

Article

Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring

Julian Spravil ^{1,†}, Christian Hemminghaus ¹, Merlin von Rechenberg ^{1,2} , Elmar Padilla ¹ and Jan Bauer ^{1,*} 

¹ Fraunhofer FKIE, Cyber Analysis & Defense, Fraunhoferstraße 20, 53343 Wachtberg, Germany

² Institute of Computer Science 4, University of Bonn, Friedrich-Hirzebruch-Allee 8, 53115 Bonn, Germany

* Correspondence: jan.bauer@fkie.fraunhofer.de; Tel.: +49-241-8021465

† Current address: Fraunhofer IAIS, NetMedia, Schloss Birlinghoven 1, 53757 Sankt Augustin, Germany.

Abstract: Today's maritime transportation relies on global navigation satellite systems (GNSSs) for accurate navigation. The high-precision GNSS receivers on board modern vessels are often considered trustworthy. However, due to technological advances and malicious activities, this assumption is no longer always true. Numerous incidents of tampered GNSS signals have been reported. Furthermore, researchers have demonstrated that manipulations can be carried out even with inexpensive hardware and little expert knowledge, lowering the barrier for malicious attacks with far-reaching consequences. Hence, exclusive trust in GNSS is misplaced, and methods for reliable detection are urgently needed. However, many of the proposed solutions require expensive replacement of existing hardware. In this paper, therefore, we present MARitime Nmea-based Anomaly detection (MANA), a novel low-cost framework for GPS spoofing detection. MANA monitors NMEA-0183 data and advantageously combines several software-based methods. Using simulations supported by real-world experiments that generate an extensive dataset, we investigate our approach and finally evaluate its effectiveness.

Keywords: GPS spoofing; anomaly detection; NMEA-0183; Maritime Cyber Security; GNSS; cyber and electromagnetic activities



Citation: Spravil, J.; Hemminghaus, C.; von Rechenberg, M.; Padilla, E.; Bauer, J. Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring. *J. Mar. Sci. Eng.* **2023**, *11*, 928. <https://doi.org/10.3390/jmse11050928>

Academic Editors: Marko Perkovic, Lucjan Gucma and Sebastian Feuerstack

Received: 29 March 2023

Revised: 20 April 2023

Accepted: 24 April 2023

Published: 26 April 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Commercial seagoing vessels, such as container ships, bulk carriers, and tankers, are among the most important means of transportation today. However, they are easy targets for different attacks in the domain of cyber and electromagnetic activities (CEMA), motivated by industrial espionage and economic sabotage to piracy and terrorism. Since the impact of such attacks can pose serious threats not only to the economy but also to humans and the environment, safety and security are of paramount importance. Because the shipping industry as a whole is moreover responsible for the international supply of goods, there is a serious risk of major economic and ecological damage caused by CEMA targeting this industry, which is by no means immune to such attacks [1,2]. Therefore, it must be protected effectively, as recognized in the last two decades by governments and organizations placing Maritime Cyber Security on their agendas.

Navigation in shipping has been fundamentally changed by the advent of civil global navigation satellite systems (GNSSs), the best-known representative of which is the Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS). Today's maritime systems are increasingly computer-aided and heavily depend on the availability of GNSS for accurate positioning, navigation, and timing (PNT), which is usually complemented by highly interconnected sensors within integrated bridge systems (IBSs) on board modern vessels. Despite significant efforts by all GNSS operating stakeholders to upgrade security or deploy new, more secure generations of systems, civil GNSSs currently do not have sufficient security measures as practically demonstrated in the case of GPS [3]. However, cryptographically authenticated GNSS signals have also recently been shown to remain vulnerable to spoofing attacks [4].

The fact that GNSS satellite signals are relatively weak when being received on the Earth's surface makes them intrinsically vulnerable. Thus, an attacker can effectively carry out jamming attacks to prevent a GNSS receiver from processing legitimate signals. Nonetheless, more and more trust is being placed in GNSSs in a risky manner.

While jamming attacks might be easily detected by the crew, since they would cause obvious failures in navigational instruments, so-called GNSS spoofing attacks can remain undetected and, thus, be much more harmful. In a spoofing attack, an adversary generates counterfeit signals, which are difficult to distinguish from legitimate ones and cause receivers to incorrectly calculate position and/or timing. Particularly in maritime off-shore scenarios, attacks on PNT are often more difficult to detect and, thus, perhaps more threatening. Because the majority of the previous work refers to GPS [3,5–8], we also focus, without loss of generality, on GPS and GPS spoofing in this paper. However, other navigation satellite systems, e.g., Galileo, GLONASS, and BeiDou, are all based on the same principle of measuring time differences in signal propagations from satellites. Thus, methods used in this paper can, in general, be transferred to other satellite navigation systems.

Vessels have a long service life. Since maritime systems are strongly embedded, accordingly outdated technologies are used that are usually prone to various emerging types of CEMA attacks. Because particularly spoofing attacks can be very devastating, appropriate countermeasures are urgently needed. Several methods for detecting such attacks exist, as surveyed in [9]. However, the proposed methods cannot be applied to existing receivers without limitations in many cases. They often require expensive and cumbersome hardware upgrades or replacements that are usually evaluated as uneconomical when assessing cybersecurity risks. Taking legacy systems into account, we believe that it is essential to consider efficient software-based approaches for the detection of GPS spoofing, which can be seamlessly retrofitted into those systems.

In this work, therefore, we propose a modular framework for GPS spoofing detection in the maritime sector based on anomaly detection. We advantageously combine different software-based methods and operate solely on network traffic. Thereby, this approach enables cost-effective retrofitting, either by software updates or by additional low-cost off-the-shelf hardware devices. In summary, our contributions are as follows:

- We identify GPS spoofing detection methods from the literature that can operate on data provided by the NMEA-0183 and can be implemented at low cost;
- we propose a MAritime Nmea-based Anomaly detection framework (MANA) that incorporates these methods;
- we generate and provide an extensive dataset including diverse spoofing attacks; and
- we finally evaluate and compare the effectiveness of spoofing detection methods and demonstrate the potential of their combination to compensate for each other's weaknesses.

2. Maritime Systems On Board Vessels

A reliable and accurate position and time estimation is crucial for navigation and the situational picture in IBSs. Hence, for redundancy, the majority of vessels are equipped with two GNSS devices [10] that are supplemented by a variety of additional sensors, networked in a maritime system [11–13]. A typical system architecture is exemplarily shown in Figure 1, and a brief introduction to these systems with a focus on GPS integration is given below.

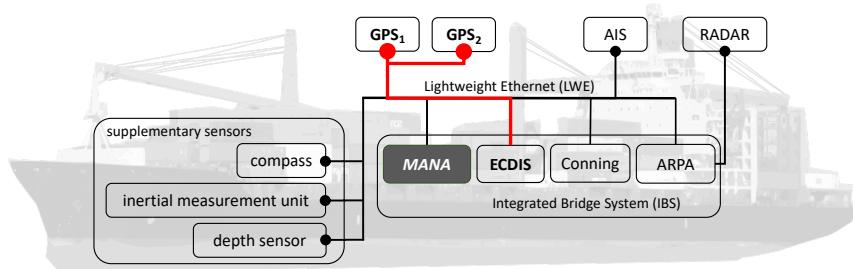


Figure 1. Simplified system architecture of a maritime system. There are multiple GPS receivers on board, along with supplementary sensors, providing navigational data to the IBS via the IP-based Lightweight Ethernet (LWE) [13]. Because the data provided by GPS receivers (red) cannot necessarily be assumed to be trustworthy, the derived PNT information must be verified, which can be achieved using our approach, MANA (gray), implemented as an additional detector component in the IBS.

2.1. GPS Dependency of Nautical Electronics

The PNT data generated by GPS receivers are strongly involved in navigation. In addition, derived measurements, e.g., speed and heading, are used for multiple purposes in maritime systems. The electronic chart display and information system (ECDIS) integrates those measurements into a digital chart to provide a situation picture to navigators to support conning decisions. For collision avoidance, the radio-based automatic identification system (AIS) broadcasts vessels' positions and course information to other maritime entities. Radar makes use of PNT, since automatic radar plotting aid (ARPA) is illustrated relative to the vessel's location and orientation. Autopilots need PNT to calculate necessary course corrections.

Since PNT data are used by many navigational aids, the impact of unreliable and manipulated information can be devastating. Recent incidents show that minimal course deviations may lead to groundings with costly global financial losses [14]. Hence, in the case of CEMA, alternative position estimation and tracking systems are recommended [15].

