On GNSS Jamming Threat from the Maritime Navigation Perspective

Daniel Medina*†, Christoph Lass*, Emilio Pérez Marcos*, Ralf Ziebold*, Pau Closas‡, Jesús García†
*Institute of Communications and Navigation, German Aerospace Center (DLR), Germany
†Computer Science and Engineering Department, Universidad Carlos III de Madrid, Madrid, Spain
‡Dept. of Electrical & Computer Engineering, Northeastern University, Boston MA, USA

***Abstract*—Global Navigation Satellite Systems (GNSS) play a fundamental part on the maritime navigation. Beyond positioning, GNSS is key for the operation of multiple interfaces on the bridge of a ship, compromising the skipper skills to perform traditional navigation. Jamming attacks have been recognized as a major vulnerability for GNSS and their proliferation have raised concerns, given the implication of GNSS into several safety-critical applications. This work provides an overview on the jamming threat and the main countermeasures techniques, especially in the fields of robust signal processing, adaptive antenna arrays and multi sensor fusion. Moreover, the effects of a Personal Privacy Device (PPD) on positioning based on conventional methods using GPS L1 is addressed. The experimentation is conducted on the Baltic Sea, where a civilian maritime jamming testbed was allocated, as result of the cooperation of DLR with the German Federal Network Agency.**

***Index Terms*—GNSS, Jamming, Maritime Navigation, Jamming Countermeasures.**

I. Introduction

Global Navigation Satellite Systems (GNSS) have established as the cornerstone for the provision of Positioning, Navigation and Timing (PNT) data. Prospective applications of intelligent transportation systems, namely driverless cars, autonomous shipping or automated landing are reliant on absolute and accurate GNSS based positioning. Besides, there is an evergrowing dependency on this technology for timing purposes. Critical services, including communications, power grid distribution, finance or emergency response have highlighted the important role of satellite technology for precise timing [1]. Despite providing accurate global positioning and timing estimates, GNSS performance can be easily disturbed due to a wide variety of factors, among them natural phenomena (e.g., ionospheric storms) or signal reflection (e.g., multipath and non line of sight). More importantly, GNSS is prone to unintended and malicious radiofrequency interference (RFI) due to the extremely low power of the signals upon their reception on the earth [2].

The proliferation of radio threats to GNSS signals has raised serious concerns on the vulnerability of the navigation process [3], [4]. In consequence, in 2001 the risks of GPS disruption were assessed for the U.S. transportation infrastructure [5] and, more recently, it was declared as a major vulnerability of cyber physical systems [6]. Intentional attacks to GNSS signals have been traditionally divided into jamming and spoofing. Jamming is the act of intentionally directing powerful electromagnetic waves toward a victim receiver with the goal of denying its positioning [7]. Spoofing consists of the transmission of counterfeit GNSS-like signals, with the intent to produce a false position within the victim's receiver without disrupting GNSS operations [8]–[10].

Although selling and using jamming devices is forbidden in several countries, among them the United States and many European countries, the acquisition and ownership of a jammer might not be illegal. Indeed, the access to jammers is uncomplicated via several webpages, even at a very low cost [11]. In [12], [13] a detailed characterization of in-car jammers is analyzed and categories based on the jammer signal characteristics are defined as well. There are two distinct motivations for the use of jamming devices: attacking other GNSS users to deprive them from navigation guidance, and protection of one's privacy. While the first is more concerning, given the malicious intentionality, the second reason is the most frequent source of jamming. Personal Privacy Devices (PPDs) refer to the jamming devices whose aim is to prevent people and vehicles from being tracked [14], [15].

In the marine case, the use of PPDs is tightly related to the service denial of Automatic Identification System (AIS). Introduced by the International Maritime Organization (IMO) in 2004, AIS allows for the exchange of dynamic, static and voyage related data among vessels via VHF broadcasting channels [16] and its use is mandatory for all passenger ships and voyaging ships with 300 or more gross tonnage [17]. Originally intended for improved situation awareness, AIS has been adopted in a variety of security applications, such as cargo tracking and fishing fleet monitoring. Thus, the use of PPDs is generally associated with illegal fishery [18]–[20], as it might deprive the detection of such actions via AIS tracking. Similarly, AIS blockage was realized to cloak oil exports from Iranian tankers [21]. Besides, GNSS jamming in maritime spaces has been frequently endorsed for military actions [22]–[24], making evident the need to understand and countermeasure this radio threat.

While the impact of radio threats has been widely studied for automotive [25]–[27] and aviation applications [28], [29], only a few authors have addressed the effects on the maritime scenario. Besides the need for accurate navigation, GNSS plays a fundamental role on the nominal working of a vessel, since a large number of systems and functionalities onboard a vessel, such as the Electronic Chart Display and Information

System (ECDIS), the AIS, and the Automatic Track Control, just to name a few, are strongly dependent on the provision of accurate PNT information.

