DOI 10.5162/ETTC2024/A3.2

Detection and Monitoring of Jamming and Spoofing of GPS/GNSS Signals in Harbours and Industrial Areas

Karen von Hünerbein[1]
[1] *Lange-Electronic GmbH, Rudolf-Diesel-Str. 29A, 82216 Gernlinden, Germany*
kvh@lange-electronic.com

Abstract:
GPS/GNSS plays a key role for navigation in autonomous vehicles.

For industrial areas and harbour terminals there is a need to use autonomous or remotely controlled vehicles, for more efficient and safe operation and transport among containers and assets.

Such industrial and harbour areas can be complex and confusing for untrained personell and external lorry drivers, who are usually unfamiliar with the structure and floor plan of container stacks, walls of boxed materials and building compounds. These container stacks and other structures reduce overall visibility for a human operator, making visual navigation more difficult. When drivers are confused they take a long time and use more fuel before arriving at the intended location for loading and unloading of bulk goods. Autonomous vehicles can be pre-programmed with a safe and efficient trajectory.

In order to navigate properly in any terrain, autonomous vehicles require a redundant navigation system, usually consisting of GNSS (Global Navigation Satellite Systems) and INS (Inertial Navigation System) and additional sensors. One disadvantage is that the GPS / GNSS environment can be and will be degraded in a complex area with a lot of metal structures and possibly jamming signals. Thus it is important to check and monitor the quality of the signal environment for smooth continuous operation of all vehicles on the ground. In this paper, we present a novel Interference Detection and Monitoring System, GIDAS, by OHB-Digital, capable of detecting and monitoring GPS/GNSS signal jamming and spoofing, 24/7 and capable of analysing and classifying the interferer types. In addition GIDAS will store snapshots of the interference signals and alert the operator of the harbour / industrial area. GIDAS allows localization of the interference source and detailed analysis in post-processing..

Key words: GPS/GNSS interference monitoring, increased efficiency, autonomous vehicles

Introduction

Harbour areas are equipped with many large metallic structures, among which vehicles, such as lorries need to find their way and arrive at predefined locations, e.g. loading areas and docks. Metallic structures include cranes and containers, some of them form a complex and variable topography and obstruct visual line of sight, making it hard for drivers to find their destination.

In order to increase efficiency of transport inside such areas, it is easier and safer to use remotely piloted or autonomous robots and vehicles for moving and transportation among the complex metallic structures and topography of an industrial area and harbour.

Most vehicles with and without drivers use GPS/GNSS satellite navigation signals for localization and navigation. These signals are very weak (at -120dBm to -130 dBm) and can be obscured and reflected from metal surfaces, which are present abundantly in harbours and industrial areas. Reflections, especially when there are a lot of them, can cause issues for a GPS/GNSS receiver, because it needs to identify the correct navigation signal for calculation of an accurate and precise position. If the receiver uses a reflected navigation signal (multipath), which is attenuated and has a different path length compared to the line of sight signal, this may result in a less accurate postion fix. In a multipath rich signal environment it can also become difficult for a receiver to acquire and process any useful signal at all.

In addition these weak satellite navigation signals can be easily interfered with by other RF signals as unintentional interference, or by intentional jamming signals. Such interference and jamming events have been observed frequently in the last 10 years. [5], [6]

In a study by Fraunhofer CML and Fraunhofer IML it has been shown that in a harbour environment efficiency and sustainability can be improved by using automated and remotely controlled vehicles. [1,2].

In this paper we would like to present how efficiency can be increased by use of automated vehicles in harbours and by monitoring the signal environment to detect and analyze jamming and spoofing signals detrimental to GPS/GNSS signal reception.

Automated Vehicles in Harbour Areas

Harbours and container terminals are full of high metallic structures and machines such as cranes and stacks of containers, which reflect and obscure GPS/GNSS satellite system signals and obstruct vision and driving routes for human drivers. Reduced visibility and complex arrangement make it harder for any lorry driver to spot and drive to the appropriate loading/unloading and other destinations inside a harbour area and inside many industrial areas.