2.2. NMEA-0183 and Maritime System Networks

Distribution of nautical data on board vessels nowadays relies on Ethernet (IEEE 802.3 product family) as a well-established network standard. The NMEA-0183 standard specified by the National Marine Electronics Association (NMEA) defines the earlier used transmission and encoding of nautical data via 4800-baud serial data bus interfaces. Although the original serial transmission of NMEA-0183 is a legacy technology, the ASCII-based encoding and message format of nautical data via so-called NMEA sentences is still used in modern IP-based protocols. *NMEA over IP* encapsulates sentences in UDP datagrams or TCP streams to distribute nautical information via uni-, multi-, or broadcasts. A more complex IP-based protocol is Lightweight Ethernet (LWE), which is standardized in IEC 61162-450 [16]. In addition to the use of NMEA sentences, LWE defines multicast groups and protocol extensions for the distribution of data files in the maritime system. Nautical devices and sensors, e.g., GNSS receivers, can be integrated into the multicast using additional network hardware, i.e., LWE gateways.

Other protocols, e.g., NMEA 2000 and NMEA OneNet, use more transmission-efficient binary encoding schemes. Although not human-readable, the encoded information is almost equal to that of ASCII-based NMEA sentences. Thus, without loss of generality, we will focus on ASCII-based NMEA in our concept and implementation. With respect to GNSS, NMEA sentences moreover not only contain functional data, e.g., latitude and longitude coordinates, elevation and azimuth angles, and time but also quality information, i.e., carrier-to-noise density (C/N_0), the number of visible satellites, and their IDs.

Overall, the multicast distribution of GPS-related and other sensor data via NMEA sentences in the network enables system-wide monitoring, cf. Figure 1. This is leveraged by our framework, MANA, in order to detect anomalies in PNT streams that are possibly caused by spoofing.

3. GPS Spoofing

GPS signals are an easy attack target. Due to the low signal strength at the Earth's surface, the signals can be effortlessly blocked [17]. In addition, the civil GPS lacks encryption, authentication, or any further security measures to protect the signal integrity. In fact, the data structure, modulation schemes, and spreading codes are publicly available [18]. Altogether, these peculiarities enable jamming and spoofing. In a jamming attack, adversaries try to suppress original GPS signals using artificial interference. As a result, benign signals become unrecognizable to receivers and can no longer be used for PNT. However, receivers are usually aware of whether they are subject to jamming attacks and can react accordingly [17]. An overview of the threat jamming poses to the maritime domain and the main countermeasures techniques is provided in [19]. With spoofing attacks, the situation is fundamentally different. In such attacks, adversaries generate signals that mimic legitimate signals. Often, their goal is to deceive the targeted receiver without being detected so that incorrect PNT estimates are calculated.

3.1. Maritime GPS Spoofing

Besides a variety of cyber and CEMA threats against a vessel in the maritime context (cf. e.g., [20]), GPS spoofing attacks represent a major threat and attract attention from researchers, practitioners, and industry. Those attacks are known to be feasible and seriously affecting maritime navigation [3]. Recent reports also highlight the risk posed by GPS jamming and spoofing attacks [15,21]. In 2017, a total of 25 ships reported the wrong position near the port of Novorossiysk, which pointed to the Gelendzhik airport [22]. It is suspected that GPS spoofing caused this incident.

In fact, a maritime environment makes the success of a spoofing attack more likely than in other domains. At sea, there are only a few landmarks to correlate GPS positions with derived information. Without a regular position input, alternative measures, such as dead reckoning, lose their accuracy over time. Therefore, smooth long-term attacks are difficult to detect. Additionally, navigators often unconsciously tend to blindly trust their devices [23]. In the domain of maritime navigation, the risk of attacks on GNSS has also long been noticed by the International Maritime Organization (IMO). The urgent demand for adequate integrity monitoring was first recognized in 2001 within the resolution MSC.915 (22) [24], and further resolutions followed. A compact summary of the evolution of the IMO integrity concepts, such as e-Navigation, can be found in [25]. The need for resilient GPS is also part of these concepts. The Department of Homeland Security provides the Resilient PNT Conformance Framework [26], with four levels of resilience reflecting the users' needs. In this context, our framework can be classified as a level 1 resilient PNT but offers the potential to reach level 2 by adding a complementary PNT source (cf. Section 4.2).

3.2. Attack Model and Scenarios

To spoof GPS receivers, an attacker can employ different techniques. Jafarnia-Jahromi et al. [5] distinguish between three types of attackers with increasing complexity. The attackers' signals range from simple unsynchronized signals to complex, near-authentic signals with even matching angles of arrival. Similarly, we define three attacker types, namely the replay attacker (A_R), the meaconing attacker (A_M), and the simulator attacker (A_S). An overview of the attackers is given in Figure 2.

The simplest attacker is A_R . Equipped with a single antenna, the attacker can generate arbitrary GPS signals or record original ones. These signals are then (re)played at a later point in time. Thus, the signals are usually not synchronized to real GPS signals [5]. Furthermore, except for superimposed signal power, no specific signal takeover strategy is performed. Attacks of this category were already demonstrated two decades ago [27].

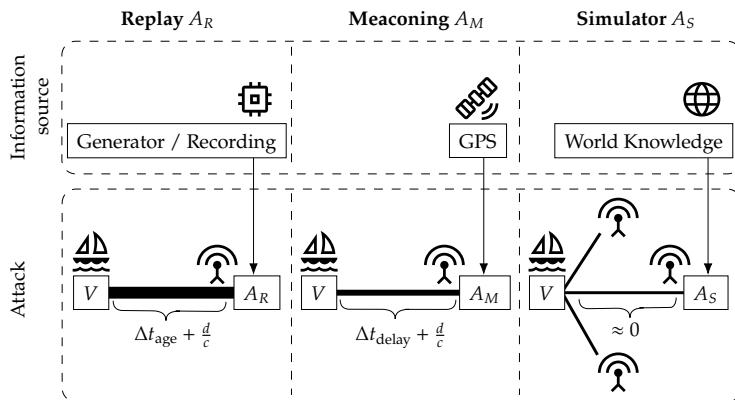


Figure 2. Illustration of the three attacker types (A_R , A_M , and A_S), their information source, and a visualization of the different attack modes on victim V . The signal strength as received by V is reflected by the line strength, ranging from superimposed (left) to normal levels (right). For each mode, the additional pseudo-distance caused by the attacker is shown, where Δt_{age} is the age of the recorded signals, Δt_{delay} is the signal processing delay, d is the actual distance between V and the attacker, and c is the propagation speed of the radio signal.

The meaconing attacker A_M can additionally receive and process genuine GPS signals and react to them with a small delay. The simplest attack this attacker can execute is meaconing, i.e., replaying authentic signals in near-real time. To actively break the lock of a receiver to the authentic satellites, the attacker can execute a jamming attack beforehand. A GPS receiver has a lock when a stable reception from a set of satellites required for PNT is established. Initially, the attacker, therefore, uses signals with a high signal strength to overpower the legitimate signals and to force the receiver to lock onto the spoofed signals. Once the attacker has obtained the lock, i.e., controls all the signals at the receiver, the spoofing power can be reduced.

Meaconing can also be effective against encrypted signals, as the signal content remains unaltered [8]. Advanced forms of meaconing allow spoofing of arbitrary positions by individually delaying each signal [4]. However, a lock on all counterfeit signals is not guaranteed and depends on factors such as the target's speed [28]. As a consequence, the resulting position of the victim is not always the attacker's position and to some extent unpredictable. This issue can be addressed by relaying the authentic signals over the Internet to the attackers' transmitter near the victim, as demonstrated with consumer hardware [29].

Besides real-time signal processing, the simulator attacker A_S can operate multiple antennas to match the original signal alignments. However, such a setup is costly and brings limitations in terms of antenna placement and effective range [5]. The precise position and other motion properties of the victim have to be known, enabling highly accurate signal construction. To manipulate the victim's receiver, the attacker performs a seamless takeover by matching the legitimate signals and carefully increasing the signal strength [7,8,18]. Real-world experiments involving a single-antenna A_S were performed in a lab environment [6] and on board a yacht [3].

4. GPS Spoofing Detection

The first spoofing detection considerations and techniques were already mentioned in the 1990s by MITRE [30]. A theoretical basis was given by Warner and Johnston [17] proposing different techniques, e.g., based on signal strengths or signal time of arrival (TOA) monitoring, to check the integrity of PNT data and to mitigate possible attacks. Following these theoretical considerations, a variety of practical implementations and improvements gradually emerged, beginning with Receiver Autonomous Integrity Monitoring (RAIM) [31]. A comprehensive overview of existing methods and techniques, as well as their complexity and effectiveness, that have been presented over the years can be found in [5,8,9].