In [30] and [31], an international measurement campaign studying RFI in the L1/E1 and L5/E5a bands on a container vessel was performed. This study reports how frequent RFI events occur, even making the GNSS service unavailable in some cases. [32] evaluates the jamming impact on the safety of the maritime navigation and the quality of on-shore services such as vessel traffic management, conducting a jamming trial on the East coast of the United Kingdom using a professional L1 band jammer. The lack of GNSSs triggers numerous alarms and failures of interfaces (like the ECDIS) on the bridge of the vessel, causing discomfort to a vessel crew that additionally needs to face the challenge of quickly reverting to traditional means of navigation. A prior work of the authors [33] complements the GNSS information with the integration of inertial sensors and Doppler Velocity Log (DVL) to provide accurate navigation solution under the effect of jamming.

This work presents a broad picture on the threat of GNSS jamming and its implication on the maritime domain. For the characterization of actual jamming conditions, the German Federal Network Agency authorized the use of an area in the Baltic Sea to serve as jamming testbed. The main countermeasure techniques against jamming are reviewed and the deterioration of the navigation solution is analyzed. Besides, the importance of detecting the interference attack is discussed and how the context-awareness can be exploited to mitigate the impact on the navigation.

The rest of the paper is organized as follows: Section 2 provides a brief overview on the main techniques for jamming detection and mitigation. Section 3 analyzes the effects of employing a PPD over conventional positioning techniques on an authorized maritime testbed. Finally, section 4 presents an outlook of the work and discusses the future lines of work.

II. Jamming Countermeasures

In general, one can distinguish three groups of solutions which can be used for mitigation of GNSS jamming. Firstly, if available, alternative terrestrial radio navigation systems are employed to enable a position determination independent from GNSS. However, after the decommission of LORAN-C (eLoran) in the US as well as in Europe, no global operational backup exists anymore. For maritime application, the so-called R-Mode (R-Ranging) is currently being developed as a terrestrial backup system. Here, existing signals of opportunity of globally available maritime infrastructure such as MF radio beacons and ashore AIS stations will be used as possible ranging sources [34]. A first experimental testbed for R-Mode will be established in the R-Mode Baltic project (2017-2020) in the western part of the Baltic Sea [35]. Within the methods of the second group the impact of jamming is mitigated inside the GNSS receiver by robust signal processing techniques and adaptive antenna arrays. Finally, within the third group the positioning information from the GNSS receiver is combined within a multi-sensor fusion scheme with independent onboard sensors.

A. Robust Signal Processing Techniques

To combat RFI, a classical approach in GNSS receivers is referred to as Interference Cancellation (IC), which consists of detecting the interference, estimating its waveform (usually through a parametric model), and mitigating its effect by substracting that estimated interference [36]–[38]. In mathematical terms, the received sampled signal is modeled as $y[n] = x_\theta[n]+i[n]+\eta[n]$, where $x_\theta[n]$ is the legitimate signals from GNSS satellites parameterized through a set of variables such as time-delay or Doppler-shift that we gather in a vector $\boldsymbol{\theta}$; $i[n]$ represents the interfering signal; and $\eta[n]$ is a random term due to thermal noise.

In IC, the various steps described earlier yield an estimate $\hat{i}[n]$ of the RFI, which is used to *clean* the received signal such that a new signal is generated

$$\tilde{y}[n] = y[n] - \hat{i}[n] = x_\theta[n] + \Delta i[n] + \eta[n] \tag{1}$$

where $\Delta i[n] = i[n] - \hat{i}[n]$ is the residual RFI estimation error. The performance of IC methods highly depends on the quality of the RFI detection (i.e., $\hat{i}[n] \neq 0$) and estimation (i.e., $\Delta i[n] \approx 0$) steps.

Many standard RFI mitigation techniques fall in the category of IC. For instance, adaptive notch filtering [39] estimates the narrowband frequency of the jamming signal to reconstruct its waveform and remove it as in (1). Another example of IC technique is pulse blanking [40], where samples above a certain threshold γ are considered jammed and thus zeroed. Then, in (1), the estimated interference is $\hat{i}[n] = y[n]$ when $|y[n]| \geq \gamma$ and $\hat{i}[n] = 0$ otherwise.

It is agreed that these techniques provide remarkable performance under challenging jamming scenarios. However, the main drawback of IC is its need for detecting and reconstructing the interference signal. Those steps constitute a point of failure when they cannot be accomplished properly or under model mismatch [4]. A more versatile set of techniques was recently proposed that overcome IC limitations, while preserving their performance. This family of techniques is known as Robust Interference Mitigation (RIM) and leverages the technically sound theory of robust statistics [41], [42] to develop GNSS receivers that are resilient to jamming signals and other outliers to the nominal model [43]. At a glance, RIM methods modify the cross-ambiguity function (CAF) used in the baseband signal processing of any GNSS receiver to automatically remove outliers, without the actual need for detecting and estimating interferences. An important feature of GNSS signals that is exploited in RIM is that those signals are buried in noise, therefore any other source raising above that level would be considered as an outlier. Such modification of the CAF takes the form of a nonlinear transformation of the incoming signal $\tilde{y}[n] = \varphi(y[n])$, which is applied before the CAF is computed. A variety of options exist for $\varphi(\cdot)$ giving raise to different RIM techniques such as myriad [44], complex signum [45] or Huber [46] nonlinearities. Additionally, RIM

techniques can also be applied in transformed domains (such as frequency domain) where certain RFIs are observed as outliers above the noise level, and thus can be better counteracted by RIM [47]. For instance, whereas continuous wave (CW) signals appear as outliers in the frequency domain, they are not in the time domain. On the other hand, pulsed interferences behave on the opposite way. The more general dual-domain RIM (or DD-RIM) methodology was proposed in [48], where the consecutive use of RIM in two domains (e.g., time and frequency) is analyzed.