In 2022, Fraunhofer Institute Center of Maritime Logistics (Fraunhofer CML) and Fraunhofer Institute for Material Flow and Logistics (Fraunhofer IML) have conducted a simulation study, in order to assess the potential for efficiency gains in container terminals when operating automated vehicles and lorries instead of lorries with human drivers. [1,2]

The project is called SALT: Simulation automatisierter LKW in Häfen und Terminals, meaning **S**imulation of **A**utomated **L**orries in harbours and **T**erminals. This study was conducted in a reference container terminal and the surrounding access roads and streets. [1,2]

In the simulation, input data were real data of traffic flow and data of control signals for the traffic lights by the Hamburg Port Authority. In addition, all relevant operational processes for lorry handling inside the harbour were included in the simulation and analysis, including OCR2-Gate, interchange, different container storage areas, and customs offices. Traffic routes and lorry trajectories were implemented in the statistical model, plus additional vehicles and all sorts of other traffic inside the terminal. Data and logic of the simulation model were validated by expert interviews. Fraunhofer CML researchers set up and ran different simulation scenarios with various conditions, e.g. different levels of automation, and various amounts of automated vehicles in relation to non-automated vehicles, because mixed traffic is occurring especially on the access roads.

Fraunhofer researchers calculated and evaluated parameters such as throughput times, traveling times and length of traffic jams, in order to analyze efficiency gains.

Results showed that no efficiency gains could be achieved on the surrounding access roads, due to crossings, merging of lanes, traffic lights and lane changes in mixed traffic. Good gains of average throughput time could be achieved on the area of the container terminal with automated vehicles of SAE levels (Safety Levels) 4 and 5: 15% improvement of throughput time in mixed traffic and even 29% of throughput time with fully automated traffic. This is due to faster shunting maneuvers and removal of manual processes.[1,2]

Positioning of Autonomous Vehicles

Autonomous and automated vehicles are generally equipped with a variety of multiple sensors and postioning technologies in order to ensure a high degree of safety and security while driving on roads, industrial areas or inside container terminals.[3,4,16,17]

At higher levels ”of autonomy, we see more and more sensors built into vehicles. Radar, LIDAR, vision and ultrasonic sensors are all in the mix, offering relative positioning capability. In other words, they can tell us how far away other objects are from the vehicle, and, by sensing the distance from landmarks, they can also be used to position it relative to the reference frame defined by these landmarks. For some use cases, however, a truly absolute positioning sensor is needed, and this is where GNSS or, more typically, GNSS fused with inertial sensors comes into the picture “ [4]

Using a a combination of sensors provides redundancy for safety, robustness for use cases and an optimized cost balance.[11,16]

GPS/GNSS Reception

A resonable or good GPS/GNSS reception with 8-12 satellites in view is a key element of the positioning in autonomous vehicles. While GPS/GNSS signal reception is generally good at sea or in rural areas, it can be degraded or severely restricted in mountainous areas, urban canyons or harbour areas, where there are a lot of high structures such as cranes and stacks of containers. The main issue in these areas is obscuration, since the high structures block GPS/GNSS signals from satellites, much like steel and rock structures blocking the direct sunlight.

In addition, certain materials reflect the GPS/GNSS electromagnetic waves and lead to

signal distortions or inaccuracy of the PNT solution (PNT: position, navigation and timing) in the receiver. GPS/GNSS signals can also be affected and drowned out by electromagnetic interference and spoofing.

“In recent years, there have been increasing concerns about intentional and unintentional interference with GPS signals [9]. GPS signals are weak at around -130 dBm, so weak that they disappear in the normal thermal back-ground noise, and can be easily disrupted. “ [9]

*“*A jammer produces stronger RF signals in the same RF band, and simply overwhelms the GPS receiver by sheer noise. When a receiver is disrupted by a jammer, it is clear to the receiver and to the user that there is a signal problem. Spoofing on the other hand is a hidden attack misleading the receiver with erroneous information, to make it believe it has different position, velocity or time than it actually has. In this case it is not clear to the receiver and the user, that there is a signal problem. Spoofing has not been observed so far in the civil world, but it has been demonstrated to work in demonstration field test” [9,11]. In the last two years, spoofing has been observed in civil life, with passenger jets being affected. [21]

Interference of GPS and GNSS Signals

One way of dealing with degraded signal environments is by monitoring the GPS / GNSS signals at the location of interest. Such monitoring measurements have already been performed in several studies around Europe.

