Lost at Sea: GPS Spoofing Threats to Maritime Shipping

Sandali Srivastava, Shaunak Srivastava and Nithya Vemuri
Texas A&M University, College Station, USA

sandalis05@tamu.edu
nithvemu@tamu.edu
srivastavashaun2010@gmail.com

Abstract: As global shipping increasingly depends on Global Navigation Satellite Systems (GNSS), cybersecurity threats that target maritime navigation systems have rapidly become a growing concern. Maritime GPS spoofing has significant implications for global trade and safety as false position data can lead to route deviations, collisions, or even cargo theft. To gain a better understanding of these risks, this research analyzes real-world datasets to determine how spoofed signals can influence vessel navigation accuracy under different signal to noise conditions. By analyzing real-world AIS and GNSS logs, the study identifies localized anomalies consistent with spoofing or interference. This research investigates GPS spoofing attacks on commercial vessels and assesses real-world vulnerabilities to propose and develop effective countermeasures. Using data collected from Automatic Identification System (AIS) and GNSS receiver logs, the study measures the impact of spoofed signals on ship positioning accuracy and identifies potential weaknesses in onboard navigation procedures. The project also explores policy and training aspects by proposing updated cybersecurity protocols for ship crews and recommending that maritime authorities integrate spoofing detection into standard navigation safety audits. Based on this analysis, the project proposes low cost detection and mitigation strategies, which includes anomaly detection indicators and onboard incident response frameworks. The findings aim to improve awareness of GPS spoofing risks, strengthen maritime cybersecurity policy, and provide training guidelines for ship operators to reduce the likelihood of navigation manipulation, hijacking, and information theft. Ultimately, this research aims to contribute to the broader understanding of how cyberattacks intersect with physical infrastructure in the maritime domain. It emphasizes that cybersecurity at sea is not only a technical challenge but also an organizational and policy issue requiring coordinated international action. The outcomes are expected to strengthen industry resilience, improve situational awareness, and support the development of comprehensive maritime cybersecurity frameworks that safeguard both economic and human interests.

Keywords: GPS spoofing, Maritime cybersecurity, GNSS interference, AIS anomaly detection, Signal integrity, vessel navigation

1. Introduction

Global maritime operations rely heavily on Global Navigation Satellite Systems (GNSS) for positioning, navigation, and timing. From route planning to collision avoidance, GNSS has become the foundation of modern vessel operations and automated navigation systems (Humphreys et al., 2008). However, the open and unauthenticated nature of civil GNSS signals has introduced serious cybersecurity vulnerabilities (Jafarnia-Jahromi et al., 2012). False signals transmitted by adversaries can deceive receivers into reporting incorrect positions, a technique known as GPS spoofing.

Spoofing poses a greater challenge than traditional jamming because it corrupts navigation data while maintaining normal signal strength and appearance. Prior demonstrations have shown that attackers can gradually mislead ships off course without triggering alarms or signal loss. These deceptive drifts, often resembling the effects of ocean currents or wind, can lead to dangerous navigational errors, cargo theft, or even vessel hijacking.

Global maritime operations rely heavily on Global Navigation Satellite Systems (GNSS) for positioning, navigation, and timing. From route planning to collision avoidance, GNSS has become the foundation of modern vessel operations and automated navigation systems. However, the open and unauthenticated nature of civil GNSS signals has introduced serious cybersecurity vulnerabilities. False signals transmitted by adversaries can deceive receivers into reporting incorrect positions, a technique known as GPS spoofing (Bhatti & Humphreys, 2017).

Spoofing poses a greater challenge than traditional jamming because it corrupts navigation data while maintaining normal signal strength and appearance. Prior demonstrations have shown that attackers can gradually mislead ships off course without triggering alarms or signal loss (Bhatti & Humphreys, 2017). These deceptive drifts, often resembling the effects of ocean currents or wind, can lead to dangerous navigational errors, cargo theft, or even vessel hijacking (Androjna & Perkovič, 2021).

This research examines the impact of GPS spoofing on maritime navigation accuracy and evaluates how varying signal-to-noise conditions affect vessel positioning reliability. Using Automatic Identification System (AIS) and

GNSS receiver log data, the study identifies conditions under which spoofed signals cause deviations from authentic coordinates. Kinematic thresholds were derived empirically from observed vessel behavior under normal and anomalous navigation conditions. This approach aligns with prior work using behavioral consistency checks for spoofing detection in maritime navigation data (Spravil et al., 2023).