The variety of anti-spoofing techniques can be classified according to the layer at which the countermeasure can be applied. For this purpose, we differentiate between system, hardware, firmware, and software layers. An overview of existing approaches for GPS spoofing countermeasures is provided in Table 1. Note that software-based approaches can also be implemented in firmware, but that involves increasing complexity and costs. Because the goal of our solution is to be retrofittable with low effort and cost, we focus on the software-based approaches, which are briefly presented in the following subsection and discussed in terms of their applicability in the maritime context.

Table 1. Classification of known GPS spoofing detection techniques with decreasing complexity of retrofitting per class and their effectiveness against different attack scenarios.

Spoofing Countermeasure Method			
		Replay (A_R)	Meaconing (A_M)
		Simulator (A_S)	
System	Symmetric encryption of full spreading code (e.g., [8,32])	●	●
	Spread spectrum security code (e.g., [32])	●	●
	Navigation message authentication (e.g., [32,33])	●	●
Hardware	L1/L2 power level comparison (e.g., [34,35])	●	●
	L1/L2 power level code phase comparison (e.g., [34])	●	●
	DOA monitoring (e.g., [36,37])	●	●
Firmware	Synthetic antenna array (e.g., [38])	●	●
	Signal strength monitoring (e.g., [17,39])	●	○
	Doppler monitoring (e.g., [40,41])	●	●
	Code and phase rates consistency check (e.g., [34])	○	○
	TOA monitoring (e.g., [17,42])	○	○
	PRN code and data bit latency (e.g., [43–45])	●	○
	Auxiliary peak tracking APT (e.g., [18])	○	●
	Signal quality monitoring (e.g., [46–48])	○	●
	Distribution analysis of correlator output (e.g., [49,50])	○	●
	C/N ₀ Monitoring (CNM) (e.g., [34,39])	●	○
Software	Physical Cross-Check (PCC) (e.g., [51–54])	○	○
	Clock Drift Monitoring (CDM) (e.g., [8,18])	●	○
	Ephemeris Data Validation (EDV) (e.g., [34,55])	●	○
	Pairwise Distance Monitoring (PDM) (e.g., [7,56])	●	●

Notation: Effective (●), semi-effective (○), and ineffective (○) GPS spoofing detection regarding individual attacker models defined in Section 3.2, cf. Figure 2.

4.1. Software Controls and Related Work

Software methods are flexible, easy to retrofit, and, thus, also cost-effective. In the literature, there are methods for software-based spoofing detection, such as anomaly detection approaches that monitor the C/N₀ [34,39] or internal clock drifts [8,18]. Other approaches validate ephemeris data [34,55] or implement cross-checks with physical constraints [51,52]. Similar to methods from other categories, the effectiveness of these approaches is diverse, as shown in Table 1. Advanced attackers cannot be detected by most software-based methods. However, they still provide reliable detection for replay and meaconing attackers.

An effective approach is presented by Tippenhauer et al. [7], which requires multiple (at least two) GPS receivers. It is based on the fact that the pairwise distances between multiple receivers in a static constellation are constant with regard to the respective deter-

mined position of each receiver (except for GPS inaccuracies). Because a second receiver is available on most commercial vessels [10], this particular approach can be easily implemented in the maritime environment, as already suggested by Zalewski [56]. With high-quality receivers typically used in maritime systems, we expect the inaccuracy of position determination to be reasonably low, which presumably increases the detection probability of this Pairwise Distance Monitoring (*PDM*) approach. Zalewski applied Tippenhauer's approach to the maritime context. Using a mathematical model and simulation, he shows that it is practically not feasible to spoof multiple GPS receivers by a single transmitter so that their relative distance remains. Recently, another approach using multiple receivers was presented in [57]. Instead of considering the effects on position, the authors focus on the time provided by GNSS to protect electrical substations in the energy sector. Similar to our approach, they rely on NMEA sentences, but they are limited to the *PDM* method for detecting spoofing attacks.

In [58], software-based approaches for anomaly detection using GPS spoofing in the context of unmanned aerial vehicles (UAVs) are explored. The authors propose machine-learning algorithms and show that promising detection results can be achieved with different one-class classifiers, which require only non-anomalous data for training. The work represents an interesting approach, the methods of which can, in principle, complement our framework. For their evaluation, they created and shared a dataset of three UAV flight recordings, i.e., one benign, one with GPS jamming, and one with spoofing [59]. However, the purpose-built dataset is restricted to timestamped positions of a single receiver and, thus, inappropriate for the analyses of all the above-mentioned *PDM* methods. In the automotive sector, Lemieszewski [53] recently dealt with the detection of spoofing attacks. The author uses a *PCC* method and correlates the GNSS position estimates with the speedometer of the vehicle, also using NMEA sentences.

A spoofing detection and mitigation approach for the maritime context is proposed in [60]. The authors use RAIM [31] in combination with a *PCC* method based on a motion model of a ship in order to detect offsets to the predefined route, while their mitigation mechanism is based on a genetic algorithm. In addition to route information, their motion model requires other sensor inputs. Our approach, in contrast, entirely relies on NMEA data provided by GPS devices and does not require route information. Nonetheless, the method of Singh et al. could in general be applied in conjunction with our framework.

Similar to our approach, Lee et al. [61] base their spoofing detection on NMEA data but in the context of smartphones. In a physical laboratory environment, the authors first generate spoofing signals that dictate positions on a specific route. These signals are then processed by a stationary GPS receiver, and the effect is investigated. The authors suggest monitoring position, velocity, and time for changes or cross-referencing the results with other sensor information. Another method they describe is to check the relationship between the signal strength and the distance to the corresponding satellite. Lastly, a comparison with other positioning systems based on the residuals of the position calculation is suggested. However, their investigation focuses solely on static scenarios, which limits their general applicability to real-world systems.

In summary, in the field of GNSS spoofing detection, several related works exist that build on software-based methods and, among them, some that obtain their data also from NMEA messages. However, these works often focus on one specific approach. Our work, in contrast, presents a holistic, modular framework that adapts and combines different methods of existing work, offering flexible configuration and tailoring them to the needs of ships in the maritime domain. The later evaluation (cf. Section 7) will show that this combination is necessary to cope with the entire attack space. Before presenting our framework in Section 5, the following paragraph first concludes by briefly discussing complementary approaches from the area of resilient PNT that are orthogonal to our work.

4.2. Complementary Approaches

In addition to the countermeasures presented above that are limited exclusively to the GNSS domain, there are novel approaches for alternative localization technologies. Those technologies can also be used to detect anomalies and potential attacks against GNSS-based positioning. In this context, Olicheri et al. [62] propose a GPS spoofing detection and localization approach that leverages the Public Land Mobile Network (PLMN) infrastructure of terrestrial mobile communication. In [54], the authors even extend their work to the use of WiFi networks and present a crowd-sourced approach. However, this promising work, which leverages the existence of existing land-based infrastructure, is not applicable at sea.

Similarly, in the maritime domain, the R-Mode (Ranging Mode), which is currently under development, is based on so-called signals of opportunity, cf. [63]. These are independent terrestrial signals from existing maritime infrastructures such as AIS, Very high frequency Data Exchange System (VDES), or other maritime radio signals that can be leveraged for ranging. Worldwide coverage of up to 40% of all vessels is predicted [64]. Under good conditions, i.e., in the middle of three R-mode transmitters, a real-time horizontal positioning accuracy of 95% at 12 m could be achieved in the Baltic Sea testbed [65].

Furthermore, Naus et al. [66] show that maritime navigation radar can be used to detect anomalies in position determination. However, the feasibility of radar navigation, in general, depends massively on the availability of characteristic echo marks. The performance at the open sea is therefore questionable. Moreover, terrain navigation is extensively used by underwater vehicles and demonstrated to be feasible for surface vessels in coastal waters to improve GNSS-based navigation [67].

In relation to our approach introduced in this paper, the alternative technologies mentioned represent complementary countermeasures that can be successfully combined. Such a combination, i.e., secured GNSS information correlated with nautical data from additional sensors and augmented by terrain, radar, or PLMNs localization techniques, has great potential not only to mitigate GNSS spoofing attacks but to entirely prevent them.

5. NMEA-Based GPS Spoofing Detection Framework

Building on a versatile selection of multiple existing software approaches presented in the previous section and leveraging the availability of PNT and NMEA data in the network, our framework MANA aims to provide low-cost yet effective integrated integrity checks as a countermeasure against GPS spoofing. Moreover, the framework allows for comprehensive comparison of the selected approaches to find out if a combined solution can compensate for their individual deficiencies. MANA, which is modularly implemented in Python 3, relies on standardized NMEA sentences. Thus, it enables generic, very flexible, and easily retrofittable deployment by adding a detector component at a central position in the maritime network, cf. Figure 1. To the best of our knowledge, no directly related work provides a comparable framework. In the subsequent sections, we will briefly describe MANA's concept and the essential details of individual methods.