One of them was the STRIKE3 Project: STRIKE3 was a”European initiative to support the increasing use of GNSS within safety, security, governmental and regulated applications. The aim of STRIKE3 was to develop international standards in the area of GNSS threat reporting and GNSS receiver testing.[12] Using thousands of threats collected from their network over a three-year period, STRIKE3 has developed a baseline set of threats that can be used to assess performance of different GNSS receivers under a range of typical real-world interference/ jamming threats” such as: wide swept frequency with fast repeat rate, narrow band signal at L1 carrier frequency, triangular and triangular wave swept frequency and tick swept frequency.” [12].

A recent paper in Inside GNSS reports about interferences observed in the Baltic Sea: “Automatic Dependent Surveillance (ADS)-B messages broadcast by aircraft are an important source of information regarding the timing and effects of GNSS RFI, and this information is now readily available online (e.g., at GPSJam, managed by John Wiseman [15], which uses data from ADS-B Exchange” [14]. The GPSJam Website is showing plenty of GPS interference around the Baltic Sea from December 2023 to February 2024, which is believed to be emitted and caused by Russian military.

In a study from 2016 conducted together with the institute of flight guidance (IFF) of the technical university of Braunschweig, we observed 238 interference events on a nearby motorway A2 within two weeks, and 34 of them with a high signal strength and severity. [6].

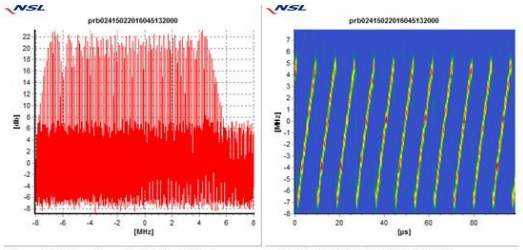

Figure 6: Chirped saw tooth (up) interference event (Feb. 15 2016, 04:51:32 UTC)

Fig. 1. Chirp Saw Tooth Up Interference in 2016

Interference Detection and Monitoring

To address these challenges, there have been several systems developed to detect, classify and store interference events.

One of the was the DETECTOR system by Nottingham Scientific laboratory NSL described in our paper from 2016 [6].

Another one has been developed by Fraunhofer IIS in Germany in 2017 [20]. Fraunhofer IIS developed a configurable and customizable GNSS interference detection station. With up to three GNSS bands with a bandwidth of up to 80 MHz and a resolution of up to 8 bit can be continuously analyzed.” [20]

The interference monitoring system, which we would like to present in this paper is the GIDAS System: GNSS Interference Detection and Analysis System by OHB Digital in Austria [7]. This system is based on a set of algorithms and has been implemented in three different versions:

- as a stationary system, which can be useful for permanent monitoring in industrial areas and harbours, or other critical infrastructure
- as a portable system in a suitcase for field testing in various locations
- as an embedded system, where the software detector algorithms are

integrated into GPS/GNSS receivers or other electronic systems.

The algorithms use a set of different detector parameters, which are combined and weighted to allow a secure and clear detection of both spoofing and jamming. [7]

The detector parameters are:

1. Power Spectral Density Detector
2. Received Power Detector
3. Carrier to Noise Ratio
4. Correlation Peak Detector
5. Clock Detector
6. Position solution
7. Number of tracked satellites

“The **power spectral density** (PSD) of the signal describes the power present in the signal as a function of frequency, per unit frequency.” [18]. In GIDAS, it is possible to define different thresholds to optimize the interference detection to the jamming types relevant to the use, e.g. narrowband thresholds, wide-band thresholds or the ICAO mask (for civil aviation), see figures 3 and 4 for an example. [7]

The **received power detector** measures the absolute received signal power within the monitored frequency band. In case of interference, the received power is usually significantly stronger and thus overwhelms the GPS/GNSS receiver frontend.

Carrier to noise ratio (C/No), is the signal to noise ratio. In case of interference, a strong drop of the carrier to noise ratio is observed, while in case of spoofing there usually is an increase in C/No, because the fake signals add to the signal strength of the original GPS/GNSS signals. Also the spoofer can try to take over the receiver tracking loops by transmitting the fake signals with a slightly increased signal strength.

