to achieve new capabilities with unmanned autonomous aircraft, three main areas come into sharp focus: vertical takeoff and landing (VTOL), launching of UAVs from other flying aircraft, and overcoming jamming in GNSS-denied environments. Coupling a high-performance inertial measurement unit

(IMU) with other sensing and navigation technologies on a UAV into a highly capable inertial navigation system (INS) can bring a solution to overcome each of these obstacles.

"The GNSS-aided INS is the backbone for these types of systems," said Jeremy J. Davis, Ph.D., Director of Engineering, VectorNav. "It can ride through GPS

outages and do it at high update rates, and still be reasonably accurate. Beyond that, different enabling technologies like anti-jam M-code and vision can merge with it and provide a more robust solution. That is a space of heavy activity right now, and we're working on solutions internally and with partners that meet these types of requirements and do so seamlessly."

VTOL, air launch and GNSS spoofing and jamming are all challenging UAV problems that haven't been fully solved yet, but state-of-the-art companies are designing next-generation vehicles that will take them on.



## VTOL

The ability to launch and retrieve a UAV without the expense, exposure and advance logistics required by a runway presents obvious tactical advantages to mobile warfighters. Rotorcraft such as helicopters and quad-rotors require only a small takeoff and landing zone, but they are inefficient compared to fixed-wing UAVs, and have dramatically lower range, payload capacity, and dwell time. Catapult-launched fixed-wing UAVs solve half the problem, but still require a runway for recovery—and catapults are cumbersome to transport.

VTOL aircraft avoid all these disadvantages and bring the cruise and payload advantages of fixed-wing UAVs. There are broadly three approaches to VTOL:

- a hybrid rotorcraft and fixed-wing vehicle, also known as a quadplane, with a set of vertical propellers for takeoff and landing and one or more horizontal props for cruising;
- a tiltrotor vehicle, using the same propellers are used for vertical and horizontal propulsion, rotating them

in mid-air relative to the vehicle;

- tail-sitter UAVs which takeoff and land on their tails, like a rocket, but cruise horizontally, accomplishing both types of flight with one fixed set of propellers.

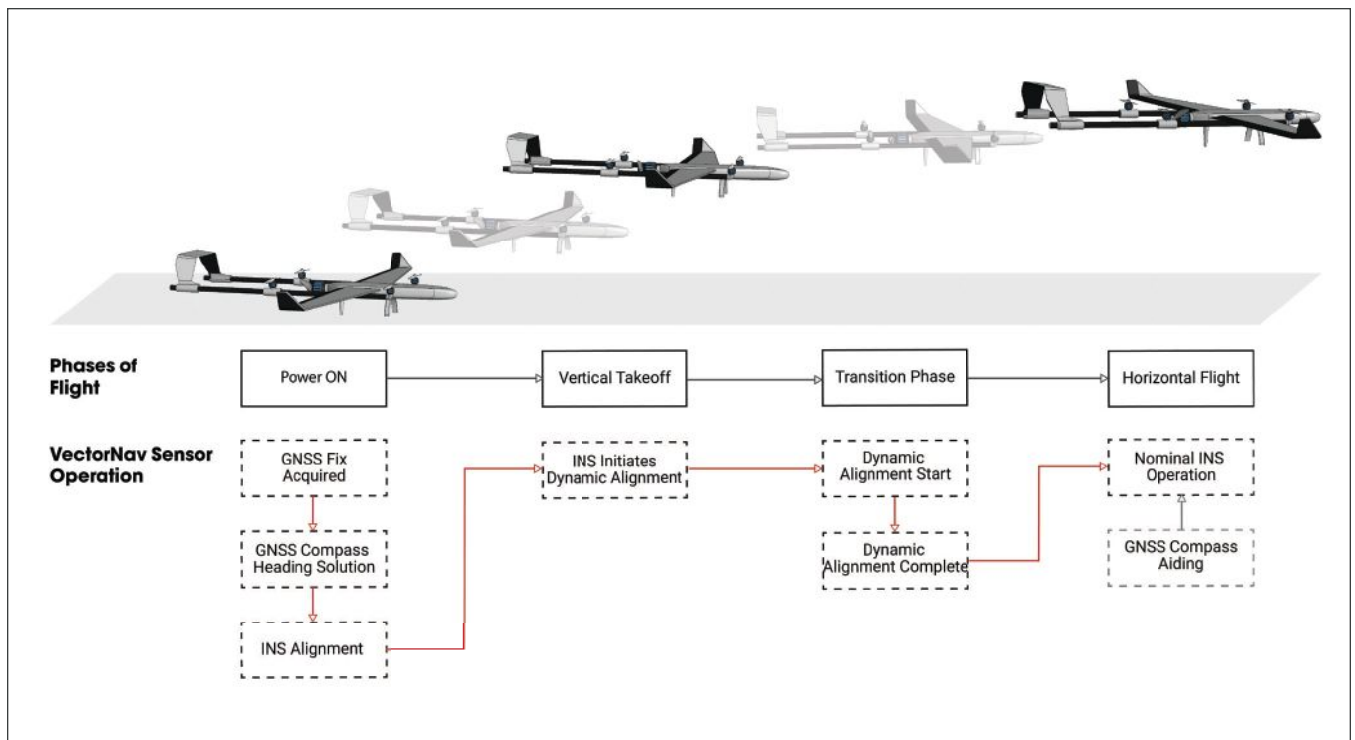
All types of VTOL craft require more from their navigation systems than other types of UAVs. “Takeoff and landing are the most dangerous, riskiest elements of flight for all types of aircraft,” said Davis. “When you’ve got these VTOL aircraft that are reimagining how to do takeoff and landing, it presents obvious inherent risks. You have to make sure you’ve got all your I’s dotted and T’s crossed.”

The introduction of a major in-flight transition at a mission’s beginning and end—quadplanes switch from one set of props to another, tiltrotors rotate their entire propulsion system, and tailsitters switch from getting lift from their wings to solely from their propellers/rotors—presents several challenges for the navigation system. VectorNav has been working through these problems with customers over the last five years and brings this experience to bear on

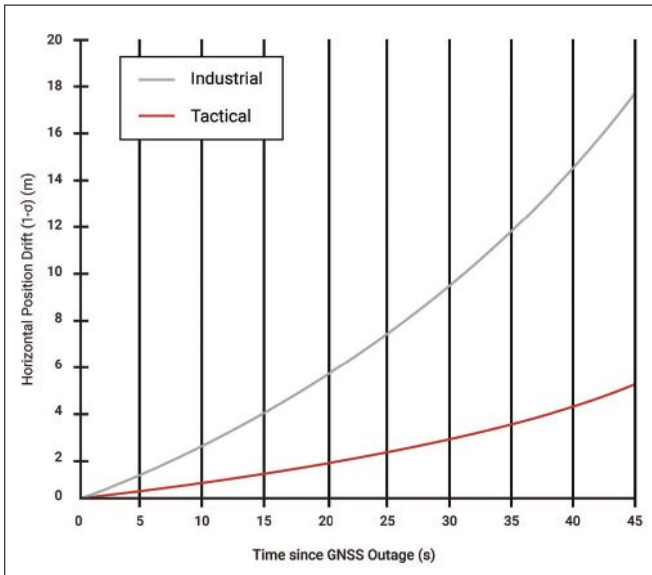
what is rapidly becoming the next frontier for tactical military UAVs.

The requirements on the navigation system include:

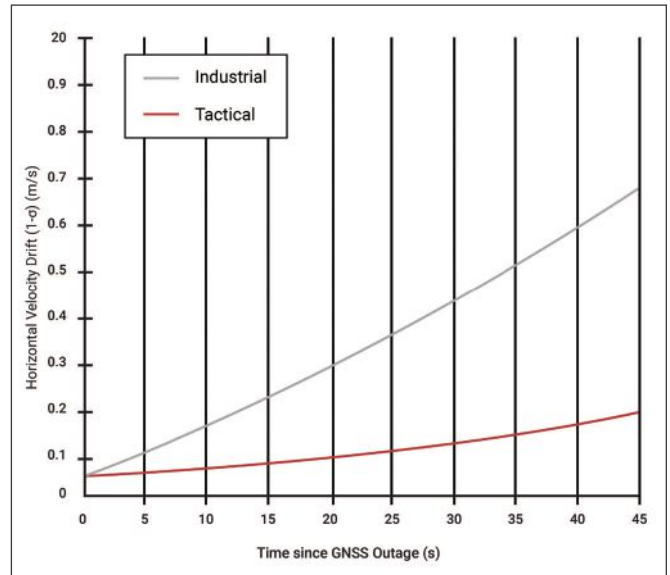
- **Absolute reliability.** Other control dynamics must be carefully monitored and managed; there’s no room to worry whether the navigation system can be trusted through the transition. For tail-sitters, this also means algorithms that avoid gimbal lock when rotating 90 degrees in pitch during the transition.
- **Slow and fast operation.** To track heading, hovering aircraft typically rely on a GNSS compass: two GNSS antennas a fixed distance apart. Fixed-wing aircraft use an INS-generated heading following a dynamic alignment process, correlating the motion measured by the GNSS and the IMU. For a VTOL aircraft, both techniques are critical for different phases of flight, and the handover between the two must be flawless to avoid compounding problems during vertical-horizontal flight switch. VectorNav dual-antenna



**FIGURE 1:** Modes of Operation of a Navigation System for a VTOL from Power-On to Horizontal Flight.



**FIGURE 2:** Horizontal Position Drift after loss of GNSS (post INS alignment).



**FIGURE 3:** Horizontal Velocity Drift after loss of GNSS (post INS alignment).

GNSS systems like the VN-300 and VN-310 smoothly transition between whichever heading source is the most accurate at any given time.

- **Landing:** Some of the most advanced systems in development must land on moving platforms such as ships or trucks. This requires extremely high precision. An RTK-enabled GNSS receiver, like those found on the VectorNav Tactical Series units, can provide centimeter-level relative positioning at high update rates.

#### AIR-LAUNCHED

One way of multiplying the range of a UAV, while also avoiding the downsides of a runway, is to launch it from a much larger aircraft already in flight. These UAVs are often tube-launched, with wings that unfold/unfurl in the first seconds of flight as it emerges from the host aircraft already at top cruising speeds. The transition phase for these UAVs is quite dramatic.

All of this places severe strains on the navigation system: rotations of a few 1,000 degrees per second in the airstream and high acceleration rates. It's a wild, rolling ride during which GNSS is typically lost, whether due to the high G's, the abrupt switch from the host's GNSS antenna to the UAV's antenna,

or the fact that the UAV antenna may not point reliably skyward until stable flight is reached.

Air-launched UAVs must also cope with buffeting from the wake of the launching aircraft. Shocks are high and the accelerations and angular rates experienced immediately upon deployment are extreme until the UAV's wings unfurl and can stabilize the craft. Stabilization itself is a critical achievement for the navigation system to control, to catch itself before falling headlong downwards.

It's an exciting handful of seconds. All of this requires the navigation system to run in a pure inertial navigation mode, tracking through high g-loading and higher angular rates. As with the VTOL aircraft, this period right after launch is critical to mission success.

#### GPS-CHALLENGED ENVIRONMENTS

Having to operate with a GNSS signal that may be spurious, or without GNSS altogether, poses a whole new set of problems for a tactical UAV. An active spoofer or jammer in operational theater area interferes with the UAV's onboard GNSS receiver, and the right mitigation technologies must come into play to maintain accurate tracking in these extremely difficult environments.

GPS M-code receivers now being gradually deployed throughout the US military and those of its allies replace the SAASM (Selective Availability Anti-Spoofing Module) receivers that previously thwarted spoofing attempts. M-code technology also takes advantage of new, more powerful signals from the latest GPS satellites to counter jamming as well. VectorNav's Tactical Series of INS systems have full support for interfacing with those new types of receivers.

To complete spoofing mitigation, anti-jam or controlled reception pattern antennas (CRPAs) consist of multiple elements, allowing them null signals coming from directions likely to contain spoofers jammers while amplifying signals from known satellite directions.

The combination of a tactical grade IMU with an M-code GNSS receiver and an anti-jam antenna provides a navigation solution robust to common GNSS-challenged (spoofed) environments.

Short-duration GNSS outages, lasting seconds to a few minutes can be readily handled by VectorNav's tactical grade GNSS/INS sensors like the VN-210, relying on pure integration of the accelerations and angular rates reported by the inertial sensors to provide navigation when GNSS is unavailable.