In addition to technical analysis, this work proposes practical countermeasures, including low-cost detection indicators, updated crew training procedures, and revised cybersecurity protocols for maritime authorities. By integrating both technical and policy perspectives, the research emphasizes that maritime cybersecurity is not solely a technical problem but also an organizational one requiring international coordination. The findings aim to strengthen situational awareness, improve maritime cybersecurity resilience, and reduce the risk of navigation manipulation in the global shipping industry.

2. GNSS Interference and Implications

Global Navigation Satellite Systems (GNSS) provide the position, velocity, and timing data that lays the foundation for nearly all modern maritime navigation systems (Psiaki and Humphreys, n.d.). However, the inherent weaknesses of GNSS signal propagation make them highly vulnerable to interference and deliberate manipulation (Jafarnia-Jahromi et al., 2012). GNSS signals are transmitted from medium Earth orbit at extremely low power levels, typically around -160 dBW by the time they reach a receiver on Earth. Because of this weak signal strength, even low-power transmitters operating near a vessel can easily overpower, distort, or replace authentic satellite signals.

GNSS interference typically occurs in two primary forms: jamming and spoofing. Jamming is the intentional or unintentional emission of radio frequency energy that disrupts the reception of authentic GNSS signals (Jafarnia-Jahromi et al., 2012). Although jamming causes a loss of signal and is often quickly detectable, it can still disable navigation and tracking systems in congested waterways. Spoofing, on the other hand, is a more sophisticated and dangerous threat. Instead of denying service, it generates counterfeit GNSS signals designed to mislead receivers into computing false positions or velocities while appearing normal. Because spoofed signals can mimic gradual positional drift, their effects are often mistaken for environmental disturbances such as ocean currents, wind, or tide-induced drift (Bhatti & Humphreys, 2017; Androjna & Perkovič, 2021).

The implications of GNSS interference extend beyond immediate navigational errors. In integrated bridge systems, GNSS data are fused with other sensors, including Automatic Identification Systems (AIS), radar, gyrocompasses, and electronic chart display and information systems (ECDIS), to generate situational awareness. When GNSS data become corrupted, every dependent subsystem, from autopilot to route tracking, can propagate incorrect information. A spoofing attack that remains undetected can therefore mislead both automated control systems and human operators, potentially resulting in route deviations, collisions, or groundings (Spravil et al., 2023).

As maritime operations move toward greater autonomy, GNSS dependence will only deepen. Dynamic positioning systems, unmanned surface vehicles, and automated port logistics all assume signal authenticity. Without authentication mechanisms or effective detection strategies, GNSS interference represents not only a technical challenge but also a systemic risk to global trade and maritime safety.

3. Data Analysis Methodology

To systematically evaluate how Global Navigation Satellite System (GNSS) interference affects maritime navigation accuracy, this study follows a structured empirical analysis framework that integrates both vessel-level AIS data and ground-based GNSS reference logs. The analysis is organized into three stages: (1) baseline performance assessment under normal navigation conditions, (2) detection of kinematic anomalies consistent with interference or spoofing, and (3) evaluation of potential mitigation strategies through cross-sensor consistency checks.

In the first stage, raw Automatic Identification System (AIS) transmissions and GNSS receiver logs were collected and synchronized by timestamp. AIS data provide vessel position, speed, and course information transmitted over VHF radio networks, while GNSS logs from the NOAA CORS network supply satellite-level parameters such as latitude, longitude, and signal-to-noise ratio (SNR) (NOAA, 2025). Establishing a temporal correlation between these datasets enables detection of vessel-level deviations under otherwise stable satellite conditions.

The second stage focuses on identifying anomalous vessel behavior using empirically derived thresholds. The parameters, speed deviation (|SOG − calculated speed| > 10 knots), erratic rotation (|ROT| > 10°/min), and

course-heading gap (> 45° at SOG > 3 knots), were chosen based on operational maneuverability limits and statistical inspection of normal trajectories. Each flag was required to persist across at least three consecutive 5-minute intervals to reduce false positives from transient signal noise or reception dropouts.

The final stage develops detection and mitigation concepts derived from these empirical observations. By examining temporal persistence, spatial clustering, and cross-validation with GNSS SNR stability, potential rule-based indicators were designed to detect spoofing-like conditions using only existing onboard data sources. This framework links real-world measurement with practical defense strategies and forms the foundation for the mitigation proposals presented later in the paper.