The combination of these three parameters PSD, C/No and overall received power are used to detect interference in GIDAS. The combination of different parameters is considered advantageous for a low false alarm rate [7]. When the interference is strong there will also be a failure of the receiver to fix a position solution. This results in a denial of GPS/GNSS service. Sometimes the receiver carries on providing position outputs to the user, however, in the presence of medium strength interference, these position fixes can become inaccurate and unreliable.

“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 nonperfect spoofer as well as victim receiver position estimation)” [7]

Correlation Peak Detector: In case of spoofing there are two correlation peaks for each satellite signal: the true signals are still present and in addition there is a fake spoofing signal for each satellite. Thus a determination of the amount of correlation peaks for each satellite is a good indication of the presence of a Spoofer.

In summary a weighted combination of clock detector, correlation peak detector and carrier to noise ratio is used to detect spoofing.

The number of tracked satellites shows whether the GPS/GNSS receiver has enough satellites in view to be able to calculate a PNT solution: position, navigation and timing. A GPS receiver needs at least four satellites to do so. If the number of tracked satellites is low, there can be various reasons. Lack of sufficient amount of satellites can be caused by interference, or it can also be caused by high structures obscuring satellite view.

Lack of sufficient number of satellites is thus a reason for alert and countermeasures, even if no spoofing or jamming is detected. [7]

Overall Functionality of the GIDAS System

The GIDAS system uses the above mentioned detector algorithms and provides a real-time 24/7 monitoring of jamming and spoofing signals for all GNSS systems on L1, and for GPS on L1,L2,L5, Galileo E1 and E5, GLONASS L1 and L2 with a maximum bandwidth of 81 MHz. The events are classified and saved for later analysis. They are also listed in the GUI and stored in a database with time of occurrence and duration. The direction of arrival of the interference systems can be determined, with an antenna with two or more antenna elements. The GIDAS system is hardware agnostic, thus different antennas can be attached. Users are alerted via E-Mail or via a custom alert interface. Information can be viewed remotely via a webbased graphical user interface. The graphical user interface displays

a map and detailed information about the interference events, all detector parameters are displayed. “Since GIDAS automatically captures and stores raw baseband signal snapshots for every interference event, it is even possible to gather more detailed insights on the jamming signals by post processing analyses.” [5]

Longterm results of a fully operational stationary GIDAS system with several monitoring stations at 3 locations around an airport are described in a whitepaper from 2023: “Since May 2022 we operate a permanent GIDAS installation at a European airport, together with the local air navigation service provider. The goal of the commonly operated GNSS quality assurance system is to gather data-based evidence for future decision-making and strategy definition on how to handle GNSS interference, inflicting air traffic surrounding the airport premises. The first eight months of operation show, that especially along motorways and construction sites, the quantity of interference signals in the restricted GNSS bands is even higher than expected. Between the 17th of May 2022 and the 18th of January 2023 (246 days of operation), the system detected 630 interference events with a severity classified as an alarm (which means that there was an actual degradation of the GNSS

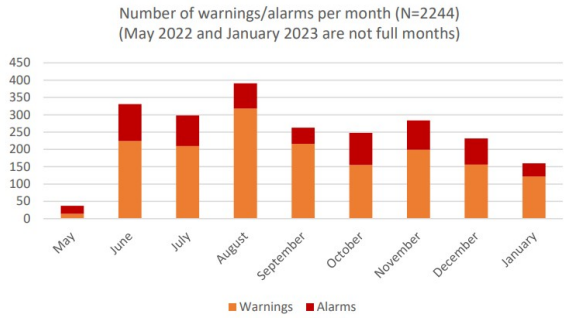

Fig. 2. Number of warnings alarms per month

measurement quality). During this period an additional number of 1614 interference events with a severity classified as a warning has been captured.” [5]

In their results they found that interference events occur on a daily basis, especially along motor ways and that a significant amount of such events correlate with daily rush hours and working hours.