“Because we have good IMUs in our tactical series,” said Jakub Maslikowski, Director, Sales and Marketing, VectorNav Technologies, “we can handle GPS challenged conditions for limited periods of time. To the extent that somebody does manage to jam you briefly, the inertial sensors will carry you through.”

**GPS-DENIED**

Increasingly, continued operation in GNSS-challenged environments isn’t enough: UAVs must also operate in fully GNSS-denied situations, where powerful enemy jammers attempt to control the field. Larger systems, including manned aircraft, can rely solely on a navigation-grade INS, which drifts on the order of kilometers per hour. But a navigation-grade INS is far too large and expensive for most UAV applications.

Achieving accurate, reliable navigation without either GNSS or a navigation-grade INS is an area of active R&D at VectorNav involving many different sensing technologies.

Electro-optical and/or infrared (EOIR) camera systems have come into increasing play for GNSS-denied navigation. Image-processing software processes each image to identify unique features that it would recognize again in the next image taken, a process known as feature matching.

If a UAS has pictures of the area taken prior to the mission, by satellites or other overflight, this enables a map-matching approach: matching the features from the real-time images to the stored image map for localization, thus determining UAV position. This can supply high accuracy but requires significant advance preparation. It only works over an already-known area, flying a predefined path at a predetermined time of day, since shadows and lighting differences can impact the accuracy of map- or image-matching.

When a map isn’t available, vision-based navigation systems can create their own map as they go, using simultaneous localization and mapping (SLAM). The drawback of SLAM is that the map will be imperfect, and those imperfections grow over time. SLAM position errors drift as a function of distance travelled.

All vision-based systems struggle, naturally, in limited visibility such as clouds or fog. Active sensing systems like radar or LiDAR, which emits laser pulses to produce a 3D map, can replace or augment vision systems. However, active sensing brings the downside of potentially revealing one’s own position to the enemy through the emitted signals.

Finally, all of these technologies fail when the environment, such as large bodies of water or a sandy desert, contains no distinct features.

As an alternative to outfitting smaller UAVs with complex GNSS-denied navigation systems, an aircraft “buddy system” can involve multiple UAVs operating in the vicinity of a larger aircraft equipped with a navigation-grade INS. The large, heavy and expensive navigation-grade INS can fly for hours without drifting more than a couple kilometers. This then shares its location with the smaller UAVs through various combinations of radio links, visual markers and other techniques.

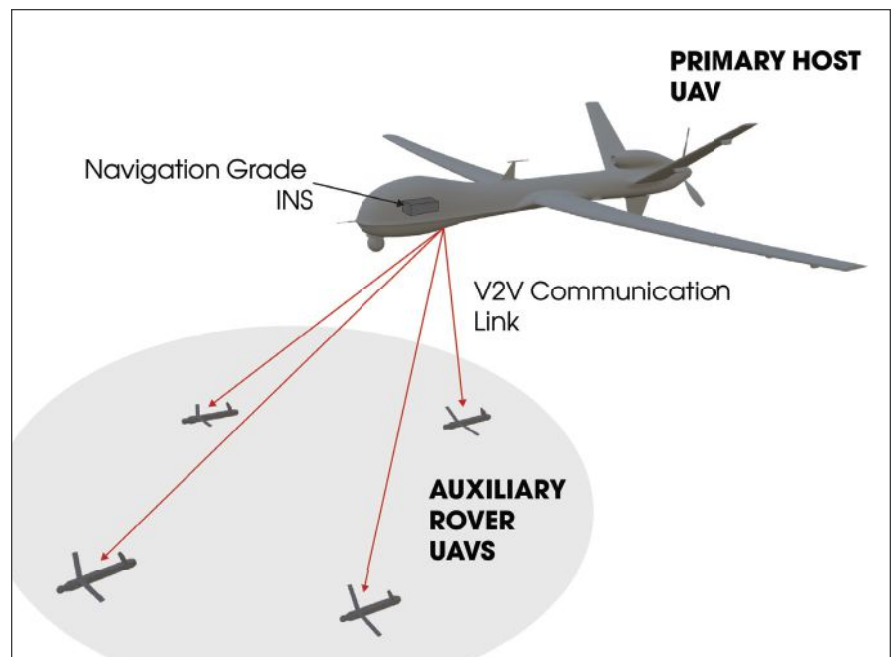
Clearly, there is no one solution that counters GNSS signal jamming under all conditions. A robust, reliable and versatile system must combine several technologies, playing

the strengths of some off the weaknesses of others. This is where a highly adaptable and flexible INS system with a tactical-grade IMU can provide tremendous value, functioning as the linkage of a multi-sensor system. VectorNav has been working for years with some of the most advanced companies exploring each of these technologies and integrating them with algorithms for a powerful anti-jamming solution.

**CONCLUSION**

VTOL and air-launched UAVs will dramatically alter the landscape of UAS for military use. Their unique flight profiles, however, require sophisticated navigation systems that go beyond traditional INS capability. VectorNav is taking the lead in integrating the latest navigation technologies to handle these demanding situations.

Making these systems robust to GPS-denied conditions means integrating the latest PNT technologies, from M-Code to anti-jam to vision. Working closely with a partner like VectorNav that can integrate with these various complementary technologies can provide tremendous value and save considerable engineering resources. Go to [www.vectornav.com](http://www.vectornav.com) to begin the process. ▲



**FIGURE 4:** Sharing of Navigation Data from Primary to Rover UAVs.



## NAUTILUS: An Embedded Navigation Authentication Testbed

The low-cost, lightweight platform can be easily configured for a variety of applications and test scenarios. This article focuses on its use for GNSS authentication.

The need to protect GNSS based Position, Velocity and Time (PVT) against malicious attack has been the subject of much research in recent years. At the system side, Galileo is in the process of implementing both Navigation Message Authentication (NMA) and Spreading Code Encryption (SCE) in the current generation of satellites [1, 2, 3], and GPS is investigating options for introducing similar protections on L1C [4].

NMA provides authentication of the navigation message, ensuring it cannot be arbitrarily modified by a malicious actor, but also tying the broadcast data to a particular instant in time. This forces the attacker to observe and repeat the true data and provides the participating user with a lower bound on the current time.

SCE is a mechanism to protect the navigation signals by modulating them with encrypted sequences, either in whole [5] or in part [4]. These encrypted sequences can be re-created only by a user with the appropriate cryptographic key. These keys are either maintained in authorized user receivers in secure tamper-proof modules [5], or kept private permanently, in which case the sequences themselves are broadcast publicly at some delay after the initial broadcast [4].

In essence, both schemes operate by adding elements of unpredictability to the broadcast signals, generating them in a way so the system operator can be demonstrated as the originator of these unpredictable elements. For NMA, the unpredictable elements are data bits included in the broadcast message, while for SCE the unpredictable elements are the chips of the spreading codes themselves.

We have developed a low-cost embedded platform, Nautilus, for testing GNSS authentication signal processing strategies in real world environments in real time. Nautilus is designed to be a low-cost, lightweight platform that can be easily configured for a variety of different applications and test scenarios. In this work we demonstrate its use in the context of GNSS authentication.

We give an overview of the Nautilus platform, describe test configurations developed, and present initial results of live sky testing and calibration, showing the platform's suitability for use in real time and post-mission testing of GNSS authentication. All the test campaigns are conducted using only publicly available information, for example the Galileo Open Service Navigation Message Authentication (OSNMA) testing specification [1], the Galileo E6 public Interface Control Document (ICD) [6] and the Chimera draft specification [7].

### System Overview

The Nautilus testbed is based on the LimeNET Micro development board from Lime Microsystems [8]. This board is designed to be a low cost (about \$350)

**CILLIAN O'DRISCOLL**  
INDEPENDENT CONSULTANT

**GIANLUCA CAPARRA**  
EUROPEAN SPACE AGENCY

platform for deploying narrow band wireless networks. It incorporates the following components:

- An LMS7002M RF transceiver chip, which performs down conversion to baseband and I/Q sampling at rates of up to 160 MHz
- A Raspberry Pi Compute Module 3+, which contains a quad core ARM Cortex A53 CPU operating at 1.2 GHz with 1 GB of RAM
- An Intel Altera MAX 10 Field Programmable Gate Array (FPGA), which acts as a gateway between the LMS7002M and the Raspberry Pi
- A u-blox MAX M8Q GNSS receiver, capable of tracking three systems at once from among GPS, Galileo, BeiDou and Glonass

The LimeNET micro is shown in **Figure 1**, with a biro included for scale. The platform is approximately the size of a modern smartphone and is easily portable.

The u-blox receiver generates a Pulse Per Second (PPS) timing signal that is input to the FPGA and used to tune the on-board oscillator—in effect operating as a low-cost GPS disciplined oscillator. This means the samples collected through the LMS7002M are collected with a clock drift measured in Parts Per Billion (ppb) relative to GPS system time, albeit with relatively poor short-term stability.

The LMS7002M is a high performance 2x2 Multi Input Multi Output (MIMO) chip, with a frequency range covering 30 MHz to 3.8 GHz, and a 12-bit Analog-to-Digital Converter (ADC) capable of operating at up to 160 Msps. The LimeNET Micro board is not able to take full advantage of this chipset. It is limited to Single Input Single Output (SISO) operation and a maximum sampling rate of about 10 to 12 Msps. The raw samples are packetized in the FPGA and then streamed to the Raspberry Pi over an integrated Universal Serial Bus (USB) interface.

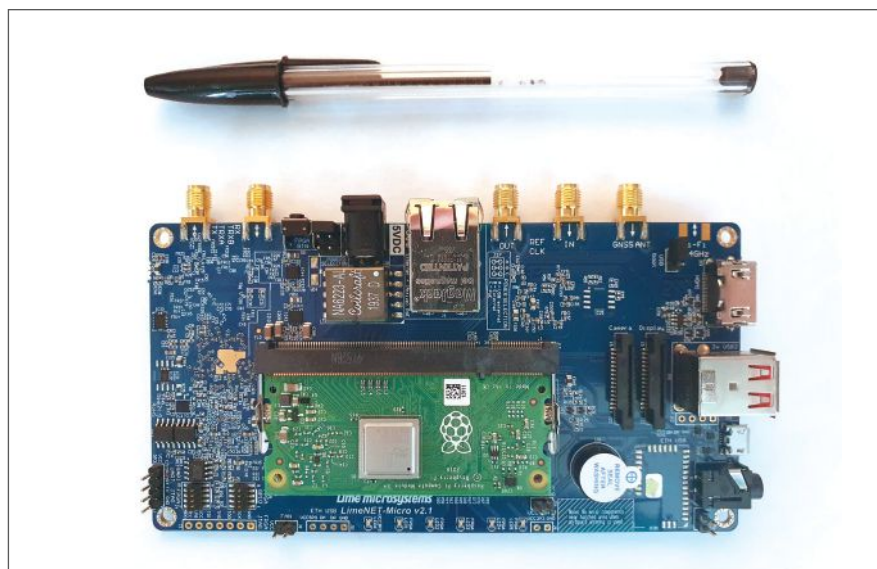
### Hardware Modifications to the LimeNET Micro

A number of minor modifications and additions were made to the LimeNet Micro to increase its usefulness for GNSS applications. The first step was to synchronize the data collection with

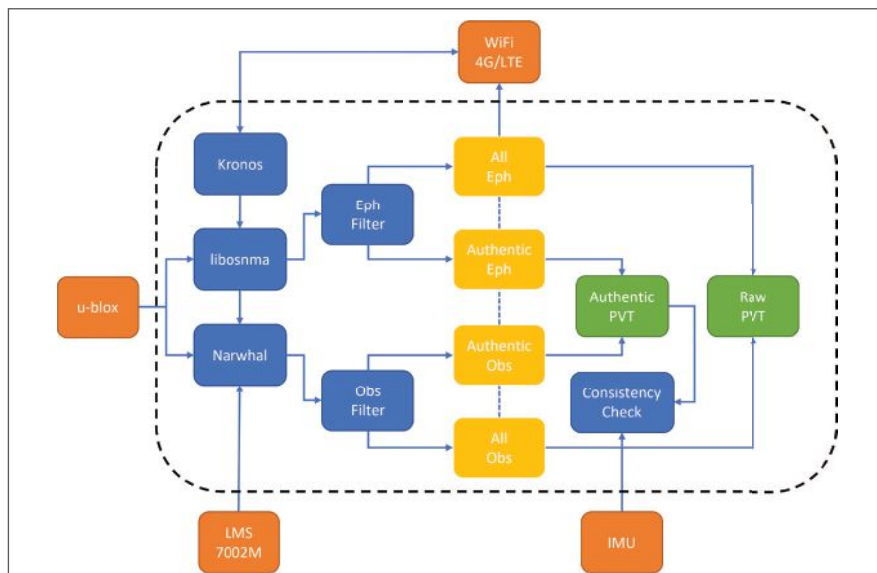
GNSS time from the u-blox receiver. The pre-existing hardware achieved a very close syntonization (i.e. matching in frequency) but for authentication we also need close alignment in time.