In summary, RIM is a powerful approach to design interference mitigation techniques for GNSS receivers, which not only has been proven to provide enhanced performance with respect to IC but also simpler tuning.

B. Adaptive Antenna Arrays

One of the most powerful technologies available to tackle the problem of high number-very strong interference signal arises from the use of multi-channel systems. Typically a GNSS receiver is formed of three basic modules: antenna, analogue signal conditioning hardware or frontend, and a digital signal processing unit. A multi-channel system expands this architecture into several identical parallel channels. That means several antenna elements are put together forming so called antenna arrays. The antenna array can vary in topology with the most used ones being: Uniform Linear Array (ULA), Uniform Rectangular Array (URA) and Uniform Circular Array (UCA). In addition, other conformal topologies are appearing to adapt the array to different surfaces and applications [49]. The use of antenna arrays enables spatial diversity capabilities. Those capabilities rely on the addition of a new mathematical dimension, the spatial one. The mathematical degrees of freedom provided allow the algorithms to mitigate several strong interference impinging the array from several directions.

In a multi-channel system, the ability to mitigate interferences can be broken into two groups, depending at which point in the processing chain the interference is mitigated. If the interference is cancelled before the correlation process, the techniques are referred to as *pre-correlation* techniques. Pre-correlation techniques are the most powerful but also the ones with higher complexity and hence requiring more resources and processing power. Usually fast real time parallel data processing is required. The advantage of those techniques is cancelling strong interferences in the early stage, before the GNSS signal processing has started. The second group, *post-correlation* techniques, influences the processing after the correlation process is completed. Hence, the post-correlation techniques can use the knowledge of the desired GNSS signal. A typical example of these techniques is the beamforming process, where the digitally constructed antenna array pattern is oriented towards the desired GNSS signal putting zeros or nulls in the directions of other non-desired signals. This method can be a good complement for the pre-correlation techniques, removing residual interferences that were attenuated before the correlation.

Aiming to obtain an array output signal where the interference is cancelled out, the elements of the antenna arrays are weighted optimally. Such optimization problem is generally derived from the Linear Constraint Minimum Variance (LCMV) algorithm. Since the navigation signal is buried under noise, the received energy above the noise level will be the interference contribution. Hence, the usual goal is to nullify all signals which exhibit a greater energy than the noise.

In the last years, a tendency towards software defined radio GNSS receivers has put aside the analogue components; however, for interference mitigation it is crucial to consider all the components and take the right design steps. The antenna array [49], [50] and frontend [51], [52] play a fundamental role in the performance of many array techniques, not only interference mitigation, but also others e.g. direction of arrival estimation. In addition, the number of elements in the array increases the complexity and cost of the system. Potential solutions to these issues include increasing the degrees of freedom thanks to more advance interference mitigation techniques that enable not only spatial diversity but also temporal [52].

C. Multi Sensor Fusion

Another way to mitigate the effects of jamming on the positioning is to fuse the information of GNSS with other sensing modalities. Inertial sensors, gyrocompass and the speed log are generally the sensors to accompany GNSS on the task of maritime navigation. Estimating the navigation solution of a multi-sensor system is realized within the framework of Recursive Bayesian Estimation, with the Kalman Filter (KF) being the most widely applied technique.

One can distinguish three architectures for GNSS integration [53]: loosely, tightly and ultra-tightly coupled. In the loosely coupled scheme the processed position and velocity solution from the GNSS measurements as well as the measurements from the Inertial Navigation System (INS) are used as inputs of the KF where the covariance matrix takes into account the uncertainity of the derived GNSS navigation solution. In contrast to this, the tightly coupled scheme uses the raw GNSS measurements, i.e. pseudoranges and Doppler measurements. Here, the covariance matrix entries describe the accuracies of the GNSS observables which can be difficult in the case of jamming as explained in the next paragraph. The third architecture, the ultra-tightly coupled scheme, uses an INS to provide receiver dynamics information which allows the receiver to track weak signals using long coherent integration.

Jamming can cause the loss of track of satellites. Therefore, it is more advantageous to employ a tightly coupled KF which applies the code and doppler measurements directly in the measurement model of the filter. In contrast to the loosely coupled KF, it does not need a snapshot position solution for each integration step which would require tracking at least four satellites. On the one hand it necessitates having a model for the pseudorange variance, on the other hand even a few GNSS code observations can help in constraining the possible drift

of the position estimation. This is typical for inertial sensors as was reported in [54].