“The highest number of interference alarms and warnings has been recorded at” at two monitoring sensors, “both close to either a motorway or a busy country road. In total, a number of 98 interference events have been critical enough to be recorded at least at two sites in parallel.” [5]

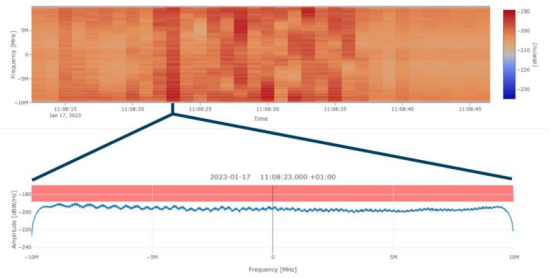

Fig. 3. A typical recorded interference event on the L1 frequency. [5]

Results from Interference Monitoring in a Harbour

In 2021 the GIDAS system was installed in the port of Tallin, and operated for 2 years. Within 11 days in November 2021 the GIDAS system recorded 1231 interference events in the L1/E1 band, 51 of them were strong enough to cause an alarm, this means interference with a high probability of negatively impacting GPS/GNSS receivers. Some events lasted several minutes, the longest one approximately 13 hours. The GIDAS installation in Tallin recorded a total of distinct 5 interference events, classified as GNSS jamming events. The most significant event started at 2021-11-21 14:39 UTC+1 and lasted for an approximate duration of 13 hours. [19]

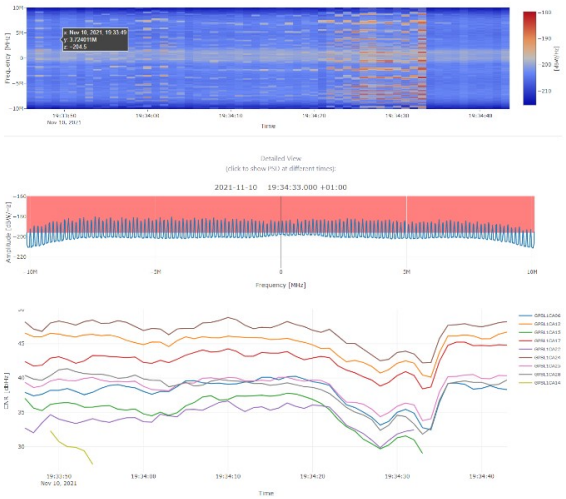

Fig. 4. Jamming event at port of Tallin 10th, Nov, 2021 [19]

The jamming event in figure 4 lasted for 3 min with an alarm duration of 45 sec.The red area in the PSD of figure 4 (plot in the middle) shows the power above the alert threshold. The satellite signals’ C/No clearly drops to much lower levels in the bottom part of figure 4, with tracking loss of 2 satellites. The top plot shows a waterfall diagram with power levels: x-axis

Time, y-axis frequency (MHz), powerlevel: color code (dBW/Hz).

Effects of Monitoring

Even though monitoring does not eliminate unintentional interference, jamming or spoofing, it increases situational awareness and provides alerts. Alerted operators can pass this information on to their automated vehicles and allow them to switch over to other sensors, such as inertial sensors and to disregard the GPS/GNSS information for a certain period of time. In addition operators can decide to stop the automated vehicles and freeze their position, while the GPS/GNSS outage lasts, which can help to prevent accidents, due to false PNT solutions and thus save loss of material and damage. Other countermeasures can be a hand over to remote control steering of the automated vehicle. Since GIDAS also allows to localize interference sources, it is possible to search for them and to remove the interference transmitters. This contributes to overall smoothness of operation and thus better sustainability.

Conclusions:

Reduction of throughput time of lorries in harbour container terminals by operation of automated vehicles will lead to an improvement in efficiency thus contributing to sustainability.

In recent years more and more interference events have been observed in Europe and other areas of the world. We have presented the GNSS monitoring system GIDAS, capable of analyzing and classifying interference events, and issueing alerts in case of such events. The GIDAS system was installed at an airport and at the harbour of Tallin and in both locations a high amount of jamming and interference has been observed. Monitoring the GNSS signal environment ensures enhanced awareness of GPS/GNSS availablity or blackouts and thus allows to optimize the operation of autonomous and automated vehicles, which in turn leads to a more efficient and sustainable operation.