To this end, the FPGA firmware was updated so that, once enabled, data collection is triggered on the next rising edge of the PPS. The LimeNET Micro is fully open-source hardware, so the FPGA source files are all available online [9]. The modified gateway for Nautilus can be found in [10]. With this modification, data collections can be triggered to occur only at 1 second boundaries, but this is not seen as a major limitation.

To know precisely the time at which the data collections are triggered, it is necessary to have an accurate time reference on the Raspberry Pi, which acts as the overall controller for the Nautilus platform. For that to be achieved, the Network Time Protocol (NTP) software is used in conjunction with the raw NMEA messages logged from the u-blox receiver. To ensure the NTP time is as closely aligned to the GNSS system time as possible, the FPGA firmware was updated again to route the u-blox PPS signal to one of the Raspberry Pi General Purpose Input/Output (GPIO) pins. The NTP software is then able to use the PPS signal to achieve time synchronization with the u-blox that



**FIGURE 1** Unmodified LimeNet Micro, with biro for scale.



**FIGURE 2** System level view of the Nautilus hardware and software components.

is accurate at the microsecond level. Again, this modification is available at [10].

The final modification to the LimeNET Micro boards was the addition of two non-fixed resistors to open up a previously unused USB connection between the Raspberry Pi and the u-blox receiver. This is a particularly important addition in that it enables two-way communication with the GNSS receiver, without modifying the configuration on its serial port, which logs the NMEA message used by the FPGA as part of the clock taming circuitry.

With this modification, it became possible to enable Galileo processing on the u-blox receiver (which was disabled by default), and to log raw navigation messages for all tracked satellites. This last feature was essential to enable real-time processing of Galileo OSNMA data. We had hoped to also log raw observables (pseudorange, Doppler and  $C=N_0$ ) but unfortunately the u-blox receiver model does not support this feature. A work-around has been developed, using a combination of decoded ephemeris, raw PVT information and raw Doppler and code-phase measurements.

In addition to the above modifications to the LimeNET micro hardware, Nautilus also includes two additional peripherals:

1. A Bosch BMO055 9-DOF Inertial Measurement Unit (IMU), connected via serial port
2. A WiFi/3G/4G LTE USB dongle

**Software Components**

The Nautilus functionality is provided through a number of inter-connected

```

11:43:44.102 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 15 AD: 8 ID: 5, CTR=10, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.102 TRACE nac_pool.c:385: VERIFICATION SUCCESS: PRN= 3, PRN_A= 25, Ad= 0, ID= 3, CTR= 3, KEY= 201
11:43:44.102 TRACE nac_pool.c:1213: Extracted MAC section from PRN 15 cstr: 474239
11:43:44.103 INFO context.c:474: Unknown mac sequence lookup: 32, svId 15 @ 1108 474239
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 15 AD: 8 ID: 5, CTR= 3, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 69 AD: 8 ID: 5, CTR= 9, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 8 AD: 8 ID: 5, CTR= 3, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 69 AD: 8 ID: 5, CTR= 4, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 15 AD: 5 ID: 5, CTR= 5, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 15 AD: 8 ID: 5, CTR= 6, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 8 AD: 5 ID: 13, CTR= 7, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 255 AD: 4 ID: 8, CTR= 6, WN: 1108, TOM: 474210, signed by key: 209
11:43:44.103 TRACE nac_pool.c:246: OSNMA_MAC_POOL Added MAC: PRN: 15 AD: 12 ID: 5, CTR= 9, WN: 1108, TOM: 474210, signed by key: 219
11:43:44.103 TRACE nac_pool.c:385: VERIFICATION SUCCESS: PRN= 13, PRN_A= 15, Ad=12, ID= 1, CTR= 9, KEY= 194
11:43:44.104 TRACE nac_pool.c:385: VERIFICATION SUCCESS: PRN= 24, PRN_A= 25, Ad=0, ID= 3, CTR= 9, KEY= 194
11:43:44.104 INFO nac.c:118: MAC data not contiguous with previous, resetting (0x902639 != 2 or 7 != 7)
11:43:44.104 INFO nac.c:127: NotLog for start of subframe
    
```

**FIGURE 3** Nautilus OSNMA logs from November 2020. Note the successful validation of a number of navigation messages.

software components, including both commercial off the shelf (COTS) and custom elements.

**COTS:**

- Network Time Security (NTS) over NTP, for authenticated time transfer [11]
- Roughtime, also for authenticated time transfer [12]

**Custom:**

- libosnma, an implementation of the OSNMA based on the user ICD for the testing phase, which is available online [1]
- Narwhal, a snapshot authentication tool
- Kronos, authenticated time synchronization using NTS over NTP and Roughtime
- Integration software implemented in Python including IMU, clock modelling (error modelling), clock bound modelling, and u-blox interface software

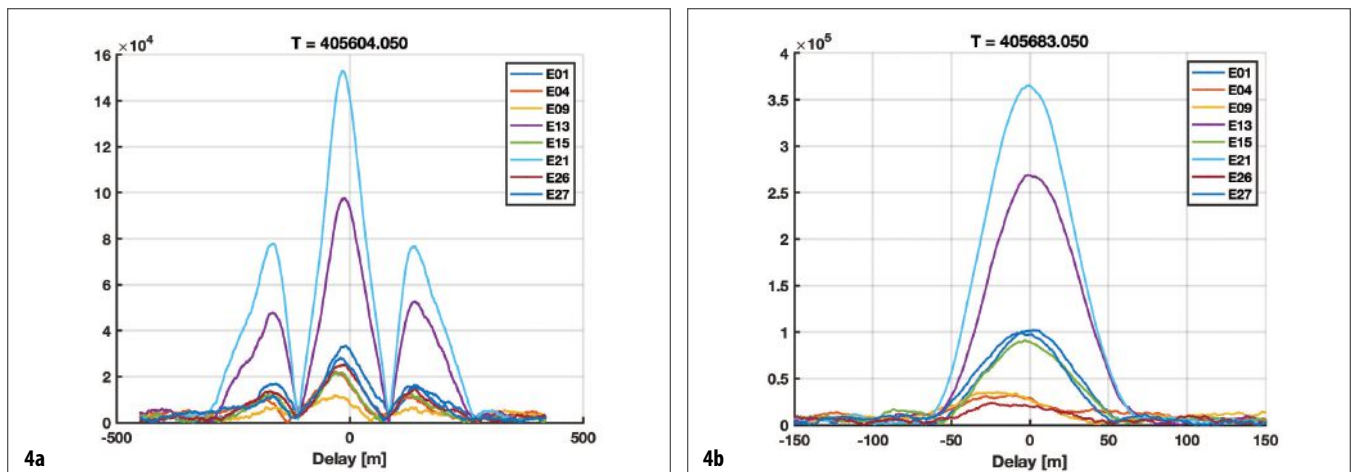
The software components are pluggable, so for example, the u-blox integration tool, libosnma and Kronos tools all integrate to provide OSNMA functionality in real-time,

including assurance that the time synchronization requirement is met. Similarly, the Narwhal snapshot tool integrates with NTP and the u-blox software to generate time-stamped snapshots including PVT, ephemeris and observation data extracted from the u-blox. This is very useful for post-processing. The raw snapshot data can be processed to determine if the expected signals are present, or if spoofing signals are present nearby, for example.

**Configuration Options**

Given the hardware and software components, Nautilus can provide the following system level services (although not necessarily all at once):

- Real-time testing of Galileo OSNMA, including the authenticated time synchronization requirement via the Kronos software
- Delayed release of encrypted sequences for spreading code authentication. For example:
  - Taking snapshots of Galileo E6-C, which will be encrypted as part of the upcoming Commercial Authentication Service (CAS)



**FIGURE 4** Snapshot correlations for 100 ms snapshots; a) Galileo E1C; b) Galileo E6C. Here the snapshots were collected at the timestamps indicated, and the Galileo E1 observables from the u-blox receiver were used to predict the pseudorange and Doppler.

[3]. These snapshots can be post-processed to determine the presence of the encrypted chips that are (potentially) released after some delay.

- Taking snapshots of GPS L1-C, which may contain secure marker sequences as part of the proposed Chimera scheme [7].
- Dynamic error model mismatch detection, using the clock model and IMU.
- Angle of arrival spoofing detection, using a different antenna for the LMS7002M than used for the u-blox receiver.
- Clock bound modeling, based on authenticated two-way time transfer.
- Anti-spoofing testbed. Using the timestamped snapshots, it is relatively straightforward to emulate a variety of different spoofing attacks in post-processing. **Figure 2** shows a system level view of the hardware and software components.

### Sample Results

Nautilus has been used as an R&D tool for GNSS authentication over the last two years. Here we show some sample processing results obtained with the platform.

### Early OSNMA Testing



In November 2020, the Galileo program began an internal OSNMA test campaign, in which valid OSNMA data was broadcast through the Galileo E1 OS signal. The details of the signal configuration, and indeed the most up to date signal specification, were not public at the time, and we did not have access to these elements for this work. Nevertheless, Nautilus was deployed to process the live OSNMA signals in real time using NTS for secure time transfer for establishing the loose time synchronization bound required for OSNMA processing.

**Figure 3** shows a snapshot from the Nautilus OSNMA log, captured as a screenshot in real-time from a remote terminal connection to the device in late November 2020.

### Snapshot Calibration and Testing

The main reason for choosing the LimeNET Micro as a basis to build Nautilus on was the synchronization of the sampling clock with GNSS time. In theory, this should allow the collection of snapshots of data with a precisely known time of reception. This, in turn, makes the tool incredibly useful in evaluating signal level authentication features, such as Galileo CAS on E6 and GPS Chimera on the L1C signal. **Figure 4** shows the correlation functions over all Galileo satellites in view for two snapshots: one for the Galileo E1 band and one for the Galileo E6 band.

The snapshots were triggered by the rising edge of the PPS from the u-blox receiver, and the nominal pseudorange and Doppler were computed based on the u-blox observables. The figures show the correlations evaluated with a 1 metre resolution over a range sufficient to cover  $\pm 1.5$  chips around the nominal peak. In this case, the nominal calibrated offset between the start of



**January 23-26, 2023**  
Hyatt Regency Long Beach  
Long Beach, CA

INTERNATIONAL  
TECHNICAL MEETING

**ITMP**

PRECISE TIME AND TIME  
INTERVAL SYSTEMS AND  
APPLICATIONS MEETING

**PTI**

One Registration  
Fee, Two Technical  
Events and a  
Commercial Exhibit

**ABSTRACTS DUE OCTOBER 7**

**ion.org**

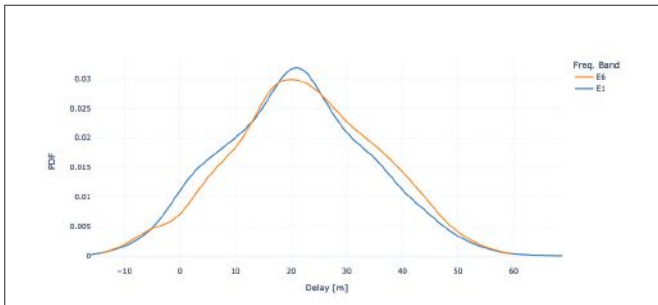


FIGURE 5A Distribution of the computed delay between the computed pseudorange and that measured from the snapshot file.