5.1. Concept of MANA

The concept of our framework and its data processing workflow are visualized in Figure 3. A stream of NMEA sentences, dispatched by at least two GPS receivers within a network, is taken as input. Alternatively, recorded network trace files can be used as input. For each detection method, a set of fields within NMEA sentences is defined that are relevant to the individual detection approach. These fields are continuously monitored such that every state change triggers the corresponding detection method(s). The relevant required information can be obtained from different and partially redundant NMEA sentences generated by GPS receivers. However, in the end, the set of required sentences can be reduced even to the three GPS-related types \$GPGGA, \$GPRMC, and \$GPGSV. An overview of the contained information, its relationship to the respective detection methods, and alternative NMEA sentences is given in Figure 4.

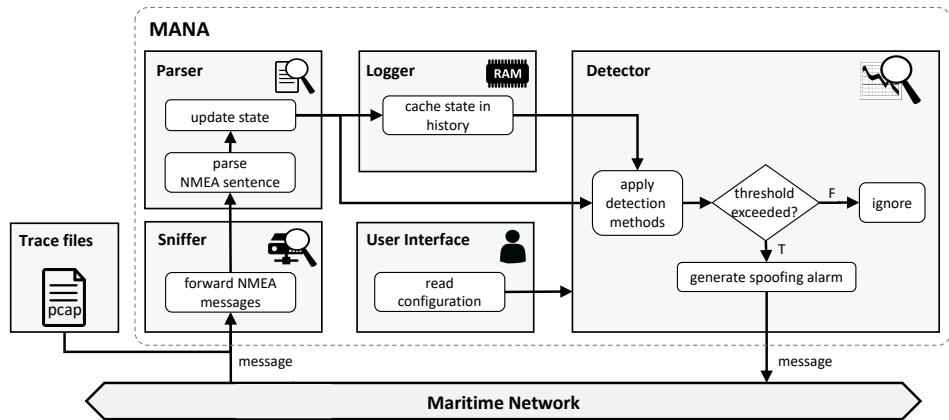


Figure 3. Conceptual overview of the GPS spoofing MANA framework and its components.

The detector generates an alarm if any of the methods indicates potential spoofing. Based on individual methods as basic building blocks, our framework allows the implementation of more complex and sophisticated detection, i.e., by composing the outputs of those methods. This offers great potential to further increase the overall detection capability; however, a detailed investigation is out of the scope of this paper. In order to evaluate if the different methods can compensate for each other's weaknesses, a simple strategy for combining different methods is nonetheless elaborated in Section 7.2.

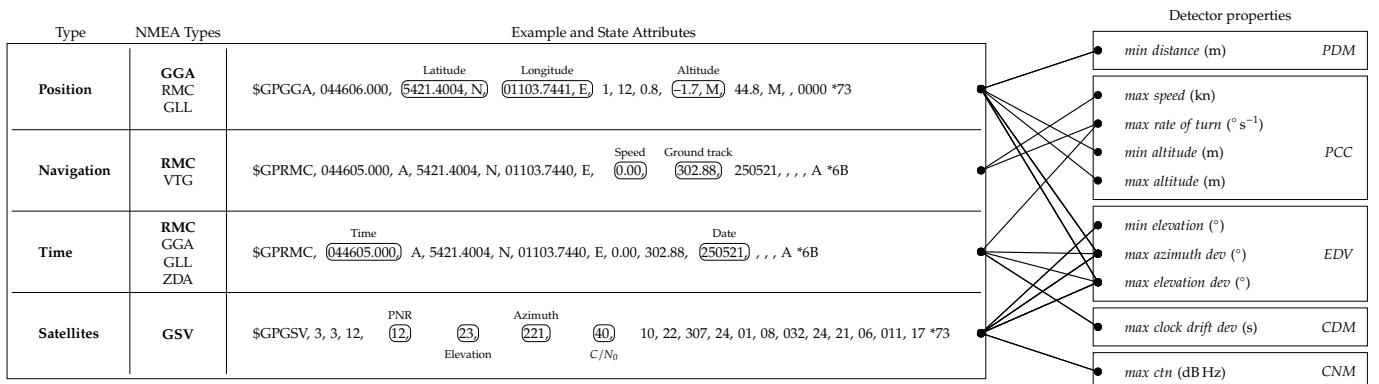


Figure 4. Visualization of the relationship (indicated by the lines) between state attributes extracted from NMEA sentences and the detection methods. The minimal working set of NMEA types is marked in bold. However, the other listed types can also be used as alternatives. Note that the asterisk (*) is the separator symbol for the following checksum in the ASCII notation of NMEA sentences.

5.2. Methods for NMEA-Based Detection

MANA comprises five software-based detection methods from the literature, introduced in Section 4, namely PCC, PDM, EDV, CDM, and CNM (cf. Table 1 and Figure 4). With the assumption that the data are smooth or predictable under normal conditions but not in case of a spoofing attack, these methods are implemented using thresholds.

Physical Cross-Check (PCC): The PCC method is subdivided with respect to the physical features considered for the respective cross-check, i.e., speed over ground (SOG) (PCC_{sog}), rate of turn (ROT) (PCC_{rot}), and height above sea level (PCC_{height}). While SOG and ROT are expected to stay within certain limits, these limits can be exceeded in the event of a perceived spoofing attack. Sudden jumps in position can result in an unreasonably high SOG and ROT if the distance or angular deviation from the course is extreme enough. To restrict the attackers' possibilities, we use maximum thresholds for PCC_{sog} and PCC_{rot} (cf. Figure 4), which must be plausibly selected for the respective vehicle. While the SOG threshold should be set slightly higher than the maximum speed of the vehicle, more tolerance is required

for the ROT threshold. The ROT is subjected to a measurement error, which is particularly high when the vessel is slowly or not moving. Therefore, it is useful to consider only ROT measurements when the SOG exceeds a certain threshold, e.g., half of SOG threshold. The altitude is expected to be close to sea level. Thus, static thresholds above and below the sea level are defined for the *PCCheight* method (cf. Figure 4).

Pairwise Distance Monitoring (PDM): PDM monitors the static formation of two receivers and requires position data simultaneously recorded for each receiver, but these are generally not synchronized. Conventional GPS receivers only update positions with a frequency of 1 Hz. Hence, the states of the two receivers have to be aligned in time. For this purpose, one of the receivers is selected as a reference. Then, the other receiver's state is linearly interpolated between its temporally adjacent values, i.e., the time, latitude, and longitude immediately before and after the corresponding reference. Moreover, we use an exponential moving average (with $\alpha = 0.1$) to reduce the effects of small-scale noise in the position sequences. Once the estimates of both receivers are aligned, the measured distance between the geographic position of the receivers can be derived. A spoofing attack is detected if the distance is smaller than the minimum threshold (cf. Figure 4).

Ephemeris Data Validation (EDV): Satellite positions are to some extent predictable. As a data source, we use so-called two-line elements (TLEs). If the TLEs are up-to-date, the predicted satellite positions can be used to validate the estimated ones. However, the decrease of TLEs' accuracies with increasing age [68] and the integer accuracy of NMEA sentences with respect to elevation and azimuth need to be considered. This is checked by the EDV method by defining a maximum allowed deviation for both angles. Furthermore, the elevation of all satellites needs to be above a static minimum threshold (cf. Figure 4), ensuring that they are actually visible to the receiver, since implausible constellations indicate potential attacks.

Clock Drift Monitoring (CDM): With regard to CDM, a linear clock drift Δt of each device is assumed, which is reasonable for a certain interval in time. The drift of an individual device can be derived by continuously comparing the received GPS time with the local system time. If enough drift measurements are available, a drift function is derived by a linear regression providing the expected clock drift Δt_{exp} for a given point in time. The difference between Δt_{exp} and Δt is then compared with the predefined threshold (cf. Figure 4) and, in cases where deviation of the clock drift exceeds this threshold, a potential spoofing attack is indicated.

C/N₀ Monitoring (CNM): This method monitors carrier noise density and derives indications of possible attacks in cases where the noise level exceeds the given threshold (cf. Figure 4). An evaluation of the CNM detection method requires real-world data or a simulation that includes a realistic signal propagation model with the associated random processes, particularly *C/N₀*. Our simulation environment, which is used for the evaluation (in Section 7), does, however, not include such a signal propagation model. Thus, CNM is excluded from the later evaluation.