During jamming attacks, observations from the tracked satellites have been shown to pose just slightly worsen stochastic error characteristics [33]. In [55], the dual-frequency Melbourne-Wübbena combination is applied on GNSS observations under a controlled laboratory jamming experiment for the stochastic modelling of the noise levels, deriving variance models for code measurements. These models BLABLA... Similarly, adaptive sensor fusion procedures can be integrated with contextual reasoning about the sensor observations to relate them with situation elements and domain knowledge [56]. In general, context is used for several key tasks such as explaining observations according to the situation, constrain the processes or refine the estimations [57]. In this case, the analysis of recorded data can be dealt as a context learning process [58], [59], providing knowledge useful to describe the presence of jamming accordingly to areas, routes, etc, which could be used to reason about particular situations and adapt the fusion parameters.

III. Analysis of the Maritime Jamming Test

To enable experimental jamming tests under real life maritime conditions, the German Federal Network Agency allocated a civilian maritime GNSS jamming testbed in the Baltic Sea. The test area is located approximately 10 km north of the Darß Peninsula, as indicated in Fig. 1. A dedicated measurement campaign was conducted for two days in October 2015, covering different test scenarios. For the sake of evaluation, a three hour-long snippet on 22nd October 2015 (DOY 295, UTC 07:00-10:00) is considered in this work. Three vessels were involved in the experimentation: the AARON chartered ship carries the jammer and acts as attacking vessel, the BALTIC TAUCHER II is a multipurpose research and diving vessel acting as victim of the radio attack and the NEUSTRELITZ is a law enforcement vessel. Along

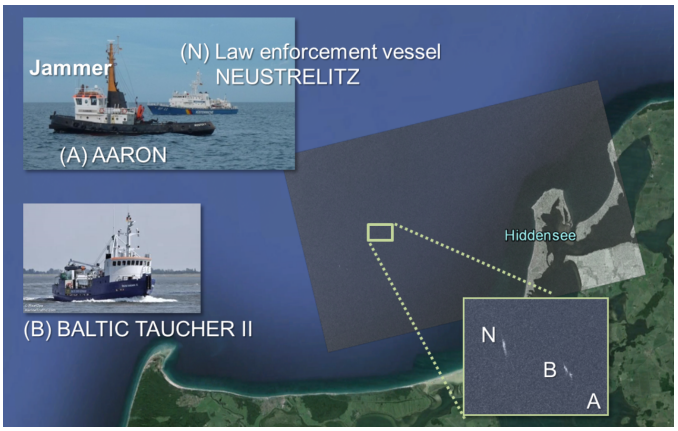

Fig. 1. An overview of the civilian maritime jamming test area 10 km North of Peninsula Darß (54,5474 N, 12,8154 E). Three vessels were involved, the BALTIC TAUCHER II (B), the AARON (A) and the law enforcement vessel NEUSTRELITZ (N). A SAR image shows the position of the ships participating in the experiment.

the three hours studied, the attacker remains anchored in the center of the test scenario and the victim ship performs maneuver trials around the AARON at distance ranging from 40 to 4000 m at a maximum speed of eight knots. Since the NEUSTRELITZ ship is not under the guidance of any DLR member, she enters the scene and moves along it at her own behalf. Equipment-wise, the AARON mounts a PPD jammer on the monkey deck (WolvesFleet WF-121G, total output power: 2 W) and geodetic GNSS equipment (navXperience 3G+C antenna and multi-frequency multi-constellation Javad Delta receiver). The victim vessel is equipped with commercial GNSS equipment and, tactical-grade inertial sensors (Imar IMU FCAI), a gyrocompass and DVL (Foruno DS 60).

Fig. 2 (left) and (right) illustrates the spectrogram and the power spectral density, respectively, of the WF-121G which is a Class II sweeping a continuous wave signal with an update rate of approx. 10 μs around the GPS L1 frequency covering a bandwidth of 17 MHz affecting both GPS L1 and Galileo E1 signal tracking, while GLONASS G1 mainly remained unaffected. This allowed us to use GLONASS for the calculation of a Precise Point Positioning (PPP) reference trajectory using RTKLib software [60] even in the direct vicinity of the jammer.