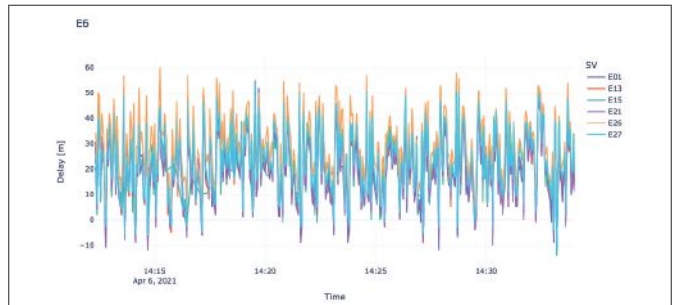


FIGURE 5B Time history of the delay for the E6 snapshots.

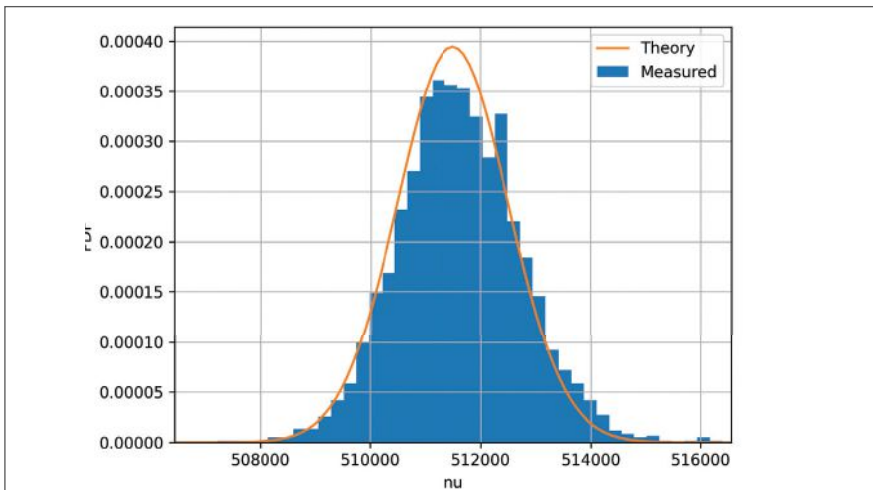


FIGURE 6 Theoretical and observed distributions of the attack agnostic defense decision statistic for static data using Galileo E6C snapshots.

**Assured PNT**

The final stage is to integrate the OSNMA-authenticated navigation messages with snapshot observations that pass the authentication check to obtain “assured” PNT solutions. Again, the resulting solution is not in fact assured at all as it is based on processing the E6C signal while it is not encrypted, but this demonstrates the feasibility of the approach.

Figure 7 shows the results for a data set collected on April 6, 2021. The data set is divided into two parts. During the first half Nautilus was configured to collect snapshots on E6, while during the second half E1 snapshots were collected. Figure 7a shows the difference in both North and East directions between the u-blox position and that computed from authenticated observations and ephemerides. Note here we assume the snapshots that pass the authentication test are authentic, even if the chips are not encrypted. This is simply as a proof of concept.

Similarly, Figure 7b shows a time history of the vertical and clock differences. Here we can again clearly see the impact of the sliding of the PPS with respect to the 10 Msp/s sampling clock as the time error varies between -30 and +30 m. Interestingly, there is also an approximate 10 m bias in the vertical, which is likely from the coupling between clock and vertical errors, but warrants further investigation.

**Conclusion**

In this work, we introduce the Nautilus GNSS authentication testbed. Its utility as a tool for the analysis of NMA and SCE has been demonstrated both in static and dynamic conditions. It is a low-cost, highly portable, highly configurable platform that is intended to be

the recording and the PPS has been subtracted.

For the purposes of calibration, a large number of such snapshots were recorded and the offset of the peak from the nominal was computed. Figure 5a shows some results for the statistics of these observed offset for data collections at 10 Msp/s. Here we see an average bias of approximately 20 m, with a variation of  $\pm 30$  m. This variation can be explained by the fact that the PPS “slips” with respect to the sampling clock, and at 10 Msp/s, each sample corresponds to approximately 30 m. This can be seen in Figure 5b where the saw-tooth nature of the delay is apparent, as is its commonality across all satellites in each snapshot.

Note this bias includes all the divergence effects between the nominal pseudorange as measured by the u-blox and observed in the snapshot, including differential group delays and the impact of the ionosphere when considering E6 (because the u-blox measurements are based on E1/L1 only). The consistency

of this bias shows Nautilus can be used for signal authentication testing.

**Signal Level Authentication**


To validate this claim, a simple test was constructed to verify a signal authentication scheme in which it is assumed the E6C samples have been encrypted. The scheme is described in detail in [13], but in essence depends on computing both the correlation function, as shown in the previous section, and the “attack agnostic decision statistic,” denoted  $v$ .

Figure 6 shows the distribution of this decision statistic as measured from E6C signals using snapshot processing with 100 ms snapshots at 12.5 Msp/s. The figure shows both the observed and theoretical distributions of the decision statistic, which are seen to match very closely. Again, this indicates Nautilus is an appropriate tool for assessing these kinds of techniques. Note also the E6C signal was not encrypted in this case, but the principle is of course the same.



used for authentication, but can easily be configured for other uses like signal quality monitoring or recording snapshots of interesting GNSS signal events such as jamming or ionospheric scintillation.

The tight time and frequency synchronization between the collected snapshots and GNSS time make this simple board a unique and incredibly useful tool for GNSS signal authentication research and development.

Unfortunately, due to the global supply chain issues resulting from the COVID-19 pandemic, the manufacturers of the LimeNET Micro have made the decision to discontinue development of this very useful board. However, the entire board is open-source hardware, with full details available from [8] should anyone wish to manufacture the board for themselves. 

### Acknowledgments

This work was supported by the European Space Agency under Contract No. 4000120583/17/NL/CRS/hh.

### References

- (1) European Commission, "Galileo open service navigation message authentication (OSNMA) user ICD for the test phase," Issue 1.0, 2021. [Online]. Available: <https://www.gsc-europa.eu/electronic-library/programme-reference-documents>
- (2) T. Cozzens, "Tests begin of Galileo's OSNMA signal authentication service," *GPS World Magazine*, 2021.
- (3) I. Fernandez-Hernandez, G. Vecchione, and F. Diaz-Pulido, "Galileo authentication: A programme and policy perspective," in 69th International Astronautical Congress, 2018.
- (4) J. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B.W. O'Hanlon, J. J.

Rushanan, L. Scott, and R. A. Yazdi, "Chips-message robust authentication (chimera) for GPS civilian signals," in Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017), 2017, pp. 2388–2416.

- (5) O. Pozzobon, L. Canzian, M. Danieletto, and A. Dalla Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," in 2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC). IEEE, 2010, pp. 1–6.
- (6) European Commission, "Galileo E6-B/C codes technical note," 2019. [Online]. Available: <https://www.gsc-europa.eu/electronic-library/programme-reference-documents>
- (7) Air Force Research Laboratory, "IS-AGT-100 Chips Message Robust Authentication (Chimera) Enhancement for the LIC Signal: Space Segment / User Segment Interface," 2019.
- (8) "LimeNET micro product page." [Online]. Available: <https://www.crowd-supply.com/lime-micro/limenet-micro>
- (9) "LimeNET micro gateway source." [Online]. Available: <https://github.com/myriadrf/LimeNET-Micro-GW>
- (10) "CODC fork of limenet micro gateway source." [Online]. Available: <https://github.com/odrisci/LimeNET-Micro-GW>
- (11) D. Franke, D. Sibold, K. Teichel, M. Dansarie, and R. Sundblad, "Network time security for the network time protocol," Working Draft, IETF Secretariat, Internet-Draft draft-ietf-ntp-using-nts-for-ntp-20, Jul. 2019. [Online]. Available: <http://www.ietf.org/internet-drafts/draft-ietf-ntp-using-nts-for-ntp-20.txt>
- (12) A. Malhotra, A. Langley, and W. Ladd, "Roughtime," Working Draft, IETF Secretariat,

Internet-Draft draft-roughimeaanal-03, Jul. 2019, <http://www.ietf.org/internet-drafts/draft-roughimeaanal-03.txt>.

- (13) C. O'Driscoll, T. Scuccato, A. Dalla Chiara, T. Pany, M. Arizabaleta Diez, M. S. Hameed, "The attack agnostic defence: a spoofing detection metric for secure spreading sequences," in Proceedings of Navitec 2022.

### Authors



#### Cillian O'Driscoll

received his M.Eng.Sc. and Ph.D. from the Department of Electrical and Electronic Engineering, University College Cork, Ireland. He

was a senior research engineer with the Position, Location and Navigation (PLAN) group at the Department of Geomatics Engineering in the University of Calgary from 2007 to 2010. He was with the European Commission from 2011 to 2013, first as a researcher at the JRC, and later as a policy officer with the European GNSS Programmes Directorate in Brussels. From January 2014 to June 2017, Dr. O'Driscoll was a research fellow at University College Cork. He is currently an independent consultant. His research interests are in all areas of GNSS signal processing.



#### Gianluca Caparra

received a Ph.D. in information engineering from the Università Degli Studi di Padova, Italy. He is currently a radio-

navigation system engineer with the European Space Agency. His research interests include positioning, navigation and timing assurance, cybersecurity, signal processing, and machine learning, mainly in the context of global navigation satellite systems.

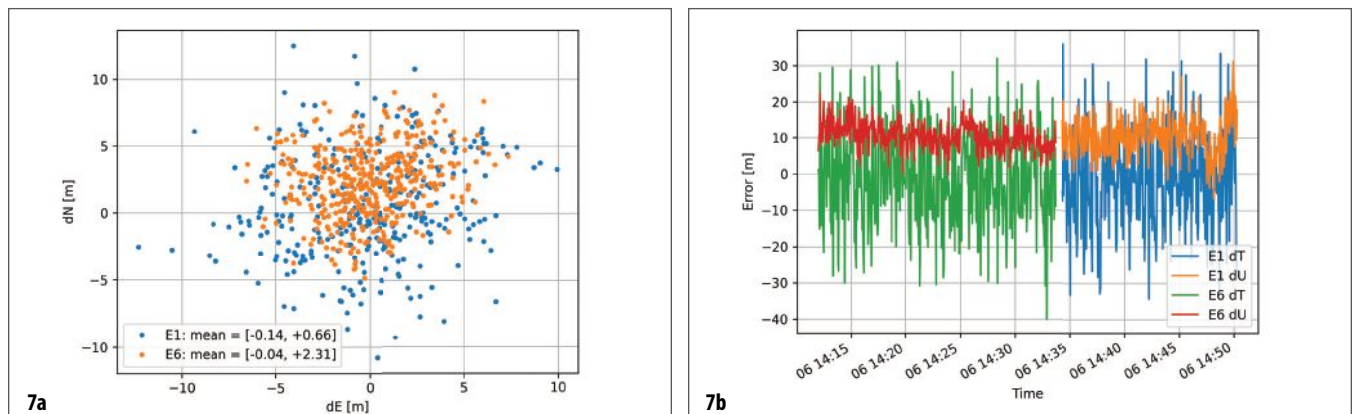


FIGURE 7 Differences between u-blox position and "assured" position from combined OSNMA and snapshot processing.

# Detecting GNSS Spoofing

This new method makes it possible to decompose the Complex Cross Ambiguity Function of GNSS signals during malicious spoofing attacks.

SAHIL AHMED, SAMER KHANAFSEH,  
BORIS PERVAN  
ILLINOIS INSTITUTE OF TECHNOLOGY

**G**lobal Navigation Satellite Systems (GNSS) are used for Positioning, Navigation and Timing (PNT) worldwide and are vulnerable to Radio Frequency Interference (RFI) such as jamming and spoofing attacks. Jamming can deny access to GNSS service while spoofing can create false positioning and timing estimates that can lead to catastrophic results.

This article focuses on detecting spoofing, a targeted attack where a malicious actor takes control of the victim's position and/or time solution by broadcasting counterfeit GNSS signals [1]. We describe, implement and validate a new method to decompose the Complex Cross Ambiguity Function (CCAF) of spoofed GNSS signals into their constitutive components.

The method is applicable to spoofing scenarios that can lead to Hazardous Misleading information (HMI) and are difficult to detect by other means, including previously proposed methods that rely on observation of the magnitude of the CCAF alone [2]. This method can identify spoofing in the presence of multipath and when the spoofing signal is power matched and offsets in code delay and Doppler frequency are relatively close to the true signal. Spoofing

can be identified at an early stage within the receiver and there is no need for any additional hardware.