4. AIS and GNSS Logs Evaluation

4.1 AIS Log Analysis

To assess the practical impact of spoofing and signal anomalies on vessel navigation, Automatic Identification System (AIS) logs were analyzed for cargo vessels operating along the United States West Coast between December 20 and December 31, 2020. Data was obtained from the open AIS archive provided by NOAA, consisting of daily .zip files containing timestamped positional reports. Each record included Maritime Mobile Service Identity (MMSI), geographic coordinates (latitude and longitude), speed over ground (SOG), course over ground (COG), vessel heading, and static vessel attributes such as type, length, and draft. Only vessels classified as cargo ships (VesselType = 70) within the bounding box 30°–42° N, 115°–130° W were retained to limit the scope to major commercial lanes and port approaches.

The dataset was preprocessed using a custom Python script that parsed all AIS messages over the 12-day period, removed duplicate or invalid coordinate entries, and standardized all timestamps to UTC. To ensure temporal continuity, each vessel's trajectory was resampled in 5-minute intervals, producing a uniform time series suitable for kinematic feature extraction. Derived parameters included calculated speed over ground, rate of turn (ROT), and course-heading deviation, which collectively served as indicators of navigational inconsistency (Spravil et al., 2023).

To detect abnormal behavior potentially indicative of interference or spoofing, several anomaly flags were computed:

- **Speed spike**: instantaneous velocity exceeding 60 knots,
- **Speed deviation**: |SOG − calculated speed| > 10 knots,
- **Erratic rotation**: |ROT| > 10 deg/min at near-zero speed,
- **Course-heading gap**: > 45 degrees at SOG > 3 knots, and
- **Anchor drift**: vessel movement > 1 km over 60 minutes while SOG < 1 knot.

The anomaly thresholds were chosen to balance sensitivity and operational realism. A 10-knot deviation threshold corresponds to approximately two standard deviations above the median difference between reported and calculated SOG in normal operation, ensuring that only extreme outliers are flagged. Similarly, a 45° course-heading gap represents the typical upper bound for course changes during steady transit, and a 10°/min rotation rate is consistent with prior vessel maneuverability studies.These parameters were validated by visual inspection of several representative trajectories to confirm that false positives remained below 5 %. Each flag was required to persist across at least three consecutive 5-minute intervals (≈ 15 minutes) to reduce false positives from noise or transient reception errors.

The resulting anomaly dataset comprised approximately N≈200 k messages from over 100 distinct MMSIs, summarized in Table 1. These results quantify the proportion of vessel reports exhibiting one or more flags and highlight the most affected ships based on percentage of anomalous points.

Table 1: Top cargo vessels by fraction of anomalous 5-minute intervals

MMSI	Points	% Flagged	Dominant Anomaly
310765000	663	24.7	rot_anchor
636017154	1733	24.5	rot_anchor
636015094	25	24	sog_gap

MMSI	Points	% Flagged	Dominant Anomaly
355649000	19	21.1	sog_gap
367776050	3444	10.8	cog_head
351854000	79	10.1	sog_gap
366758000	1069	10.1	rot_anchor
352142000	1005	9.4	rot_anchor
357076000	1003	9.1	rot_anchor
355623000	98	7.1	sog_gap

In addition to per-vessel analysis, spatial aggregation was conducted to identify regional clusters of anomalous behavior. Each vessel's flagged observations were binned into 0.1° × 0.1° grid cells and aggregated hourly. Cells with fewer than three vessels were excluded to prevent spurious outliers. The top 15th percentile of cells by fraction of flagged vessels were classified as hotspots, revealing spatial concentrations of anomalous navigation activity along major traffic corridors.