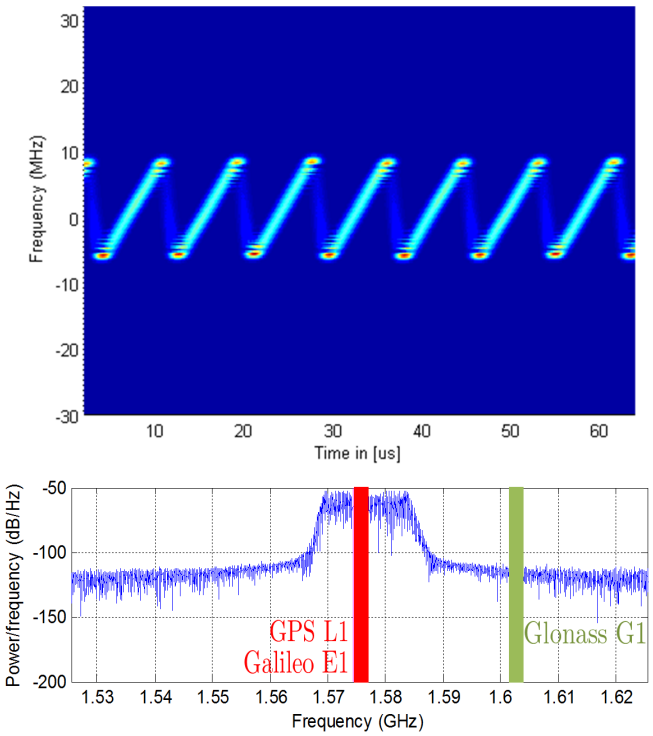

Fig. 2. Characterisation of the WF-121G PPD jammer. On the top, spectogram of the saw-tooth-like chirp signal. On the bottom, power spectral density of the jammer together with the location of the GNSS signals GPS L1, Galileo E1 and GLONASS G1.

Along the three hours of evaluation, the jammer is switched off for five minutes in periods of approximately twenty minutes, with the intention of studying the time for satellite acquisition under jamming conditions. Fig. 4 depicts the mean

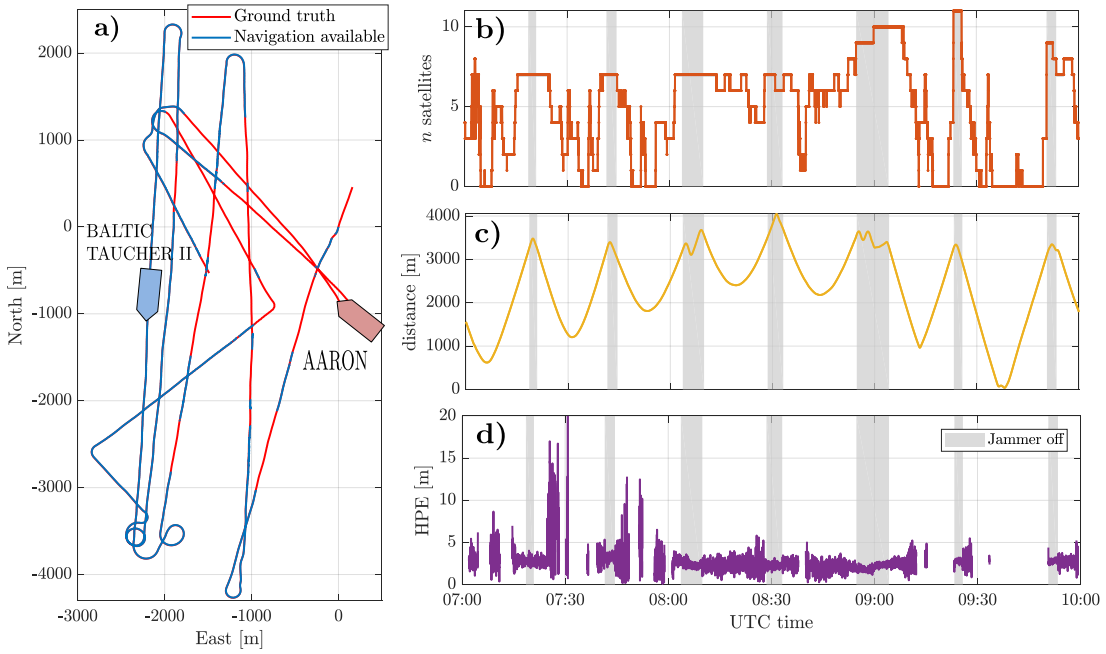

Fig. 3. Evaluation of the availability and quality of the PNT solution, using a SPP solver on GPS L1 observations. **a)** Situation depiction of the attacking and victim vessels along the three hours of evaluation. The blue line corresponds to the navigation solution based on an ordinary method and the red line corresponds to the positioning estimated using a PPP solution when the SPP is unavailable. **b)** Number of satellites tracked for GPS on the L1 frequency. **c)** Distance from the BALTIC TAUCHER to the attacking vessel. **d)** Horizontal Positioning Error (HPE) over time.

C/N_0 among the tracked satellites over time and it highlights with on shaded gray the periods in which the jammer is turned off. One can easily observe the immediate deterioration of the signal strength as soon as the jammer is active. Unlike phenomena related to signal reflection, where sudden drops of C/N_0 might occur on single satellite links, jamming can be easily identified due to the abrupt deterioration on the C/N_0 affecting all tracked satellites.

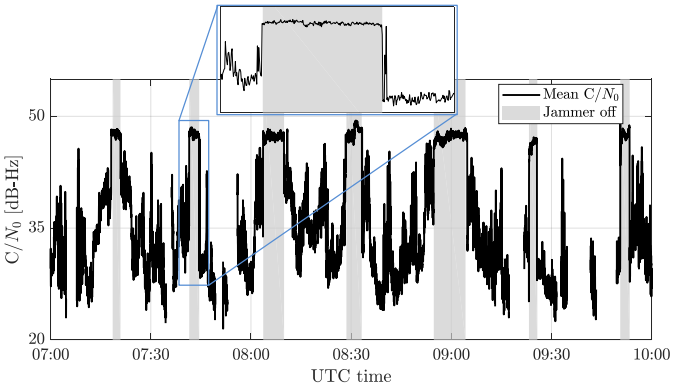

Fig. 4. Average C/N_0 along the three hours of evaluation. The PPD jammer is permanently switched on, except for small periods of around five minutes – indicated as shaded-gray areas.