6. Simulation Environment and Dataset

For ease of feasibility and better reproducibility, we use simulations to evaluate the effectiveness of our approach but collected real data in experimental field trials to (i) calibrate simulation models and (ii) appropriately determine thresholds for the detection algorithms, i.e., for the parametrization of MANA. For the latter, it is important to find the right balance between triggering false alarms (false positives) and missing the detection of spoofing attacks (false negatives). For this purpose, we carried out two experiments, a static and a dynamic scenario. In the first experiment (Section 6.1.1), a stationary measurement was conducted to collect static GPS tracks that enable trace-based modeling of GPS errors in our later simulation. In the second experiment (Section 6.1.2), we used two mobile receivers moving in a static formation, i.e., at a fixed distance to each other, and continuously collected all data provided via NMEA sentences. The goal of the second experiment was to record the clock drift and position measurements of the GPS receivers, both for modeling in

the simulation and to support the determination of thresholds for clock drift and distance between GPS receivers, required for the *CDM* and *PDM* detection methods (cf. Figure 4).

6.1. Simulation Environment

We use an in-house simulation environment for maritime networks including various sensor information, such as course over ground, heading, compass, and AIS, with a special focus on GPS and its spoofing. The simulation environment is capable of simulating multiple ships, where each ship calculates its current position and time by triangulation based on the algorithm presented in [69]. Physical vessel-related parameters such as velocity and turn rate were set to be appropriate for the commercial seagoing vessels that we consider in this paper. The values used for the evaluation are listed under the category *Ship* in Table 2.

Table 2. Simulator properties and parametrization.

Category	Parameter	Value
Ship	Velocity	20 kn
	Rate of turn	$0.5 \text{ }^{\circ} \text{s}^{-1}$
	Number of GPS receivers	2
	Distance between GPS receivers	4 m
Clock error	Distribution	Gaussian
	μ	0.0012
	σ	0.0076
Clock drift	Drift per second	10.55 μs

For a more realistic simulation, we implemented a trace-based approach to model natural GPS noise using data from the first experiment, which is described in more detail in Section 6.1.1. In addition, random noise is artificially added to the time derived from GPS using a Gaussian distribution and a clock drift according to a second field experiment for which a detailed description follows in Section 6.1.2. According to the results of the experiment, we used a clock drift of ($\approx 10.55 \mu\text{s}/\text{s}$). Individual samples are further randomly distributed around the regression line according to the measured distribution, for which the parameters can be found in Table 2 under the category *Clock error*.

Furthermore, based on the results of the second experiment, which showed that an insufficient distance (of 2.5 m) between the receiver pair limits reliable detection, the distance was increased in the simulative evaluation. According to [6], a distance between 3 and 5 m can be considered to be feasible for the *PDM* method. Thus, we initially chose a distance of 4 m, cf. Table 2.

6.1.1. Modeling GPS Errors

To include natural GPS noise in the simulation, we chose a trace-based approach for modeling GPS errors. Therefore, we recorded representative GPS tracks files that can be used as trace files by the simulator. Thus, in the first experiment, two GPS receivers were installed in fixed positions, and their outputs, i.e., NMEA sentences, were recorded for multiple hours. The tracks of both receivers were analyzed regarding their spatiotemporal characteristics. As expected and shown in Figure 5a, we observed an averaged error in the position estimation of each receiver of up to several meters induced by natural noise and a varying C/N_0 . In addition, a clear temporal correlation of errors was observed for both distance and azimuth.

Especially when processing algorithms, e.g., detection methods (cf. Section 5.2), average the (simulated) GPS error in time, and this temporal correlation can have a crucial impact. Therefore, errors must not be randomly selected from the recorded tracks without considering their temporal correlation. Hence, we utilize recordings of static GPS receivers

as a noise source and construct a sequence of offsets (distance and azimuth) to the fixed position in our simulations. For each replication and each receiver, a random index is chosen within the sequence as a starting position. At each time step, this index is incremented by one, and the corresponding offsets are added to the simulated position measurement. In this way, individual error models are obtained for each receiver.

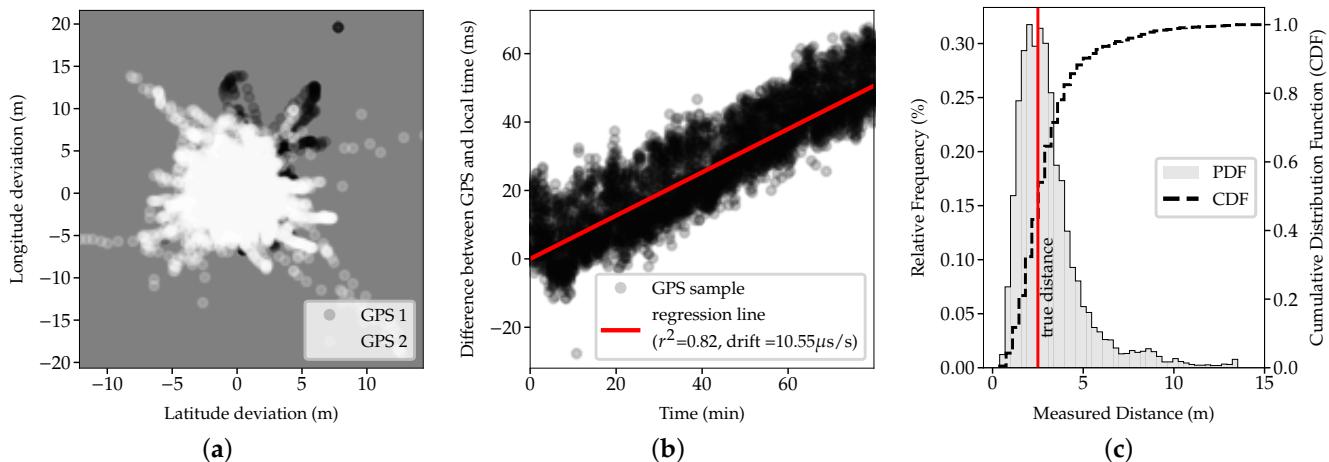


Figure 5. Experimental data from field trials to calibrate simulation models and derive thresholds for detection methods. (a) Simultaneous GPS measurements of two static receivers showing a measurement error of up to several meters. (b) The time difference between local and GPS time reveals a linear internal clock drift. (c) The PDF of measured distances between the position estimates of the two receivers is centered around the true distance.

6.1.2. Modeling Clock Drift

Besides the GPS error, modeling the clock drift is necessary for an evaluation of the different detection methods, particularly the CDM detection method. Additionally, the CDM detection method requires a threshold for the clock drift to distinguish between benign clock drift measurements and measurements that indicate a spoofing attack. Furthermore, we have to simulate multiple GPS receivers with a sufficiently large distance between them for the PDM detection method to work. Therefore, the second experiment was carried out to collect clock drift data and to determine suitable values for the GPS receivers' distance. For the second experiment, the tracks of two mobile GPS receivers were recorded. While moving the receivers, they had a fixed distance to each other of 2.5 m. The log file collected in the experiment provides rich GNSS-related data generated by both receivers, including various NMEA data.

Concerning the internal clock drift, a slight drift was found that is similar for both receivers (roughly 50 ms during 80 min). This drift is constant and, thus, grows linearly over time, as can be seen in Figure 5b, exemplarily shown for the first device. Nevertheless, there is a variance in the sequence of time samples, which can be attributed to the data processing within the receiver and for logging. Using linear regression, the clock drift is determined to be approximately $10.55\mu\text{s}/\text{s}$, which is typical for quartz oscillators as integrated into common devices. With the clock drift value and the measured variance, the clock drift can be accordingly modeled for realistic simulation, and a balanced threshold for the CDM detection method can be derived.

6.1.3. Calibrating Detection Thresholds

To determine suitable thresholds to parametrize various detection methods of MANA, we have to find a trade-off between false positives and false negatives. Due to the combination of different detection methods in our framework, occasional false negatives of individual methods are expected to be tolerated, because they are complemented by the indications of the other methods. Therefore, we use rather relaxed thresholds overall in

MANA. For the detection of spoofing based on *CDM*, the internal clock drift has to be known for each receiver. To this end, linear regression over a certain time interval could also be used by the detection algorithm in order to "learn" the clock drift. Based on the clock drift and distribution of measurements, the detection algorithm uses a threshold of ± 100 ms to identify possible spoofing while avoiding false positives.

PDM is based on monitoring the measured distance between two GPS receivers and comparing the measurements with the known real distance. Consequently, for the method to work, the distance between the GPS receivers has to be larger than the measuring error (cf. Figure 5a). Even though the second experiment shows that the distance derived from the positions is centered around the true distance (Figure 5c), it can be seen, at the same time, that the estimated distance can become very small due to the measurement errors of both receivers. Thus, it may falsely trigger *PDM*'s minimum threshold. Hence, the distance between the GPS receivers in the simulation has to be significantly larger than 2.5 m for the *PDM* detection method to work.