Different methods have been proposed to detect spoofing, such as received power monitoring, signal quality monitoring (SQM), pseudorange residual checks, signal direction of arrival (DoA) estimation, inertial navigation system (INS) aiding, and others [3] [4]. Each of these methods have their own advantages and drawbacks.

CAF monitoring approaches [5] can be used to detect spoofing but have disadvantages in environments with multipath and when the Doppler frequency and code phase of the received signal are closely aligned with the spoofed signal. Here, CAF monitoring refers to the inspection of only the magnitude of the CCAF, which is typical of signal acquisition algorithms and previously proposed spoofing monitoring methods.

A sampled signal can be represented in the form of a complex number,  $I$  (in-phase) and  $Q$  (quadrature), as a function of code delay and Doppler offset. In existing CAF monitoring concepts, a receiver performs a two-dimensional sweep to calculate the CAF by correlating the received signal with a locally generated carrier modulated by pseudorandom code for different possible code delay and Doppler pairs. Spoofing is detectable when two peaks in the CAF are distinguishable in the search space.

This could happen, for example, if a power matched spoofed signal does not accurately align the Doppler and code phase with the true received signal. In practice, because detection using the CAF is not reliable under multipath and for spoofed signals close to the true ones, we instead propose to exploit the full CCAF. We decompose the CCAF of the received signal into its contributing components—true, spoofed and multipath—as defined by their signal amplitudes, Doppler frequencies, code delays and carrier phases.

We introduce a method to decompose a CCAF made up of  $N$  contributing signals by minimizing a least-squares cost function. The optimization problem is non-convex. To deal with the nonconvexity we implement a Particle Swarm Algorithm (PSA). We show simulated results decomposing three different signals (true, spoofed and multipath) into their respective defining parameters—signal amplitudes, Doppler frequencies, code delays and carrier phases—for the ideal case without any noise and code cross correlations. We also show experimental results implementing the method in a software defined receiver in the presence of thermal noise and code cross-correlation (as well as multipath). The new method is validated against publicly available spoofing datasets, including TEXBAT [6].

## Signal Processing

GNSS signals are transmitted in the form of radio waves with data modulated on them. Signal processing is an

integral part of demodulating the data on the carrier waves. We process GNSS signals using a Software Defined Radio (SDR). The GPS L1 signal is used in this work, but the method is generally applicable to all GNSS signals.

### GPS L1 Signal

The GPS L1 signal is transmitted at a frequency of  $f_L=1575.42$  MHz (19 cm wavelength) from all satellites in the form of radio waves that are modulated with pseudo-random (PRN) codes  $x(t)$  at the rate of 1.023 Mega-chips per second (300 m chip length) to distinguish between different satellites and then again modulated with Navigation Data  $D(t)$  at the rate of 50 bits per second. The modulation scheme used is Binary Phase Shift Keying (BPSK), where the 0s and 1s in a binary message are represented by two different phase states in the carrier signal.

### GPS Receiver Architecture

As shown in **Figure 1**, the GPS signal is received at a receiver's antenna with code delay  $\tau$ , Doppler  $f_D$ , and carrier phase  $\theta$ . The signal is then amplified, passed through a band pass filter, and then down converted to an intermediate frequency  $f_{IF}$  by mixing with a locally generated mixing signal. It is then passed through a low pass filter to remove the high frequency components. The advantage of converting the signal to an intermediate frequency is it simplifies the subsequent stages, making filters easy to design and tune. The signal is then digitized and mixed again (**Figure 2**) with two locally generated replicas of the carrier signal  $\bar{f}_D$ , in-phase and quadrature, differing in phase by a quarter cycle,  $\bar{\theta}$  and  $\bar{\theta}+\pi/2$ . It is then passed through a low pass filter to remove the intermediate frequency, and finally mixed with a local replica of the PRN code with delay  $\bar{\tau}$ .

### In-Phase and Quadrature Components

The in-phase  $I$  and quadrature  $Q$  components of an uncorrupted output signal (i.e., no spoofing or multipath) with amplitude  $\sqrt{C}$  are shown in **Equations 1 and 2**. When presented in complex form, as in **Equation 3**, the in-phase and

quadrature components are the real and imaginary parts of the signal, respectively. The coherent integration time  $T_{CO}$  can range from 1 to 20 milliseconds, the upper limit to avoid integration across boundaries of a GPS data bit  $D(t)$ . Coherent integration is performed to reduce the effects of thermal noise.

$$I(\sqrt{C}, \tau, \bar{\tau}, f_D, \bar{f}_D, \theta, \bar{\theta}) = \frac{\sqrt{C}}{T} \int^{\tau_{CO}} x(t - \tau)x(t - \bar{\tau}) \cos(2\pi(f_D - \bar{f}_D)t + \theta - \bar{\theta}) dt \quad (1)$$

$$Q(\sqrt{C}, \tau, \bar{\tau}, f_D, \bar{f}_D, \theta, \bar{\theta}) = \frac{\sqrt{C}}{T_{CO}} \int_0^{\tau_{CO}} x(t - \tau)x(t - \bar{\tau}) \sin(2\pi(f_D - \bar{f}_D)t + \theta - \bar{\theta}) dt \quad (2)$$

$$S = I + iQ \quad (3)$$

Performing the integrals in **Equations 1 and 2**, **Equation 3** can be expressed as

$$S(\sqrt{C}, \tau, \bar{\tau}, f_D, \bar{f}_D, \theta, \bar{\theta}) = \sqrt{C} R(\tau - \bar{\tau}) \text{sinc}(\pi(f_D - \bar{f}_D)T_{CO}) \exp(i\pi((f_D - \bar{f}_D)T_{CO} + \theta - \bar{\theta})) \quad (4)$$

where<sup>+</sup>

$$R(\xi) = \begin{cases} \frac{\xi}{T_c} + 1 & -T_c < \xi < 0 \\ -\frac{\xi}{T_c} + 1 & 0 < \xi < T_c \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

and  $T_c$  is the duration of a single chip.

To simplify the notation, we define  $a \triangleq \sqrt{C}$ . Summing  $N$  component signals ( $i=1, \dots, N$ ), we have

$$S_N(g|\bar{\tau}, \bar{f}_D, \bar{\theta}) = \sum_{j=1}^N a_j R(\tau_j - \bar{\tau}) \text{sinc}(\pi(f_{Dj} - \bar{f}_D)T_{CO}) \exp(i\pi((f_{Dj} - \bar{f}_D)T_{CO} + \theta_j - \bar{\theta})) \quad (6)$$

where  $g=(a_1, \tau_1, f_{D1}, \theta_1, \dots, a_N, \tau_N, f_{DN}, \theta_N)$ . For example, given the true satellite signal, a spoofed signal, and a single multipath signal,  $N=3$ .

Strictly, **Equation 5** is true only for infinite length random codes. Finite length PRN codes like GPS L1 C/A,  $R(\xi)$  will have additional small, but non-zero, values outside

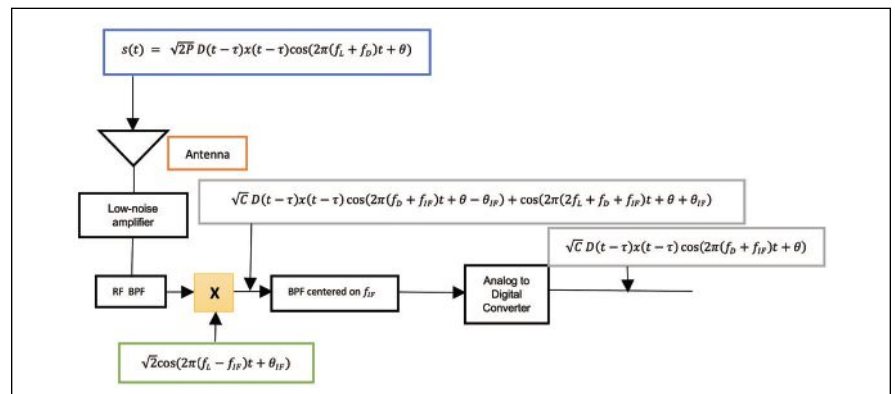


FIGURE 1 The front end of a GPS receiver.

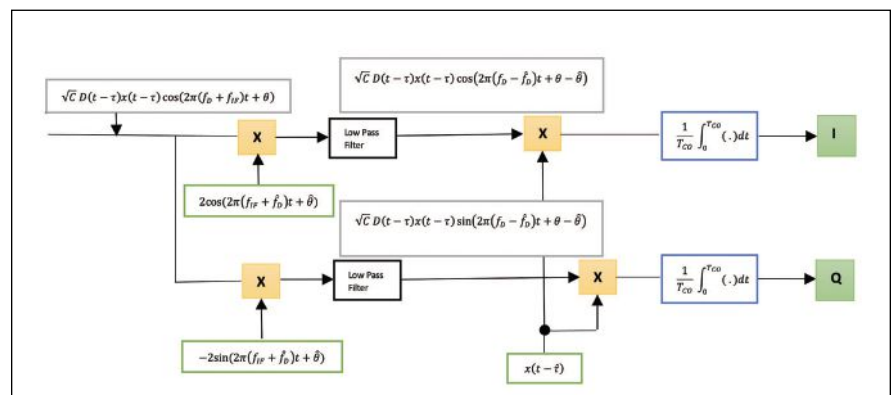


FIGURE 2 GPS receiver architecture after signal is digitized.

the domain  $\xi \in (-T_c, T_c)$ . We ignore these for now but will address their impacts later.

**CCAF Measurement Space**

A Doppler frequency ( $\bar{f}_D$ ) and code delay ( $\bar{\tau}$ ) pair search sweep is done to correlate the incoming signal from satellites with a local replica. The measurement space is spanned by a two-dimensional grid across Doppler frequency  $\bar{f}_D$  and code delay  $\bar{\tau}$ . The carrier phase is held constant across the grid at an arbitrary value (for example at 0 or the punctual value retrieved from the loop; the actual number used does not matter). Each measurement then corresponds to a complex value  $S_N(g|\bar{\tau}, \bar{f}_D)$ , which is the CCAF.

When spoofing and multipath are not present, the magnitude of CCAF (i.e., the CAF) is visualized in **Figure 3**. The total number of cells in the measurement space is equal to the number of code phase bins times the number of Doppler bins.

When visualizing the CAF from the Doppler frequency point-of-view, the peak is represented by a sinc function with frequency  $1/T_{CO}$ ; from the

code delay view it is a triangle with base length of 2 chips (**Figure 4**). The coherent integration time affects the resolution of the Doppler frequency. It is generally preferred to have longer  $T_{CO}$  for noise reduction reasons, but this will also require narrower Doppler bins because the sinc function itself becomes narrower. The software defined radio allows flexibility to change the Doppler bin widths. However, the code delay bins are determined by the sampling rate of the receiver.

**Spoofing**

When a spoofed signal is present and the code delays and Doppler frequencies of the signals are not closely aligned, two peaks are visible in the magnitude of the CCAF,  $\|S_2(g|\bar{\tau}, \bar{f}_D)\|$ , as shown in **Figure 5 (left)**. The two peaks merge if the code delays and Doppler frequencies are closely aligned, as shown in **Figure 5 (right)**. The proposed idea is to decompose the CCAF of mixed signals into their constitutive parameters.