Since the vast majority of mass-market GNSS receivers are single-frequency capable and apply an ordinary Single Point Positioning (SPP) method to calculate the position, the evaluation of the PNT estimation will only use GPS L1 on a SPP. Fig. 3 a) depicts the position of the AARON (attacking vessel) and the maneuvers performed by the BALTIC TAUCHER II (victim vessel). The blue line indicates the estimated position, while the red line depicts the positions where the vessel could not be tracked. The size of the area affected by the radio attack is massive, despite using a relatively simple PPD as jammer. However, the unavailability of the PNT service is not entirely correlated with the closeness to the source of attack. For instance, shortly after 09:30 a PNT solution can be obtained roughly 750 m away from the jammer, while around 09:50 a PNT solution cannot be estimated at a 3000 m distance to the attacker, as can deducted from Fig. 3 c) and d).

IV. Conclusions and Future Work

This work provides an overview on GNSS jamming attacks and the growing relevance of radio threats for intelligent transportation systems. In particular, GNSS plays a major role in the maritime world, since not only the vessel navigation is heavily reliant on it, but also a variety of interfaces present on the skipper bridge. Throughout the last years, it has been shown that the maritime domain often faces the jamming menace, either due to military or illegal fishery activities. Thus, a broad view on the main techniques for jamming detection and mitigation is presented, highlighting the most advanced methods related to robust signal processing, antenna array technology and sensor fusion.

Besides, the effects of a jamming attack over conventional navigation techniques is addressed on a maritime scenario where the German authorities allowed DLR to conduct such

an experiment. Three vessels participate on the experiment conducted on the Baltic Sea, where a moored vessel mounts a PPD and behaves as attacker and the victim vessel performs maneuvers in the surroundings of the first. It has been shown that the jamming influence area surpasses a radius of three kilometres, although its effect is uneven. Jamming detection via C/N_0 monitoring has been shown to perform reasonably, as all tracked satellites suffer simultaneously from an abrupt drop on such parameter, available even in low-cost mass-markets receivers.

Future lines of work include analyzing the individual performance gain achieved by different jamming mitigation technologies, i.e., robust signal processing, multi-antenna arrays and sensor fusion, as well as the combination of them. Moreover, the early detection of a radio attack can be considered a relevant source of context-inferred knowledge, which is in turn fundamental for gaining situation awareness. Thus, parameters of navigation algorithms can be automatically tuned and the crew of the ship might understand that illegal activities are being carried out in the vicinity.

ACKNOWLEDGMENT

P.C. was supported by the National Science Foundation under Awards CNS-1815349 and ECCS-1845833.

REFERENCES

[1] M. G. Amin, P. Closas, A. Broumandan, and J. L. Volakis, "Vulnerabilities, threats, and authentication in satellite-based navigation systems [scanning the issue]," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1169–1173, 2016.

[2] F. Dovis, *GNSS Interference Threats and Countermeasures*. Artech House, 2015.

[3] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[4] D. Borio and P. Closas, "A fresh look at GNSS anti-jamming," *Inside GNSS*, vol. 12, pp. 54–61, 2017.

[5] J. A. Volpe, "Vulnerability assessment of the transportation infrastructure relying on the global positioning system," Volpe National Transportation Systems Center, Tech. Rep., 2001.

[6] M. Leccadito, T. Bakker, R. Klenke, and C. Elks, "A survey on securing UAS cyber physical systems," *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 10, pp. 22–32, 2018.

[7] D. Borio, F. Dovis, 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, June 2016.

[8] E. Kaplan and C. Hegarty, *Understanding GPS: principles and applications*. Artech house, 2005.

[9] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Radionavigation laboratory conference proceedings*, 2008.

[10] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, no. 2, pp. 40–46, 2009.

[11] P. Boulton, R. Borsato, B. Butler, and K. Judge, "GPS interference testing: Lab, live, and lightsquared," *Inside GNSS*, vol. 5, no. 4, pp. 32–45, 2011.

[12] F. Dimc, M. Bažec, D. Borio, C. Gioia, G. Baldini, and M. Basso, "An experimental evaluation of low-cost GNSS jamming sensors," *Navigation: Journal of The Institute of Navigation*, vol. 64, no. 1, pp. 93–109, 2017.

[13] T. Kraus, R. Bauernfeind, and B. Eissfeller, "Survey of in-car jammers-analysis and modeling of the RF signals and IF samples (suitable for active signal cancelation)," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR*, 2011, pp. 430–435.

[14] S. Pullen and G. X. Gao, "GNSS jamming in the name of privacy: Potential threat to GPS aviation," *Inside GNSS*, vol. 7, no. 2, pp. 34–43, 2012.