6.2. MARSIM Dataset

Based on the simulation environment, we generated a dataset, hereinafter referred to as the MARitime SIMulated (MARSIM) dataset. It consists of multiple scenarios (benign and attacked) with a duration of 120 s, provided as network traffic recordings (in packet capture (pcap) format). Each recording contains the NMEA sentences transmitted within the network of a single vessel heading north from a fixed point with constant velocity, cf. Table 2. By filtering background network traffic, the recordings are reduced to two PNT transmitting devices, namely the pair of GPS receivers, which are placed at a fixed distance of 4 m from each other. All information that is necessary for the detectors discussed in this work can be retrieved from these records. The system clock results from the timestamps of the entries and can thus be compared with the GNSS time within the recordings. With a probability of 50 %, spoofing attacks were started after 60 s in a scenario. The attacks are executed by the attackers A_R , A_M , and A_S (cf. Figure 2).

- A_R replays a recording with a certain *age* of a ship that followed a similar route as the victim but shifted eastward by a specified *distance*.
- A_M performs a meaconing attack with a *delay* to its own static position. The attacker is thereby located relative to the victim at a *distance* to the east at the onset of the attack.
- A_S finally constructs signals that will slowly shift the victim's position with a velocity defined by *shift speed* and an azimuth angle of *shift angle*.

All three attackers are equipped with a single sending antenna. Note that for mobile targets, a multi-antenna A_S attack is very complex and extremely difficult to realize in practice. Since most vessels are, moreover, not equipped with more than two GNSS receivers [10], which also cannot acquire the signals' angle of arrival, and the detection of such sophisticated attacks is, in any case, not expected to be feasible using software-based approaches. Hence, we only simulate single-antenna attackers that have actually been demonstrated in practice [3,6].

The mentioned parameters of the individual attackers are expected to have an impact on the detection capabilities of our framework. The parameter space is listed in Table 3. The two-dimensional parameter space has 19 gradations per dimension, resulting in a total of 361 parameter configurations per attacker. A set of 20 benign and 20 spoofed recordings that differs in the noisy position and time measurements are created for each parameter configuration. Hence, in total, our labeled dataset consists of 43,320 scenarios and can be scientifically used for the development and benchmarking of GPS spoofing detection and prevention methods.

Table 3. Parameter space for each attacker model.

Attacker	Parameter	Parameter Space
Replay A_R	$distance$	Physical separation between attacker and victim
	age	Age of the replayed recording $\{0 \text{ ms}, 15 \text{ ms}, \dots, 240 \text{ ms}\} \cup \{1 \text{ min}, 1 \text{ d}\}$
Meaconing A_M	$distance$	Physical separation between attacker and victim
	$delay$	Time delay introduced by the attacker $\{0 \text{ ms}, 15 \text{ ms}, \dots, 270 \text{ ms}\}$
Simulator A_S	$shift \ angle$	Azimuth in which the victim's position is shifted $\{0^\circ, 10^\circ, \dots, 180^\circ\}$
	$shift \ speed$	Speed with which the victim's position is shifted $\{0 \text{ kn}, 4 \text{ kn}, \dots, 72 \text{ kn}\}$

7. Performance Evaluation

In this section, we evaluate the effectiveness of MANA to detect GPS spoofing attacks based on the MARSIM dataset (cf. Section 6.2). After describing our methodology and metrics in Section 7.1, we investigate the capability of each method of our framework and evaluate their individual potential in Section 7.2.

7.1. Methodology and Metrics

For our dataset, we propose a binary classification task. Thus, for each file of the dataset, the method needs to decide whether the corresponding scenario is spoofed or not. Furthermore, we group the scenarios by the type of attacker involved, i.e., A_R , A_M , and A_S (cf. Figure 2). The performance is measured using the common metrics *precision* and *recall*, defined as:

$$precision = \frac{true \ positives}{true \ positives + false \ positives}, \quad recall = \frac{true \ positives}{true \ positives + false \ negatives}.$$

Intuitively, recall represents the actual detection capability. Precision, on the other hand, can be considered as the reliability of a method's indication.

We experimentally adjusted the parameters *max speed* and *max rate of turn* to minimize false detection of spoofing attacks under benign conditions (i.e., relaxed thresholds, cf. Table 4) and consequently achieve high *precision*. CDM's *max clock drift dev* threshold is set based on our observations in Section 6.1.3, whereas for *min distance* and *min speed*, half of the actual distance between receivers and *max speed*, respectively, are used. While this decision may inherently have a negative impact on the *recall*, we expect that a combination of methods can compensate for the potentially lower sensitivity of each method.

Table 4. Configuration of MANA's detection methods.

Method	Parameter	Value
PDM	<i>min distance</i>	2 m
	<i>min speed</i>	15 kn
PCC	<i>max speed</i>	30 kn
	<i>max rate of turn</i>	7.5° s^{-1}
CDM	<i>max clock drift dev</i>	100 ms

7.2. Evaluation Results

The results of our evaluation reveal that the success of spoofing detection methods investigated in our experiments depends, in different ways, on the attackers' parameters. Some methods depend on both attack parameters (PCC_{sog} and PCC_{rot}), others only on a single parameter (CDM), and still others are found to be independent of the selected parameters (PDM), as can be seen in Figure 6. According to the relaxed thresholds mentioned above, the mean *precision* over all displayed methods is 0.92.

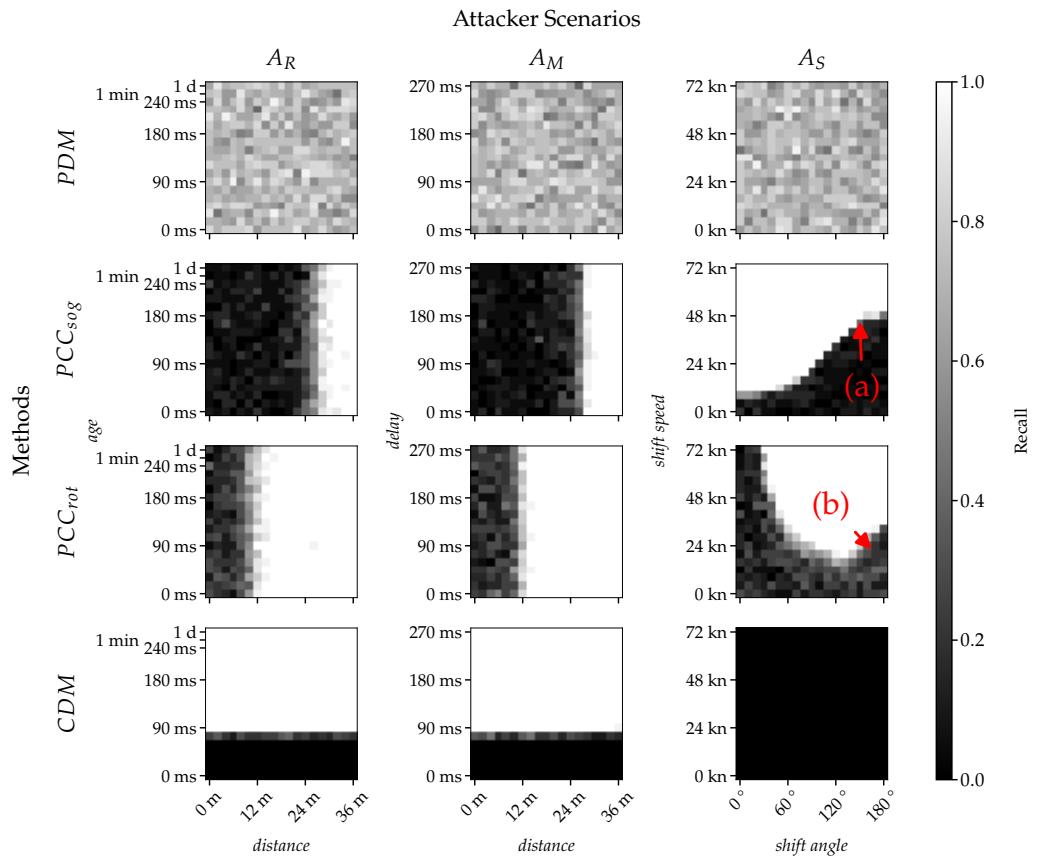


Figure 6. The recall achieved by individual detection methods depends on the type of attacker. Each heatmap has a resolution of 19×19 pixels exploring the parameter space for the given attacker, cf. Table 3. The grayscale of each pixel represents the *recall* calculated over 40 scenarios (20 benign and 20 spoofed) for the given attacker and its parameter constellation. Note that the brighter a pixel, the better the respective method performs. It is observable that the detection capabilities of the methods differ and are often influenced by the attacker parameters either in only one or in both dimensions. Note that both labels (a) and (b) highlight specifics of the evaluation that will be addressed in the textual description (in Section 7.2).