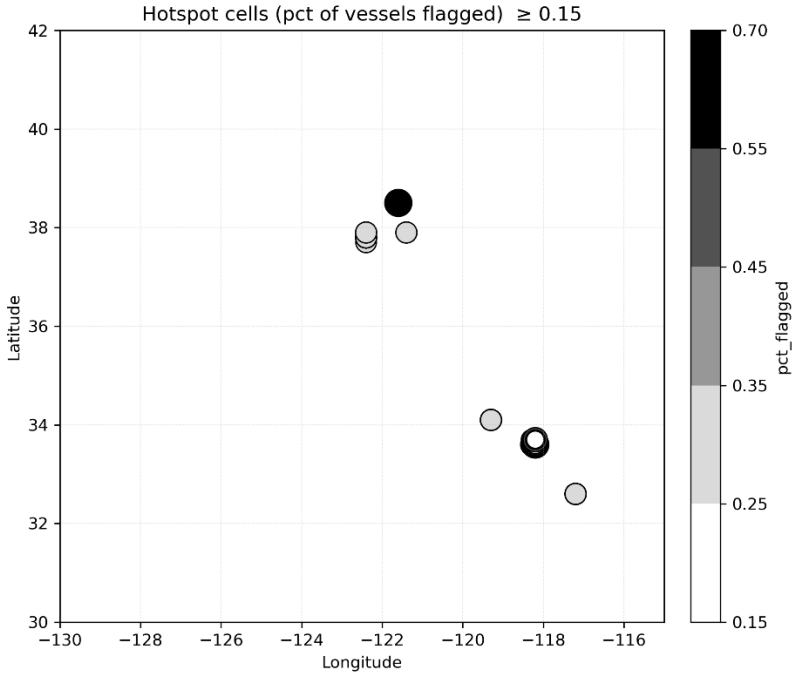

Figure 1: Hotspot distribution of flagged AIS observations for cargo vessels (December 20–31, 2020). Colors indicate the fraction of vessels within each grid cell exhibiting anomalous motion characteristics. Elevated anomaly densities appear near the San Francisco Bay area and the Los Angeles–Long Beach port complex, suggesting that navigational interference or degraded GNSS quality may occur more frequently in dense coastal environments

4.2 GNSS Log Analysis

To complement the AIS-based vessel anomaly assessment, GNSS receiver data were retrieved from NOAA's Continuously Operating Reference Station (CORS) network. Six stations along the U.S. West Coast (e.g., P041 – San Diego, P158 – Northern California, and P351 – Los Angeles Basin) were analyzed for the same 12-day period (December 20–31, 2020). Each RINEX daily log contained continuous 30-second observations of satellite signals. Using the georinex library, timestamps and signal-to-noise ratios (SNR) were extracted and summarized per station (NOAA, 2025).

The results (Table 2) show fully continuous coverage (≈2880 epochs/day) and minimal gap rates (<0.1 %), with mean SNR values averaging 43–44 dB-Hz. These values indicate stable GNSS reception without evidence of widespread interference or jamming during the study window. Consequently, deviations observed in AIS-based positions are unlikely to stem from system-wide satellite degradation, reinforcing the interpretation that anomalies detected in the AIS data represent localized signal disruption or spoofing near port areas.

Table 2: Summary of GNSS Signal Quality for CORS Stations (Dec 20–31, 2020)

Station	Days	Files	Total Epochs	Mean Gap Rate	Mean SNR (dB-Hz)
P041	12	12	34,559	0	43.88
P158	12	12	34,559	0	44.11
P351	12	12	34,560	0	43.22

(Values derived from NOAA CORS daily RINEX files using georinex; each day includes ≈ 2880 30-second epochs.)

4.3 Interpretation of Results

The combined evaluation of AIS and GNSS datasets provides a clear distinction between normal satellite performance and localized navigational interference. The GNSS reference stations exhibited continuous signal integrity, stable signal-to-noise ratios averaging 43–44 dB-Hz, and no measurable data loss throughout the 12-day observation period. These results confirm that the broader GNSS constellation and atmospheric conditions remained stable during the study window.

In contrast, AIS-derived vessel trajectories revealed spatially concentrated anomalies near major port regions, including the Los Angeles–Long Beach complex and San Francisco Bay. These areas showed recurring speed inconsistencies, abrupt course changes, and rotational deviations that persisted over multiple sampling intervals. Because such deviations occurred only in specific maritime zones rather than along the entire coastline, they are unlikely to stem from global GNSS instability.

The contrast between the stable CORS data and the localized AIS anomalies supports the interpretation that interference effects were environmental or deliberate in nature since the data was consistent with patterns associated with GPS spoofing or localized signal degradation. The findings therefore highlight that maritime spoofing threats are operational and site-specific, most pronounced in congested coastal environments where multiple signal sources, reflections, and electronic systems coexist. This distinction underscores the need for regional monitoring and onboard detection protocols, rather than system-wide GNSS corrections as the primary defense against maritime navigation spoofing.