Acknowledgements

I am grateful for the support and data from Sina Willrodt, Fraunhofer CML, and the support and unpublished data from Sascha Bartl, from OHB-Digital and would like to thank them for their support and cooperation.

References

[1] S. Willroth, I. Völkel; Einsatz automatisierter LKW in Häfen und Terminals; Schiff und Hafen, March 2022, S.54-55.

[2] S. Willrodt, P. Zimmermann. Simulationsbasierte Analyse Automatisierter Verkehrsflüsse In Häfen und Terminals. 2022. Fraunhofer-Allianz Verkehr Newsletter.

[3] O Julien, R Bryant, C Hide, I Sheret. Tight Position Bounding for Automotive Integrity. Inside GNSS May/June 2021: 34-41.

[4] S. Igarashi et al. Autonomous Driving Control of a Robotic Mower on Slopes Using a Low-Cost Two-Frequency GNSS Compass and an IMU, January 2022. Journal of the ASABE 65(6):1179-1189, DOI: 10.13031/ja.15032

[5] M. Kadletz. Jamming and Spoofing of Safety Critical Infrastructure. January 2023. Whitepaper by OHB-Digital

[6] M. Stanisak, K. Hünerbein K, U. Bestmann, W. Lange, (2016) “Measured GNSS Jamming Events at German Motorways”, Proc. of POSNAV ITS, DGON Conference, Berlin, Germany, 5th-6th July, 2016.

[7] S. Bartl, M. Kadletz et al. (2022) Mitigating the Threat of Jamming and Spoofing to Aeronautics. Inside GNSS Sep/Oct 2022, vol. 17, no. 5: 46-55.

[8] P. Gutierrez, (2014) A GNSS Wake Up Call for Europe; Apr 2014, European Navigation Conference in Rotterdam, Netherlands

[9] K. Hünerbein, W. Lange, A New Solution of Generation of Spoofing Signals for GNSS Receivers. DGON Conference CERGAL 8th-9th July 2014, in Dresden. International Symposium on the Certification of GNSS Systems and Services.

[10] M. Jones, “The Civilian Battlefield”, Inside GNSS, March/April 2011, vol. 6, no. 2, pp. 40-49

[11] M. Baus. Safe GNSS/Inertial Positioning for Highly Automated Driving. Presentation. 2018 Munich satellite Navigation Summit in Munich, 2018

[12] M Creadie, M. Pattinson, M Dumville, Standardisation Of GNSS Threat Reporting And Receiver Testing Through International Knowledge Exchange,Experimentation And Exploitationstrike3, Final Report. 2019.

[13] M. Petovello, How can we ensure GNSS receivers are robust to real-world interference threats? Inside GNSS Jul/Aug 2018, Vol 13 No 4: 33-37.

[14] Z. Liu, S Lo et al. Solutions: What do we know about recent observations of GNSS Interference and Spoofing in Eastern Europe?… Inside GNSS March April 2024 Vol19, No2: 28-35

[15] J. Wiseman; GPSJam: Daily Maps of GPS Interference, https://gpsjam.org

[16] SA Negru, P Geragersian, I Petrunin, W Guo. (2024). Resilient Multi-Sensor UAV Navigation with a Hybrid Federated Fusion Architecture. Sensors, 24(3).https://doi.org/10.3390/s24030981

[17] Ruwisch F., Schön S. (2022): GNSS Feature Map: Representation of Signal Propagation-related Features in Urban Trenches, Proceedings of the 2022 International Technical Meeting of The Institute of Navigation, Long Beach, California, January 2022, pp. 701-711. DOI: 10.33012/2022.18171

[18] https://en.wikipedia.org/wiki/Spectral_density#Power_spectral_density

[19] Sascha Bartl, OHB Digital (2024) personal communication.

[20] A Rügamer et al (2017) Versatile and Configurable GNSS Interference Detection and Characterization Station; Proceedings of the ION Pacific PNT 2017 Conference, ION PNT 2017, Honolulu, Hawaii, May 1-4, 2017

[21] S Schweitzer (2024) Jamming of a Parked Passenger Jet: Sensitivity of the aircraft to Jamming with Varying Power. European Navigation Conference in Nordwijk, NL, May 22-24, 2024