**Particle Swarm Decomposition**

Stacking the measurements from the

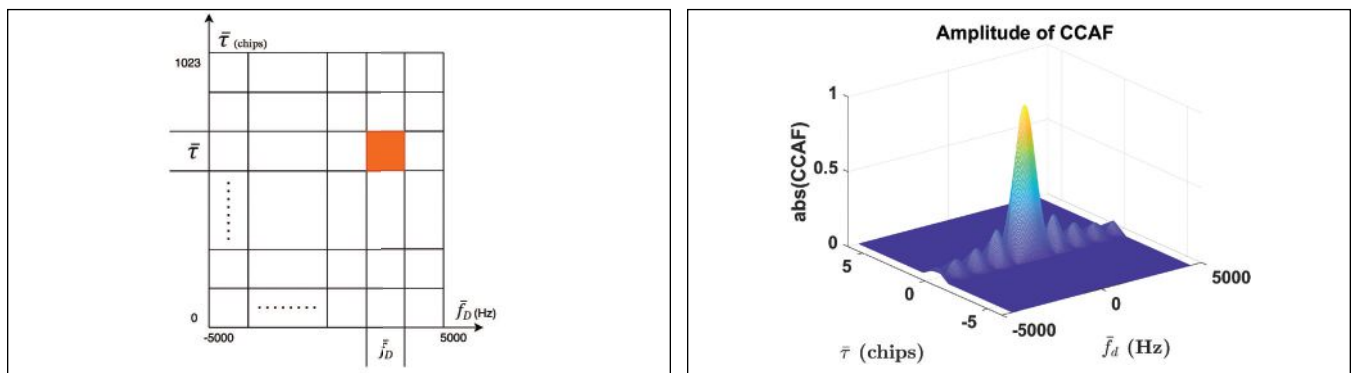
grid space  $(\bar{\tau}, \bar{f}_D)$ , the measurement model can be written as

$$z = S_N(g|\bar{\tau}, \bar{f}_D) + v \tag{7}$$

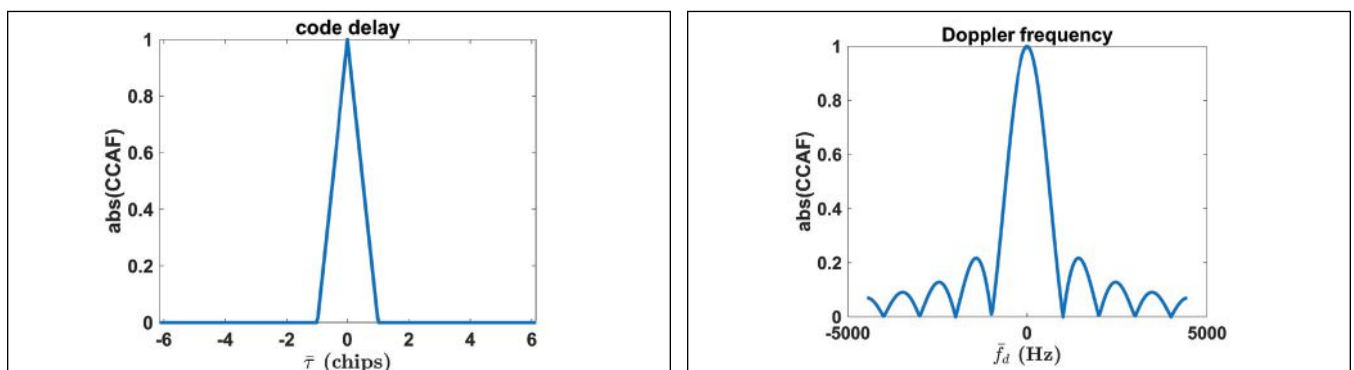
where  $v$  is the vector of measurement errors, including the effects of thermal noise and code cross-correlation. To decompose the N signals, we seek to obtain an estimate of the parameter vector,  $\hat{g}$ , that minimize the cost function.

$$J = \|z - S_N(\hat{g}|\bar{\tau}, \bar{f}_D)\|^2 \tag{8}$$

Unfortunately, due to the structure of  $S_N$  the cost function is non-convex, and a global minimum cannot be obtained by standard gradient-based methods. In computational science, Particle Swarm Optimization (PSO) is an optimization algorithm that works by generating a population of “particles” randomly that are actually candidate solutions given upper and lower bounds. These particles are moved around in the N dimensional space based on their own best-known position  $p_i$  and the entire population’s best-known position  $g$  as shown in **Equations 9 and 10**. When a particle finds a better position that minimizes the cost function better than the



**FIGURE 3** Complex Cross Ambiguity Function Search Space (left) and 3D search space with amplitude of CCAF (right).



**FIGURE 4** Code Delay (left) at 0 chips correlation peak and Doppler frequency (right) at 0 Hz represented by a sinc function.

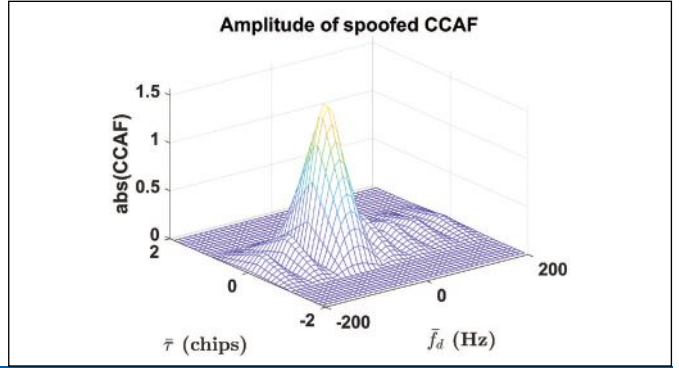
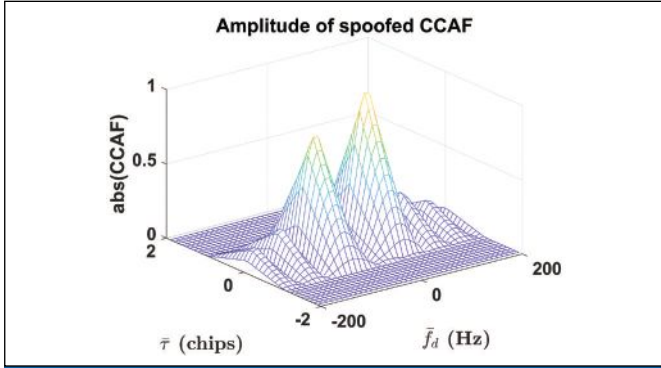


FIGURE 5 Amplitude of CCAFs when code delay and Doppler frequency pair are far apart (left). Amplitude of CCAFs when code delay and Doppler frequency pair are closely aligned (right).

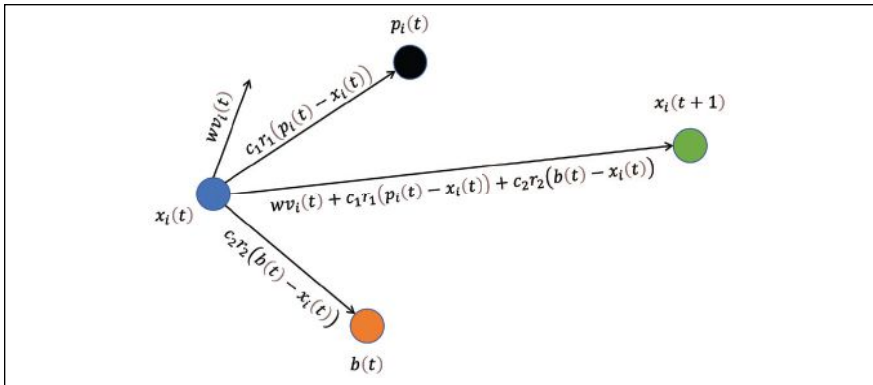
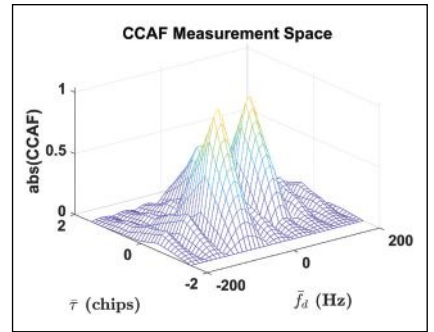


FIGURE 6 Search mechanism of the particle swarm algorithm as particle position updates based on hyperparameters.



CASE 1	True Parameters	Output Parameters
	$g$	$\hat{g}$
a1	1.0	1
$\tau_1$	-0.5	-0.5
$f_d1$	-60	-60
$\theta_1$	1.5707	1.5707
a2	0.5	0.5
$\tau_2$	0.8	0.8
$f_d2$	0	-1.85E-16
$\theta_2$	0.7853	0.7853
a3	0.9	0.9
$\tau_3$	0.1	0.1
$f_d3$	56	56
$\theta_3$	0	7.06E-17

CASE 1 A table showing the output parameters in comparison with the true parameters (bottom). The amplitude of CCAF is plotted against the code delay and Doppler frequency for visualization of three signals and how much further apart from each other they are in the search space (top).

previous known position,  $p_i$  gets updated based on Equation 11. If that particle's position is best among all other particle positions (minimizes the cost function)  $b$  is updated based on Equation 12 and called the best global solution of the swarm.

A simple PSO algorithm is shown here:

Generate  $n$  number of particles generated randomly with "position"  $x_i(t) \in X$  and "velocity":  $v_i(t) \in V$

For each  $i=1,2,\dots,n$  particle

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (9)$$

$$v_i(t+1) = w * v_i(t) + c_1 * r_1 * (p_i(t) - x_i(t)) + c_2 * r_2 * (b(t) - x_i(t)) \quad (10)$$

$$p_i(t+1) = \begin{cases} p_i(t) & f(p_i(t)) \leq f(x_i(t+1)) \\ x_i(t+1) & f(p_i(t)) > f(x_i(t+1)) \end{cases} \quad (11)$$

$$b(t+1) = \max\{f(p_i(t)), f(b(t))\} \quad (12)$$

where:

- $r_1, r_2$  are the uniformly distributed random number with  $N(\mu, \sigma^2)$
- $w$  is the inertia coefficient
- $c_1, c_2$  is the acceleration coefficient
- $p_i(t)$  is the best local position

$b(t)$  is the best global position

The PSO algorithm is applied to minimize the cost function  $J$  stated in Equation 8. The measurements  $z$  is in the form of CCAF, which is based on I and Qs and may be comprised of  $N$  signals, subtracts the CCAF( $\hat{g}$ ),  $S_N(\hat{g}|\bar{\tau}, \bar{f}_d)$  based on the best global solution of the PSO algorithm is the cost function in this work, where  $\hat{g}=(\hat{a}_1, \hat{\tau}_1, \hat{f}_{d1}, \hat{\theta}_1, \dots, \hat{a}_N, \hat{\tau}_N, \hat{f}_{dN}, \hat{\theta}_N)$  are the estimates of the signals' parameter.

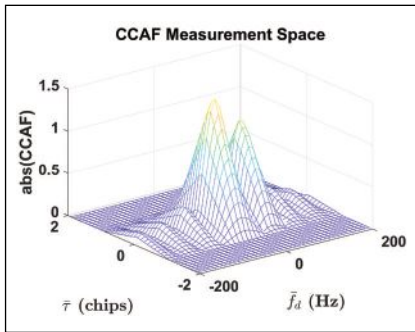
## Results

To evaluate the capability of the PSO algorithm in decomposing the multiple signals given the measurements, we decomposed the CCAF comprised of three signals, i.e., 12 parameters without any thermal noise and code cross correlation, and the results are:

## Simulated Results

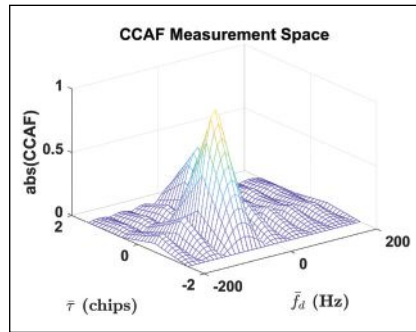
In Case 1, the CCAF is comprised of three signals in which the Doppler frequency and code delay pairs are closely aligned in the measurement space. The

Particle Swarm Algorithm estimates and output of the signals' parameters,  $\hat{g}$  are very close to the true parameters  $g$  as shown in Case 1 Table (bottom). For the purposes of visualization, CCAF magnitude is shown in Case 1 Figure (top)



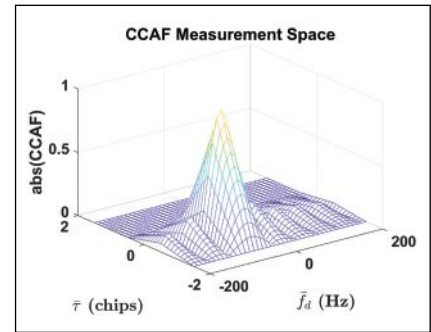
CASE 2	True Parameters	Output Parameters
	<b>g</b>	<b>ĝ</b>
a1	1.0	0.9906
τ1	-0.1	-0.1006
f <sub>d</sub> 1	-20	-19.9913
θ1	1.5707	1.5707
a2	0.5	0.5071
τ2	0	-0.0006
f <sub>d</sub> 2	-20	-20.0132
θ2	0.7853	0.7985
a3	0.9	0.8999
τ3	0.1	0.0999
f <sub>d</sub> 3	56	55.9966
θ3	0	0.0001

**CASE 2** A table showing the output parameters in comparison with the true parameters (bottom). The amplitude of CCAF is plotted against the code delay and Doppler frequency for visualization of three signals, where two of them are closely aligned while the third signal is far in the search space (top).