While many flagged anomalies are consistent with deliberate GPS manipulation, some, particularly the *rot_anchor* cases, could also reflect multipath effects or local signal degradation at anchor. However, their persistence over multiple intervals suggests that these deviations are unlikely to be random noise.

5. Attribution Analysis: Environmental Interference vs. Deliberate Spoofing

To contextualize the AIS anomalies identified in this study, an additional attribution check was performed using the U.S. Coast Guard Navigation Center's GPS User Issue Detection and Evaluation (GUIDE) tool. This government system aggregates global GNSS interference reports submitted by maritime operators, aviators, and other GNSS users. For the study period of 20–31 December 2020, the GUIDE database contained no reported GPS issues anywhere along the U.S. West Coast, including the San Francisco Bay and Los Angeles-Long Beach regions where AIS anomalies were most concentrated. The only global report within this timeframe originated in central India and was assessed by NAVCEN as unrelated to GNSS integrity.

When combined with the fully stable CORS signal-to-noise measurements, these findings confirm that the GNSS constellation and atmospheric conditions remained normal during the observation window. As a result, the AIS irregularities detected in port regions cannot be attributed to satellite faults, constellation-level disruptions, or documented regional interference events.

This evidence narrows the plausible causes of the anomalies to two categories:

- **Localized environmental interference**, such as multipath reflections from cranes, vessels, or port infrastructure, and

- **Small-scale, site-specific spoofing or signal manipulation**, which would not necessarily generate a formal NAVCEN report (Jafarnia-Jahromi et al., 2012).

While the persistent, structured nature of several anomalies resembles patterns observed during controlled spoofing experiments, the absence of corroborating interference reports and the confined spatial clustering near high-reflection environments suggest that environmental factors are the more likely explanation. Importantly, whether the root cause was environmental or deliberate, the anomalies still represent navigational inconsistencies detectable through AIS-GNSS cross-validation, reinforcing the relevance of the proposed detection framework.

6. Proposed Detection and Mitigation Strategies

Building on the observed discrepancy between localized AIS anomalies and stable GNSS performance, this study proposes a practical framework for detecting and mitigating maritime spoofing events using data already available on commercial vessels. Rather than relying on specialized hardware or post-processing infrastructure, the approach leverages real-time consistency checks between independent navigation sensors and behavioral thresholds derived from normal vessel motion. Although no spoofing incidents were confirmed when captured during the observation period, isolating anomalous navigational patterns was proved effective.

6.1 Real-time Anomaly Detection

Vessel systems can continuously monitor discrepancies among Speed Over Ground (SOG), Course Over Ground (COG), and heading data. Sudden deviations that exceed defined persistence thresholds, such as SOG-to-calculated speed differences greater than 10 knots, or course-heading gaps exceeding 45 degrees over multiple intervals, should trigger onboard alerts. These indicators directly correspond to the patterns identified in the AIS dataset, allowing ships to recognize spoofing-like conditions within minutes of onset.

6.2 Cross-referencing with GNSS Quality Metrics

Integration of basic GNSS diagnostics (e.g., signal-to-noise ratio, satellite count, and dilution of precision) enables vessels to differentiate between sensor drift and external interference. For instance, persistent navigation anomalies occurring while GNSS SNR remains above 40 dB-Hz suggest an artificial signal source rather than environmental obstruction (Psiaki and Humphreys, n.d.).

6.3 Incident Response and Data Sharing

Detected anomalies can be logged and transmitted to coastal monitoring centers or nearby vessels through AIS message extensions. Aggregated anomaly reports would allow regional authorities to identify interference “hot zones” and investigate recurring spoofing events. This decentralized reporting model offers a low-cost early-warning mechanism without requiring modifications to satellite infrastructure.

Together, these strategies provide a scalable foundation for maritime spoofing detection and mitigation. By combining onboard rule-based monitoring with lightweight data exchange, vessels can maintain navigational integrity and contribute to a broader situational awareness network, reducing the operational risks associated with localized GNSS interference.

The integration of AIS-based anomaly detection with ground-validated GNSS diagnostics establishes a comprehensive method for identifying spoofing risk in maritime navigation. By combining vessel-level behavioral analysis with regional signal verification, the study bridges empirical observation and applied defense strategy. This connection forms the foundation for a broader discussion on how localized monitoring can enhance maritime cybersecurity resilience.