The methods in the focus of this evaluation are *PDM*, *PCC*, *EDV*, and *CDM*. In accordance with the classification of known GPS spoofing detection techniques in Table 1, we anticipate *PDM* to perform best and the other methods to perform slightly lower, while we suspect that the effectiveness of *PCC* methods varies considerably.

By checking the fixed distance between receivers, *PDM* (first row in Figure 6) shows the most consistent performance over all scenarios. While there are missed detections (false negatives) for all attacker models, they do not appear to be correlated with the attackers' parameterization. Missed detections are caused by noisy position measurements that keep the calculated distance between receivers above the *min distance* threshold (cf. Table 4). In Section 7.2.2, the impact of the actual distance between receivers on the detection performance of *PDM* will be investigated separately.

In comparison, the rather simple *PCC_{sog}* method, which detects spoofing attacks based on unrealistically high SOG estimates, gives all three attacker models a fairly large margin to remain undetected (black areas in Figure 6). Replay and meaconing (*A_R* and *A_M*) are only limited to a similar extent by the choice of the *distance* between the victim and the recorded ship or between victim and attacker. The exceeding of this 26 m limit is almost always detected. The transition between the undetectable (black) and the detectable area (white) is smoother for *A_R* than for *A_M*, probably due to the movement of the recorded vessel that is replayed in comparison to the static position of *A_M*. The relationship between the *A_S* parameters and the detection capability is more complex. While an increasing *shift*

speed in the direction of travel (i.e., *shift angle* of 0°) does not offer much margin for the attacker (roughly 12 kn), the margin significantly increases up to about 46 kn as soon as the *shift angle* passes the mark of approximately 140° (see label *a*) in Figure 6). The victim interprets a *shift angle* of $>140^\circ$ and a *shift speed* of up to 40 kn as traveling in the opposite direction, explaining the observed results. This effect is visualized in Figure 7.

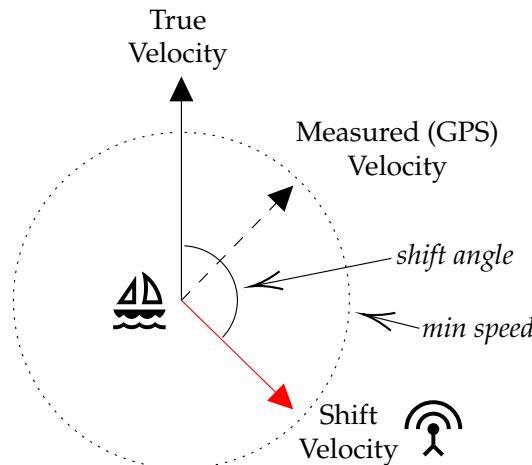


Figure 7. Visualization of the attack performed by A_S and the effect on the *min speed* property of PCC_{rot} . The attacker shifts the victim's position by a constant velocity defined by *shift speed* and *shift angle*. The victim observes a combination (dashed) of the shift velocity (red) and its true velocity (black) based on GPS measurements. Even if the true velocity is above the *min speed* threshold, this combination can fall below, resulting in the effect observed in Figure 6 at labels (a) and (b).

Similar to PCC_{sog} , PCC_{rot} is insensitive to changes in signal *age* or *delay* caused by replay or meaconing attacks (A_R and A_M). However, the attackers are already exposed at a *distance* of roughly 12 m, leading to a significantly increased ROT measurement. The detection of the simulator attacker A_S again depends on both *shift speed* and *shift angle*. A low *shift speed* allows for a large *shift angle* and vice versa. An exception to this rule is marked by label (b) in Figure 6 and has similar reasons as for label (a) (see Figure 7). The area of missing detections is caused by the *min speed* requirement of PCC_{rot} (cf. Section 5.2). If the shift vector composed of *shift speed* and *shift angle* points approximately in the opposite direction of travel, the total speed derived from GPS may fall below that threshold. If the *min speed* threshold is decreased, the caused blind spot eventually disappears. Nonetheless, the threshold needs to be sufficiently high so that the ROT measurement based on noisy GPS positions is reliable and does not cause false positives.

CDM directly monitors the local system clock of the device executing MANA with respect to the time provided by GPS. This results in a limitation of at most 75 ms for the signal *age* of A_R and the *delay* of A_M . A time jump of this magnitude with additional noise (cf. Figure 5b and Section 6.1.2) often exceeds the allowed drift range of 100 ms. Thus, both *age* and *delay* need to stay below this mark to avoid being detected (black area in Figure 6). All other parameters are time-independent and have no influence on *CDM*'s outcome.

The two methods, PCC_{height} and EDV , are not shown in Figure 6, since neither of these proved effective in our simulations. PCC_{height} and EDV detect A_R only if the signal *age* exceeds several hours or minutes, respectively, whereas A_M and A_S were found to be hardly detectable with these methods in our scenarios.

7.2.1. Ensemble of Methods

The performance of an ensemble of all investigated methods can be seen in Figure 8. Here, the binary outputs of the individual methods are combined with a logical OR. Thus, as long as at least one method is triggered, spoofing is detected. Note that this initial approach is rather simple and weights each method equally. The exploration of improved combinatorial methods is part of our future work. For attackers A_R and A_M , a combination

of the methods PDM , PCC_{rot} , and CDM is sufficient, while A_S requires PCC_{sog} in addition to PCC_{rot} and PDM . Overall, it turns out that a significant area of the parameter space for each attacker is solely covered by the PDM method (highlighted in red in Figure 8), which thus significantly contributes to the combined performance.

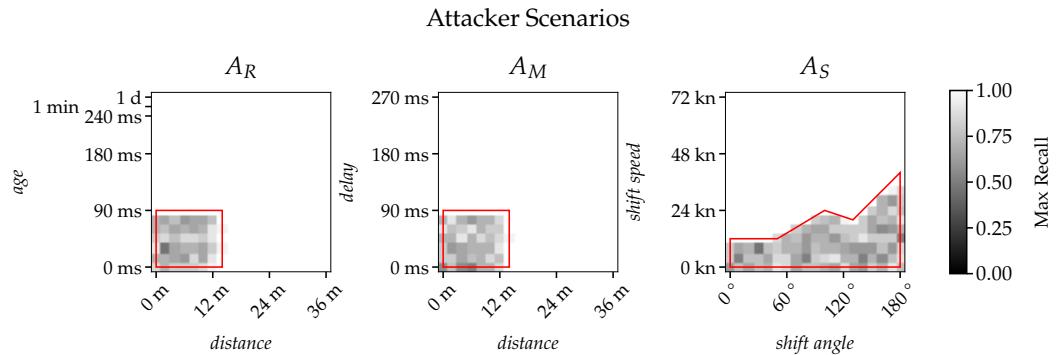


Figure 8. Maximum achieved recall considering all methods from Figure 6 shows the potential effectiveness of combining methods. This combination covers large parts of the attacks represented in the dataset. For each attacker, however, small areas exist (highlighted in red) that are solely covered by the PDM method.

7.2.2. Impact of Distance between Receivers on PDM

The performance of PDM depends on the distance between receiver pairs. To investigate the impact of this distance on the recall, we varied the distance of two receivers between 2 and 10 m with 100 increments in an A_S scenario. For each increment, 100 repetitions are conducted. We keep the *shift angle* and *shift speed* fixed to zero, effectively disabling the attacker. However, the detection capabilities of PDM are not related to the parameter choice of the attacker, cf. Figure 6. Hence, the only varying factor is the GPS noise. The results are depicted in Figure 9. As can be seen, the distance significantly impacts the capability of PDM . The impact vanishes at a distance of roughly 6 m, which is consistent with the results of Jansen et al. [6].

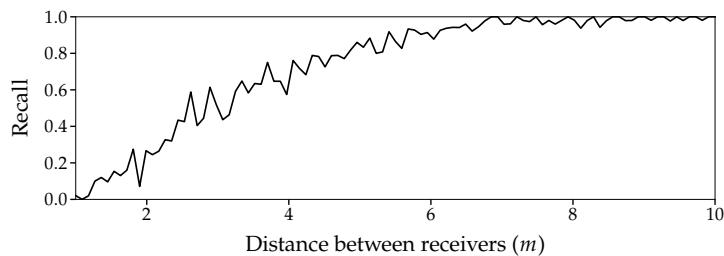


Figure 9. Performance of the PDM method in terms of recall as a function of distance between two receivers. Note that the *min distance* threshold is again always set to half the true distance between receivers (x-axis) and that distance measurements are smoothed with a moving average (with $\alpha = 0.1$).