CASE 3	True Parameters	Output Parameters
	<b>g</b>	<b>ĝ</b>
a1	1	1
τ1	-0.5	-0.5
f <sub>d</sub> 1	-60	-60
θ1	1.5707	1.5707
a2	0.5	0.5
τ2	0.8	0.8
f <sub>d</sub> 2	0	5.20E-16
θ2	0.7853	0.7853
a3	0	0
τ3	0	-0.7064
f <sub>d</sub> 3	0	64.0637
θ3	0	-0.4483

**CASE 3** A table showing the output parameters in comparison with the true parameters (bottom). The amplitude of the CCAF is plotted against the code delay and Doppler frequency for visualization of two signals, where two of them are present in the search space (top).



CASE 4	True Parameters	Output Parameters
	<b>g</b>	<b>ĝ</b>
a1	1	1
τ1	-0.5	-0.5
f <sub>d</sub> 1	-60	-60
θ1	1.5707	1.5707
a2	0	0
τ2	0	-0.2137
f <sub>d</sub> 2	0	-16.1011
θ2	0	-0.2913
a3	0	0
τ3	0	-0.4034
f <sub>d</sub> 3	0	-5.8490
θ3	0	0.5963

**CASE 4** A table showing the output parameters in comparison with the true parameters (bottom). The amplitude of the CCAF is plotted against the code delay and Doppler frequency for visualization of one signal, one of them are present in the search space (top).

and all three signals can be identified by three distinct peaks.

In **Case 2**, three signals are used in which the Doppler frequency and code delay pairs for the two signals are tightly aligned and the third signal is relatively far away in the CCAF measurement space. The PSO algorithm decomposed the signals and output their respective parameters  $\hat{g}$  as shown in the **Case 2 Table (bottom)** and are visualized in the **Case 2 Figure (top)**. Note the two tightly aligned signals are merged and only one peak is identified when the CCAF magnitude is used.

In **Case 3**, the input CCAF is comprised of two signals while the PSO algorithm searches for the three sets of signal parameters. This case is generated to evaluate the behavior of the

algorithm in the scenario when there is only multipath signal present, and no spoofing. Because the algorithm is initialized in the same way as in **Cases 1 and 2**, the output is constrained to three signals. The third signal estimated by the algorithm has an amplitude of zero, implying the algorithm successfully identified there are only two signals present as shown in the **Case 3 Table (bottom)**.

In **Case 4**, the input CCAF is comprised of only one signal, while the PSO algorithm tries to minimize the cost function for a CCAF comprised of the three signals. As shown in the **Case 4 Table (bottom)**, two of the signals estimated by the algorithm have amplitudes of zero implying, again, the algorithm identified there is only

one signal present with its parameters as the output  $\hat{g}$ .

### Sensitivity Analysis

The PRN codes for the GPS L1 signal are transmitted at 1.023 Mega-chips per second (1,023 chips per millisecond) i.e., 1 code per millisecond, while the GNSS receiver usually has a faster sampling rate. The code is then distributed over the sampling rate of the receiver. To determine the precision of the algorithm, a sensitivity analysis is conducted next.

This analysis uses a 25 MHz sampling rate from the TEXBAT dataset. The samples per code is 25,000 and one chip contains 24 samples. The code delay search space consists of five chips with bin size of 0.0409

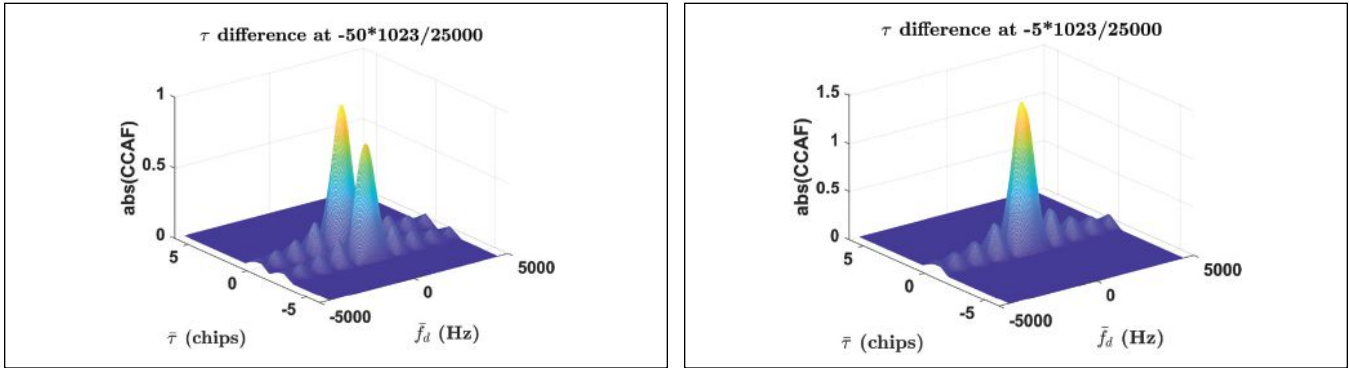


FIGURE 7 Amplitude of the CCAF when a difference in code delay of both signals is 2.046 (left). The amplitude of CCAF when the difference in code delay of both signals is 0.2046 (right).

and Doppler bin ranges from -4500 Hz to 4500 Hz with bin size of 20 Hz. In each case, the candidate solution population is 1,000 and each case runs 100 iterations. We take a search space mixed with two CAFs as the two signals are further apart in the code delay and two peaks are sufficient to visualize the amplitude of CCAF as shown in **Figure 7 (left)**. The CCAF with code delay at 0 chips is fixed and we change the second CCAF in code delay from -1.8414 to 0 with a step size of 0.2046. When the code delays for both signals are close in alignment, only one peak is detected (**Figure 7, right**).

The true parameters are shown in **Table 1**, while the output parameters' decomposition results for each code delay gap is shown in **Table 2**. Until the code delay for both signals merges, the Particle Swarm Algorithm decomposes each CCAF into its respective output parameters very precisely.

Decomposition of the CCAF into the signals' parameter vectors are shown in **Table 2**, as code delay gap between the two signals is reduced.

	True Parameters ( $g$ )
a1	1
$\tau_1$	0
$f_d 1$	0
$\theta_1$	1.5707
a2	0.8
$\tau_2$	-1.8414 to 0 with step size of 0.2046
$f_d 2$	0
$\theta_2$	0.7853

TABLE 1 True parameters ( $g$ ) for sensitivity analysis.

When both signals are perfectly aligned in the CCAF evaluation space, there may be only one signal detected; the amplitude of the signal depends on the carrier phase of the signal. Note that when the Doppler frequency and code delay pair for both signals are in perfect alignment, there is no spoofing as the navigation solution for a spoofed signal is the same as the true signal. However, as soon as the spoofer tries to pull the location of the receiver off the truth, both CCAF

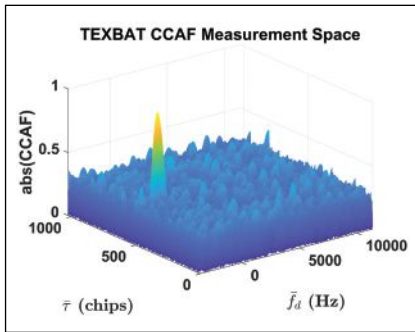
are decomposed into the respective signals. If the amplitude for both is significant, spoofing is detected.

### TEXBAT Dataset

We have shown the capability of the Particle Swarm Algorithm to decompose CCAF made of up to  $N$  contributing signals and output the parameters vector  $\hat{g}$  without any noise and code cross-correlation present. To test the algorithm in a real scenario, we have taken an instant in the TEXBAT dataset that includes thermal noise and cross correlations. The measurement space for PRN 13 consists of 1,023 chips that are distributed over 25,000 samples, i.e., code delay bins, with Doppler frequency ranging from -3650 Hz to 11350 Hz with bin size of 10 Hz, a total of 1,501 bins. This can be seen in the figure in **Case 5 (top)**, where two signal are present. The Particle Swarm algorithm searches for three signals, while the input CCAF has two prominent signals present. As shown in the **Case 5 Table**, the algorithm detects the signal parameters very near to the true parameters.

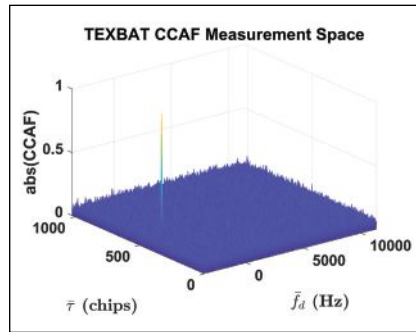
$\tau$ GAP	1.8414	1.6368	1.4322	1.2276	1.023	0.8184	0.6138	0.4092	0.2046	0
a1	1	1	1	1	1	1	1	1.0000	1.0122	1.4774
$\tau_1$	-1.31E-17	-2.71E-17	-2.30E-17	3.32E-17	-4.56E-18	-3.66E-17	-1.27E-16	2.17E-06	0.0015	-0.0002
$f_d 1$	6.67E-23	3.00E-17	-4.67E-22	2.63E-16	6.45E-23	-7.64E-16	1.50E-13	3.78E-05	0.0143	-10.8423
$\theta_1$	1.5707	1.5707	1.5707	1.5707	1.5707	1.5707	1.5707	1.5707	1.5659	1.2596
a2	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.7999	0.7881	0.1899
$\tau_2$	-1.8414	-1.6368	-1.4322	-1.2276	-1.023	-0.8184	-0.6138	-0.4092	-0.2061	-0.0017
$f_d 2$	-7.68E-16	-1.16E-15	-1.50E-17	-5.10E-16	-9.75E-16	-3.56E-16	-3.37E-13	-0.0001	0.0533	84.8491
$\theta_2$	0.7853	0.7853	0.7853	0.7853	0.7853	0.7853	0.7853	0.7853	0.7783	0.9467

TABLE 2 Output parameter vectors  $\hat{g}$  as the code delay gap between two signals changes left to right with a step size of 0.2046 chips.



CASE 5	True Parameters	Output Parameters
	$g$	$\hat{g}$
a1	1	0.9891
$\tau_1$	507.7690	507.7127
$f_{d1}$	-1649.2695	-1669.0176
$\theta_1$	0	-0.3230
a2	0.9560	0.9854
$\tau_2$	506.1740	506.1454
$f_{d2}$	-1649.2695	-1653.8006
$\theta_2$	-1.9123	-1.2370
a3	0	0.0000
$\tau_3$	0	505.5803
$f_{d3}$	0	-2407.6364
$\theta_3$	0	0.4319

**CASE 5** A table showing the output parameters in comparison with the true parameters (bottom). The amplitude of CCAF is plotted against the code delay and Doppler frequency for visualization of the signals present in the TEXBAT dataset (top) for 1 millisecond coherent integration time.




CASE 6	True Parameters	Output Parameters
	$g$	$\hat{g}$
a1	1	1.0452
$\tau_1$	506.133	506.2817
$f_{d1}$	-1659.2695	-1660.9876
$\theta_1$	0	0.1069
a2	0.9801	1.0213
$\tau_2$	507.7280	507.8261
$f_{d2}$	-1659.2695	-1663.4713
$\theta_2$	-1.1391	-1.5707
a3	0	0.0000
$\tau_3$	0	501.5564
$f_{d3}$	0	-1087.3015
$\theta_3$	0	0.2369

**CASE 6** A table showing the output parameters in comparison with the true parameters (bottom). The amplitude of the CCAF is plotted against the code delay and Doppler frequency for visualization of the signals present in the TEXBAT dataset (top) for 20 milliseconds coherent integration time.

### Spoofting Detection Monitor

Under normal circumstances, when spoofing is not present, the decomposed true signals will be geometrically consistent across all visible satellites but the decomposed multipath signals won't. However, if spoofed signals are introduced, they also will be consistent across satellites. In this case, two independent decomposed signal sets (true and spoofed) will both be geometrically consistent across satellites. Our proposed basis for the spoofing detection is then to use an 'inverse' Receiver Autonomous Integrity Monitoring (RAIM) mechanism, where the existence of more than one consistent decomposed signal triggers a spoofing alarm.