[15] S. Pullen, G. Gao, C. Tedeschi, and J. Warburton, "The impact of uninformed RF interference on GBAS and potential mitigations," in *Proceedings of the 2012 International Technical Meeting of the Institute of Navigation (ION ITM 2012), Newport Beach, CA*, 2012, pp. 780–789.

[16] G. Siegert, P. Banyś, J. Hoth, and F. Heymann, "Counteracting the effects of GNSS jamming in a maritime multi-target scenario by fusing AIS with radar data," in *ION International Technical Meeting. Monterrey, CA, USA: International Organization of Navigation*, 2017.

[17] I. Maritime Organization (IMO), "Revised guidelines for the onboard operational use of shipborne automatic identification systems (AIS)," IMO, Tech. Rep. A.1106(29), December 2015.

[18] Ship Technology. (2018, August) Transparent transhipping: detecting illegal fishing with satellite data. [Online]. Available: https://www.ship-technology.com/features/global-fishing-watch/

[19] World Wildlife Fund (WWF). (2018) Technology helps fight illegal fishing. [Online]. Available: https://www.worldwildlife.org/stories/technology-helps-fight-illegal-fishing

[20] Illegal, Unreported and Unregulared Watch (IUUWATCH). (2019, January) Fuel tankers help highlight illegal fishing hotspots. [Online]. Available: http://www.iuuwatch.eu/2019/01/fuel-tankers-help-highlight-illegal-fishing-hotspots/

[21] The Jerusalem Post. (2018, October) Avoiding detection: The team tracking Irans attempt to cloak its oil exports. [Online]. Available: https://www.jpost.com/Middle-East/Avoiding-detection-The-team-tracking-Irans-attempt-to-cloak-its-oil-exports-570236

[22] InsideGNSS. (2013, April) North koreas GPS jamming prompts south korea to endorse nationwide eloran system. [Online]. Available: https://insidegnss.com/north-koreas-gps-jamming-prompts-south-korea-to-endorse-nationwide-eloran-system/

[23] Business Insider Australia. (2018, April) China has jamming equipment in the south china sea – and the US may 'not look kindly on it'. [Online]. Available: https://www.businessinsider.com.au/china-jamming-us-navy-jets-off-aircraft-carriers-pacific-2018-4

[24] GPS World. (2018, November) GPS disrupted for maritime in mediterranean, red sea. [Online]. Available: https://www.gpsworld.com/gps-disrupted-for-maritime-in-mediterranean-red-sea/

[25] N. Vagle, A. Broumandan, and G. Lachapelle, "Multiantenna GNSS and inertial sensors/odometer coupling for robust vehicular navigation," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4816–4828, 2018.

[26] R. Bauernfeind, I. Krämer, H. Beckmann, B. Eissfeller, and V. Vierroth, "In-car jammer interference detection in automotive gnss receivers and localization by means of vehicular communication," in *2011 IEEE Forum on Integrated and Sustainable Transportation Systems*. IEEE, 2011, pp. 376–381.

[27] D. Borio, "Swept GNSS jamming mitigation through pulse blanking," in *2016 European Navigation Conference (ENC)*. IEEE, 2016, pp. 1–8.

[28] J.-L. Issler, L. Ries, J. Bourgeade, L. Lestarquit, and C. Macabiau, "Contribution of altboc to interference mitigation for civil aviation," in *First CNES workshop on GALILEO signals*, 2006.

[29] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks," in *Radionavigation Laboratory Conference Proceedings*, 2012.

[30] E. Pérez. Marcos, S. Caizzone, A. Konovaltsev, M. Cuntz, W. Elmarissi, K. Yinusa, and M. Meurer, "Interference awareness and characterization for GNSS maritime applications," in *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, April 2018, pp. 908–919.

[31] E. Pérez. Marcos, A. Konovaltsev, S. Caizzone, M. Cuntz, K. Yinusa, W. Elmarissi, and M. Meurer, "Interference and spoofing detection for GNSS maritime applications using direction of arrival and conformal antenna array," in *Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, September 2018, pp. 2907–2922.

[32] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS jamming and the impact on maritime navigation," *The Journal of Navigation*, vol. 62, no. 2, pp. 173–187, 2009.