7. Conclusion

This research investigated GPS spoofing vulnerabilities in maritime navigation through a dual analysis of AIS vessel trajectories and GNSS reference station data along the U.S. West Coast. The AIS analysis revealed distinct clusters of anomalous motion, such as speed spikes, erratic rotations, and course-heading deviations, concentrated near dense port regions. In contrast, GNSS reference logs from NOAA’s CORS network showed continuous, high-quality signal reception with no evidence of system-wide degradation.

The contrast between these datasets indicates that navigation irregularities are not caused by satellite instability but by localized interference, reflection, or deliberate spoofing within port environments. These findings suggest

that maritime spoofing and interference effects are geographically contained and operational in nature, emphasizing the importance of regional detection over global corrections.

Although the dataset analyzed in this study originates from December 2020, the research remains highly relevant to the 2026 maritime cybersecurity landscape. Since 2020, documented GNSS spoofing and interference incidents have increased in frequency and geographic scope, particularly in the Black Sea, Eastern Mediterranean, Red Sea, and other strategically important maritime regions. These events have demonstrated that vessel navigation systems remain vulnerable to manipulation despite advances in maritime cybersecurity awareness. While the data examined in this study are historical, the fundamental weaknesses of unauthenticated civilian GNSS signals have not been fully resolved. Therefore, the anomaly detection methods and mitigation strategies proposed here continue to address an active and evolving threat facing commercial shipping and maritime infrastructure.

The proposed detection framework translates these insights into actionable measures: continuous onboard consistency checks, correlation with GNSS signal metrics, and distributed incident reporting. Together, these tools can enable early identification of spoofing events and support coordinated responses among vessels and coastal authorities.

Overall, the study demonstrates that combining vessel-level AIS behavior with regional GNSS diagnostics provides a robust and scalable foundation for improving maritime navigation security. This approach supports both operational awareness and long-term policy development aimed at safeguarding the integrity of global positioning systems in maritime domains.

Ethics declaration: This research used publicly available maritime Automatic Identification System (AIS) data and Global Navigation Satellite System (GNSS) reference station logs obtained from open government archives. No human subjects were involved, and no personally identifiable information was collected or analyzed. All data used in this study describe vessel movement and signal quality at an operational level and do not identify individual operators or crew members.

AI declaration: Artificial intelligence tools were used in a limited capacity to assist with language refinement, structural organization, and clarification of technical explanations during the preparation of this manuscript. The AI-generated content was used primarily to improve readability, rephrase existing material, and suggest wording for summaries and explanatory sections. All technical analysis, data processing, methodology design, interpretation of results, and conclusions were developed by the authors. The authors reviewed, edited, and validated all AI-assisted text to ensure accuracy and alignment with the research findings. No AI tools were used to generate data, conduct analysis, or produce experimental results.

References

A. Androjna and M. Perkovič, “Impact of Spoofing of Navigation Systems on Maritime Situational Awareness,” Transactions on Maritime Science, vol. 10, no. 2, pp. 361–373, Oct. 2021, doi: https://doi.org/10.7225/toms.v10.n0z2.w08.

Bhatti, J. and Humphreys, T.E. (2017). Hostile Control of Ships via False GPS Signals: Demonstration and Detection. Navigation, 64(1), pp.51–66. doi:https://doi.org/10.1002/navi.183.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. and Lachapelle, G. (2012). GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. International Journal of Navigation and Observation, [online] 2012, pp.1–16. doi:https://doi.org/10.1155/2012/127072.

Psiaki, M. and Humphreys, T. (n.d.). GNSS Spoofing and Detection. [online] Available at: https://radionavlab.ae.utexas.edu/images/stories/files/papers/gnss_spoofing_detection.pdf.

Spravil, J., Hemminghaus, C., Merlin von Rechenberg, Padilla, E. and Bauer, J. (2023). Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring. Journal of Marine Science and Engineering, 11(5), pp.928–928. doi:https://doi.org/10.3390/jmse11050928

T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, and P. M. Kintner, Jr., “Assessing the spoofing threat: Development of a portable GPS civilian spoofer,” in Proc. ION GNSS, Savannah, GA, 2008, pp. 2314–2325.

US (2025). NGS Weekly - NGS News - National Geodetic Survey. [online] Noaa.gov. Available at: https://geodesy.noaa.gov/web/news/.