### Conclusion

In this article, we developed a method to decompose the CCAF into the  $N$  contributing signals by minimizing a cost function  $J$  and estimating the output parameter of vector  $\hat{g}$ . We have tested the algorithm in several challenging scenarios to determine its capability where the PSO algorithm searches for a greater number of signals than actually present in the CCAF measurement space. A sensitivity analysis has been performed on the characteristics of a GNSS receiver to demonstrate the capabilities of PSO in decomposing CCAF. We also demonstrated how PSO successfully decomposed the publicly available benchmarked spoofing dataset TEXBAT into two signals identifying their parameters. 

### Acknowledgment

This article is based on material presented in a technical paper at ION GNSS+ 2021, available at [ion.org/publications/order-publications.cfm](http://ion.org/publications/order-publications.cfm).

### References

(1) T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon und P. M. Kintner, "Assessing the Spoofing Threat : Development of a Portable GPS Civilian Spoofer," in Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah GA, 2008.

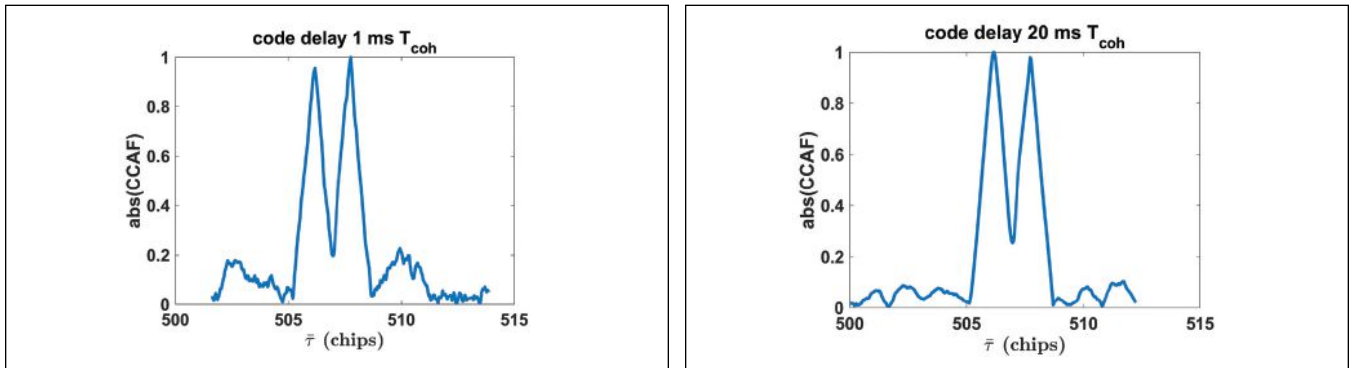
The two-signals detected by the algorithm are the authentic signal and the spoofing signal in the measurement space. The two signals are zoomed in and shown in **Figure 8**. The third signal that outputs by the PSD algorithm has zero amplitude, which represents there is no third signal present.

The noise floor as shown in **Case 5** includes thermal noise. Cross correlations can be reduced by increasing the coherent integration time. In **Case 6**, the coherent integration time is 20 milliseconds because for GPS L1 C/A signal, the Navigation Data bit is 20 milliseconds long. The other advantage of using longer coherent integration time is the preciseness in code delay and Doppler frequency estimates from

the Particle Swarm Decomposition Algorithm. The limit on coherent integration time can be disregarded if used in pilot signals.

The zoomed-in view of both **Case 5** and **Case 6** along a constant Doppler cut is shown in **Figure 8**. The noise floor in 20 milliseconds coherent integration time (**Figure 8, right**) is significantly lower than the 1 millisecond coherent integration time (**Figure 8, left**). Both results are normalized; one of the peaks represents an authentic signal and the other represents a spoofing signal. The peaks' magnitudes also change with respect to each other when the coherent integration time changes from 1 millisecond to 20 milliseconds.





**FIGURE 8** Constant Doppler Cut, zoomed-in view. Code delay shows two distinct peaks (authentic and spoofed signal) with 1 millisecond coherent integration time (left) and 20 millisecond coherent integration time (right).

- (2) M. Focreas, J. Leclère, C. Botteron, O. Julien, C. Macabiau, P.-A. Farine und B. Ekambi, "Study on the cross-correlation of GNSS signals and typical approximations," in *GPS Solutions*, Springer Verlag, 2017.
- (3) M. Pini, M. Fantino, A. Cavaleri, S. Ugazio und L. L. Presti, "Signal Quality Monitoring Applied to Spoofing Detection," in Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011), Portland OR, 2011.
- (4) E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter and P. Enge, "Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers," in Proceedings of the 2018 International Technical Meeting of The Institute of Navigation, Reston, Virginia, 2018.
- (5) T. Humphreys, J. Bhatti, D. Shepard und K. Wesson, "The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques," in Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012), Nashville, TN, 2012.
- (6) K. D. Wesson, D. P. Shepard, J. A. Bhatti und T. E. Humphreys, "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," in Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011), Portland, OR, 2011.
- (7) H. Christopher, B. O'Hanlon, A. Odeh, K. Shallberg und J. Flake, "Spoofing

Detection in GNSS Receivers through CrossAmbiguity Function Monitoring," in Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), Miami, Florida, 2019.

### Authors



**Sahil Ahmed** is currently a Ph.D. Candidate at the Navigation Laboratory in the Department of Mechanical and Aerospace Engineering, Illinois Institute of

Technology (IIT). He also works as a Pre-Doctoral Researcher at Argonne National Laboratory. His research interest includes spoofing detection in GNSS receivers, software-defined radios (SDR), satellite communication, statistical signal processing, estimation and tracking, sensor fusion for autonomous systems, sense and avoid algorithms for unmanned aerial vehicles (UAV), machine learning and deep learning algorithms.



**Dr. Samer Khanafseh** is currently a research associate professor at Illinois Institute of Technology (IIT), Chicago. He received his Ph.D. degrees in Aerospace

Engineering from IIT in 2008. Dr. Khanafseh has been involved in several aviation applications such as autonomous airborne refueling (AAR) of unmanned air vehicles, autonomous shipboard landing for the NUCAS and JPALS programs, and the Ground Based Augmentation System (GBAS). His research interests are focused on high accuracy and high integrity navigation algorithms, cycle ambiguity resolution, high integrity applications, fault monitoring, and

robust estimation techniques. He is an associate editor of *IEEE Transactions on Aerospace and Electronic Systems* and was the recipient of the 2011 Institute of Navigation Early Achievement Award for his outstanding contributions to the integrity of carrier phase navigation systems.



**Dr. Boris Pervan** is a Professor of Mechanical and Aerospace Engineering at IIT, where he conducts research on advanced navigation systems. Prior to joining

the faculty at IIT, he was a spacecraft mission analyst at Hughes Aircraft Company (now Boeing) and a postdoctoral research associate at Stanford University. Prof. Pervan received his B.S. from the University of Notre Dame, M.S. from the California Institute of Technology, and Ph.D. from Stanford University. He is an Associate Fellow of the AIAA, a Fellow of the Institute of Navigation (ION), and Editor-in-Chief of the ION journal *NAVIGATION*. He was the recipient of the IIT Sigma Xi Excellence in University Research Award (2011, 2002), Ralph Barnett Mechanical and Aerospace Dept. Outstanding Teaching Award (2009, 2002), Mechanical and Aerospace Dept. Excellence in Research Award (2007), University Excellence in Teaching Award (2005), *IEEE Aerospace and Electronic Systems Society* M. Barry Carlton Award (1999), RTCA William E. Jackson Award (1996), Guggenheim Fellowship (Caltech 1987), and Albert J. Zahm Prize in Aeronautics (Notre Dame 1986).

Consult conference websites periodically for changes.

See additional listings at  
[INSIDEGNSS.COM/CATEGORY/EVENTS/](http://INSIDEGNSS.COM/CATEGORY/EVENTS/)

## September 2022

**SEPTEMBER 17-18**  
**AFA NATIONAL CONVENTION**  
**National Harbor, MD**

[afa.org/events/national-convention?msclkid=fa40b497cd5b11ec8c2940afa219965f](http://afa.org/events/national-convention?msclkid=fa40b497cd5b11ec8c2940afa219965f)



Photo courtesy of G. Edward Johnson, CC BY 4.0, via Wikimedia Commons.

**SEPTEMBER 19-23**  
**ION GNSS+ 2022**  
**Denver, Colorado**

[ion.org/gnss/upload/GNSS22-Prospectus.pdf](http://ion.org/gnss/upload/GNSS22-Prospectus.pdf)

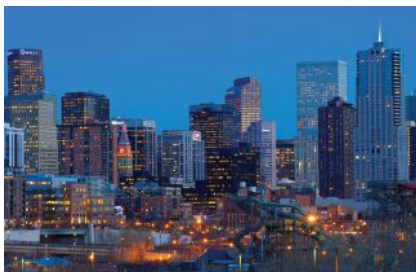


Photo courtesy of Larry Johnson <https://www.flickr.com/people/drljohnson/>, CC BY 2.0, via Wikimedia Commons.

## October 2022

**OCTOBER 10-12**  
**ASSOCIATION OF THE U.S. ARMY (AUSA)**  
**ANNUAL MEETING & CONVENTION**  
**Washington, D.C.**

[defenseadvancement.com/events/ausa/](http://defenseadvancement.com/events/ausa/)

**OCTOBER 18-20**  
**INTERGEO**  
**Essen, Germany**  
[intergeo.de](http://intergeo.de)

## January 2023

**JANUARY 5-8**  
**CES 2023**  
**Las Vegas, Nevada**  
[ces.tech/](http://ces.tech/)



Photo courtesy of Gb11111, CC BY-SA 4.0, via Wikimedia Commons.

**JANUARY 23-26**  
**ION INTERNATIONAL TECHNICAL MEETING**  
**Long Beach, California**  
[ion.org/itm/](http://ion.org/itm/)

## April 2023

**APRIL 24-27**  
**IEEE/ION PLANS**  
**Monterey, California**  
[ion.org/plans/](http://ion.org/plans/)



Photo courtesy of Carol M. Highsmith, Public domain, via Wikimedia Commons.

## May 2023

**MAY 23-25**  
**EUROPEAN NAVIGATION CONFERENCE**  
**Amsterdam, The Netherlands**  
[enc2023.eu](http://enc2023.eu)



Photo courtesy of Massimo Catarinella, CC BY-SA 3.0, via Wikimedia Commons.

## ADVERTISERS INDEX

Company	Page Number
Advanced Navigation	3
Applanix	55
CAST Navigation	2
GPS Networking	25
Ideal Aerosmith	23
ION	63
HITEC	35
Jackson Labs	9
KVH	27
M3 Systems	19
NavtechGPS	15, 41
NovAtel	76
NovAtel Navwar	17
Orolia	7
Physical Logic	33
Racelogic/LabSat	75
RX Networks	13
SBG	21
Silicon Sensing	37
Syntony	43
Tallysman	29
TeleOrbit	6
Topcon	5
VectorNav	11, 56

## June 2023

**JUNE 12-15**  
**JOINT NAVIGATION CONFERENCE**  
**San Diego, California**  
[ion.org/jnc/](http://ion.org/jnc/)



# Record Anywhere. Capture live-sky GNSS signals with LabSat

Lightweight, portable and affordable  
- your ideal test partner anywhere you  
need to Record raw GNSS RF data.



## Multi-Frequency

Record & Replay 3  
different frequency bands  
simultaneously



## Multi-Constellation

GPS, GLONASS, Galileo,  
BeiDou and NavIC



## Easy to Use

One touch Record and  
Replay with simple  
configuration



## Affordable Range

Options to suit any  
budget - starting from  
\$5,495

**RECORD / REPLAY / SIMULATE**

**labsat.co.uk**



**WE'RE HIRING**

# How does “doing cool stuff that matters” sound for a job description?

Autonomy is shaping the world, so join the leader shaping autonomy.

Hexagon is a global leader in digital reality solutions, combining sensor, software and autonomous technologies. We are putting data to work to boost efficiency, productivity, quality and safety across industrial, manufacturing, infrastructure, public sector, and mobility applications. You'll be joining a diverse workforce of over 23,000 people in 50 countries on the leading edge of your field. In short, you'll be working on some very cool stuff in areas of immense importance, so what you do is going to matter. A lot. If you want to make a difference, Hexagon is the place for you.

Do cool stuff that matters | [hexagonpositioning.com/careers](https://hexagonpositioning.com/careers)