[33] R. Ziebold, D. Medina, M. Romanovas, C. Lass, and S. Gewies, "Performance characterization of GNSS/IMU/DVL integration under real maritime jamming conditions," *Sensors*, vol. 18, no. 9, p. 2954, 2018.
[34] P. S. Gregory Johnson, "Feasibility study of R-Mode combining MF DGNSS, AIS, and eLoran transmissions," German Federal Waterways and Shipping Administration, Federal Waterways and Shipping Agency, Final report Accseas Project, Tech. Rep., 2014.
[35] S. Gewies, M. Dziewicki, and M. Hoppe, "R-mode baltic - a user need driven testbed development for the baltic sea," in *ION GNSS+ 2018*, Oktober 2018. [Online]. Available: https://elib.dlr.de/122034/
[36] P. H. Madhani, P. Axelrad, K. Krumvieda, and J. Thomas, "Application of successive interference cancellation to the GPS pseudolite near-far problem," *IEEE_J_AES*, vol. 39, no. 2, pp. 481–488, April 2003.
[37] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," *IEEE_J_PROC*, vol. 104, no. 6, pp. 1233–1245, Jun. 2016.
[38] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, "Protecting GNSS receivers from jamming and interference," *IEEE_J_PROC*, vol. 104, no. 6, pp. 1327–1338, Jun. 2016.
[39] D. Borio, L. Camoriano, and L. Lo Presti, "Two-pole and multi-pole notch filters: A computationally effective solution for GNSS interference detection and mitigation," *IEEE Systems Journal*, vol. 2, no. 1, pp. 38–47, Mar. 2008.
[40] D. Borio and E. Cano, "Optimal global navigation satellite system pulse blanking in the presence of signal quantisation," *IET Signal Processing*, vol. 7, no. 5, pp. 400–410, Jul. 2013.
[41] P. J. Huber and E. M. Ronchetti, *Robust Statistics*, 2nd ed., ser. Wiley Probability and Statistics. John Wiley and Sons, Mar. 2009.
[42] A. M. Zoubir, V. Koivunen, Y. Chakhchoukh, and M. Muma, "Robust estimation in signal processing: A tutorial-style treatment of fundamental concepts," *IEEE Signal Processing Magazine*, vol. 29, no. 4, pp. 61–80, 2012.
[43] D. Borio, "Robust signal processing for GNSS," in *Proc. of the 2017 European Navigation Conference (ENC)*, Lousanne, Switzerland, May 2017, pp. 150–158.
[44] ——, "Myriad non-linearity for GNSS robust signal processing," *IET Radar Sonar and Navigation*, vol. 11, no. 10, pp. 1467–1476, Oct. 2017. [Online]. Available: http://digital-library.theiet.org/content/journals/10.1049/iet-rsn.2016.0610
[45] D. Borio and P. Closas, "Complex signum non-linearity for robust GNSS signal mitigation," *IET Radar Sonar and Navigation*, pp. 1–10, Apr. 2018. [Online]. Available: http://digital-library.theiet.org/content/journals/10.1049/iet-rsn.2017.0552
[46] D. Borio, H. Li, and P. Closas, "Huber's non-linearity for GNSS interference mitigation," *Sensors*, vol. 18, no. 7, p. 2217, 2018.
[47] D. Borio and P. Closas, "Robust transform domain signal processing for GNSS," *Navigation*, 2019.
[48] H. Li, D. Borio, and P. Closas, "Dual-domain robust GNSS interference mitigation," in *Proceedings of the International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2019)*, Miami, FL, 16-20 Sept 2019.
[49] K. A. Yinusa, E. P. Marcos, and S. Caizzone, "Robust satellite navigation by means of a spherical cap conformal antenna array," in *2018 18th International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM)*, Aug 2018, pp. 1–2.
[50] S. Caizzone, "Miniaturized E5a/E1 antenna array for robust GNSS navigation," *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 485–488, 2017.
[51] M. Cuntz, A. Konovaltsev, M. Heckler, A. Hornbostel, L. Kurz, G. Kappen, and T. Noll, "Lessons learnt: The development of a robust multi-antenna GNSS receiver," in *ION GNSS 2010*, September 2010.
[52] E. P. Marcos, A. Konovaltsev, M. Cuntz, and M. Meurer, "STAP as a solution for imperfections in multi-antenna GNSS receivers," in *NAVITEC 2016*, December 2016.
[53] P. Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, Second Edition*. Artech House, 2013.
[54] R. Ziebold, M. Romanovas, and L. Lanca, *Activities in Navigation. Marine Navigation and Safety of Sea Transportation*. CRC Press, 2015, ch. Evaluation of Low Cost Tactical Grade MEMS IMU for Maritime Navigation, pp. 237–246.
[55] C. Lass and R. Ziebold, "Modelling the noise of GNSS signals under jamming conditions," in *navitec 2018*. ESA, 2018.
[56] F. Caron, E. Duflos, D. Pomorski, and P. Vanheeghe, "Gps/imu data fusion using multisensor kalman filtering: introduction of contextual aspects," *Information fusion*, vol. 7, no. 2, pp. 221–230, 2006.
[57] J. Gómez-Romero, M. A. Serrano, J. García, J. M. Molina, and G. Rogova, "Context-based multi-level information fusion for harbor surveillance," *Information Fusion*, vol. 21, pp. 173–186, 2015.
[58] L. Snidaro, J. García, and J. Llinas, "Context-based information fusion: a survey and discussion," *Information Fusion*, vol. 25, pp. 16–31, 2015.
[59] B. J. Rhodes, "Taxonomic knowledge structure discovery from imagery-based data using the neural associative incremental learning (nail) algorithm," *Information Fusion*, vol. 8, no. 3, pp. 295–315, 2007.
[60] T. Takasu, "RTKLIB: An open source program package for GNSS positioning," 2011.