8. Discussion and Outlook

Simulating reality in all its details is generally too complex and not target-oriented. Therefore, our simulator comes with some reasonable abstractions, in the context of which the CNM method has also been excluded from the evaluation as explained in Section 5.2. Still, an investigation of CNM 's detection capabilities, especially on advanced signal take-over strategies described by Tippenhauer et al. [7], would be desirable and is left for future work. Other random processes are simplified in the simulation for the sake of abstraction. A trace-based approach was used to model the GPS error. Further modeling of random probability distributions was chosen and parametrized based on field experiments (cf. Section 6).

Our simulation equips each attacker with only a single antenna, although advanced simulator attackers A_S can be in possession of multiple antennas (cf. Figure 2). The effectiveness of *PDM* weakens when attackers use multiple antennas. However, this could be simply counteracted by adding more receivers to the victim to further reduce the dimensional freedom of the attacker, as proposed in [7]. As a rule of thumb, *PDM* requires always one more receiver for detection than antennas available to the attacker.

Overall, the methods in our framework MANA showed promising results. While the *PDM* method, in particular, covers the entire attack space, *PCC* methods have the potential to further improve the effectiveness of MANA's detection capabilities in many scenarios. In this context, the ensemble of individual methods plays an important role. Although our simplified approach is sufficient for many scenarios, there is a limitation: All methods are weighted equally, requiring strict thresholds to avoid false positives. Therefore, many insights of relatively weak methods are discarded, decreasing the overall performance. A possible solution to this problem may be to support the ensemble with neural networks to predict a single spoofing indicator. This approach would even allow temporal information to be included in the detection process. Such a network could be trained with our dataset and later refined with short network recordings of the actual vessel in which the detector will be installed, eliminating the need to manually set thresholds.

Nevertheless, it should be noted that there will never be a complete guarantee for the detection of spoofing attacks. Therefore, for the purpose of countering CEMA-based GNSS attacks, it is necessary for practice to develop complementary, GNSS-independent localization systems such as the R-Mode, described in Section 4.2, and to integrate them into the localization process for reliable situational awareness.

In view of the current autonomy trend and the first unmanned vessels now reaching practical operation, the need becomes more urgent. For manned ships, GNSS spoofing can be detected and even mitigated to some degree by using other navigation technologies such as radar or visual aids to verify the vessel's position. If crew members suspect that GNSS signals are being falsified, they can also manually adjust the vessel's course and inform other vessels or port authorities of any navigational problems. In contrast, for unmanned vessels, the effects of spoofing can be much more severe, as these vessels tend to rely almost entirely on GNSS for navigation and communications and generally depend more heavily on automated systems. However, they may not yet have the ability to verify their position and accordingly adjust their course. Without crew members on board, it may also take longer to detect and respond to spoofing attacks. Therefore, the risk of collisions, groundings, or other accidents is much higher.

9. Conclusions

The fact that GPS signals are weak when they reach the Earth's surface makes it easy for adversaries to attack navigation systems, which is particularly problematic in the maritime domain, which is heavily reliant on GNSS. In this context, the paper provides a brief overview of research on detecting and mitigating GPS spoofing attacks at different layers. Since a simple and cost-effective retrofit is crucial for maritime practice, we focused on software-based methods. We proposed MANA, a novel framework comprising a selection of methods that continuously monitors and analyzes information derived from GPS, delivered as NMEA sentences via the maritime network.

Through a maritime simulator that uses real-world data to model realistic behavior, a comprehensive labeled dataset was generated, including legitimate and spoofed samples. This dataset provides not only the basis for our evaluation but can also be used for future benchmarking. In our evaluation, we compared the effectiveness of MANA's individual methods and show that it greatly differs. Pairwise Distance Monitoring (*PDM*) that requires multiple receivers was identified to be the most promising method in our software-based approach and is particularly applicable to maritime systems. We show that *PDM* achieves reliable detection for a wide range of common GPS spoofing attacks while still leaving room for improvements. As our evaluation suggests, alternative methods could support

PDM and thereby compensate for remaining deficiencies in many cases. In our future work, we thus plan to extend our evaluation and investigate the potential of a smart ensemble of individual detection methods of MANA.

Author Contributions: Conceptualization, J.S., C.H. and J.B.; methodology, J.S., C.H. and J.B.; software, J.S. and C.H.; validation, J.S., C.H. and J.B.; investigation, J.S., C.H., M.v.R. and J.B.; writing—original draft preparation, J.S., C.H. and J.B.; writing—review and editing, J.S., M.v.R. and J.B.; visualization, J.S., C.H., M.v.R. and J.B.; supervision, J.B. and E.P.; All authors have read and agreed to the published version of the manuscript.

Funding: This work is part of the project MUM2 (<https://www.mum-project.com>, accessed on 23 April 2023). It was partially funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK) within the “Maritime Research Programme” with contract number 03SX543B managed by the Project Management Jülich (PTJ). The authors are responsible for the contents of this publication.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The MARSIM dataset introduced in Section 6.2 (pcap and csv files) and the source code of MANA are available at: <https://github.com/fkie-cad/mana>, accessed on 23 April 2023. Moreover, a Wireshark dissector for maritime protocols developed by our research group is available as open source at: <https://github.com/fkie-cad/maritime-dissector>, accessed on 23 April 2023. This dissector can be used to interpret and analyze maritime network traffic, especially the NMEA sentences within the recorded pcap files of MARSIM.

Acknowledgments: The authors thank Konrad Wolsing for supporting the field experiments.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIS	automatic identification system
APT	auxiliary peak tracking
ARPA	automatic radar plotting aid
C/A	coarse/acquisition code
CDM	Clock Drift Monitoring
CEMA	cyber and electromagnetic activities
C/N ₀	carrier-to-noise density
CNM	C/N ₀ Monitoring
DOA	direction of arrival
ECDIS	electronic chart display and information system
EDV	Ephemeris Data Validation
GNSS	global navigation satellite system
GPS	Global Positioning System
IEC	International Electrotechnical Commission
IBS	integrated bridge system
IMO	International Maritime Organization
LWE	Lightweight Ethernet
MANA	MARitime Nmea-based Anomaly detection
MARSIM	MARitime SIMulated
MCS	Maritime Cyber Security
NAVSTAR	Navigational Satellite Timing and Ranging
NMEA	National Marine Electronics Association
PCC	Physical Cross-Check
PDM	Pairwise Distance Monitoring
PLMN	Public Land Mobile Network

PNT	positioning, navigation, and timing
PRN	pseudo-random noise
RAIM	Receiver Autonomous Integrity Monitoring
ROT	rate of turn
SOG	speed over ground
TLE	two-line element
TOA	time of arrival
UAV	unmanned aerial vehicle
VDES	Very high frequency Data Exchange System

References

1. Tam, K.; Jones, K. Factors Affecting Cyber Risk in Maritime. In Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Oxford, UK, 3–4 June 2019; pp. 1–8. [CrossRef]
2. Androjna, A.; Perkovic, M. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. *Trans. Marit. Sci.* **2021**, *10*, 361–373. [CrossRef]
3. Bhatti, J.; Humphreys, T.E. Hostile Control of Ships Via False GPS Signals: Demonstration and Detection. *J. Inst. Navig.* **2017**, *64*, 51–66. [CrossRef]
4. Motallebighomi, M.; Sathaye, H.; Singh, M.; Ranganathan, A. Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals. *arXiv* **2022**, arXiv:2204.11641v3. [CrossRef]
5. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *Int. J. Navig. Obs.* **2012**, *2012*, 127072. [CrossRef]
6. Jansen, K.; Tippenhauer, N.O.; Pöpper, C. Multi-Receiver GPS Spoofing Detection: Error Models and Realization. In Proceedings of the Conference on Computer Security Applications (ACSAC), Los Angeles, CA, USA, 5–8 December 2016; pp. 237–250. [CrossRef]
7. Tippenhauer, N.O.; Pöpper, C.; Rasmussen, K.B.; Capkun, S. On the Requirements for Successful GPS Spoofing Attacks. In Proceedings of the International Conference on Computer and Communications Security (CCS), Chicago, IL, USA, 17–21 October 2011; pp. 75–86. [CrossRef]
8. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
9. Meng, L.; Yang, L.; Yang, W.; Zhang, L. A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sens.* **2022**, *14*, 4826. [CrossRef]
10. Januszewski, J. Shipborne satellite navigation systems receivers, exploitation remarks. *Sci. J. Marit. Universiy Szczec.* **2014**, *40*, 67–72.
11. Lund, M.S.; Gulland, J.E.; Hareide, O.S.; Jøsok, Ø.; Weum, K.O.C. Integrity of Integrated Navigation Systems. In Proceedings of the Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–5. [CrossRef]
12. Hemminghaus, C.; Bauer, J.; Wolsing, K. SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures. In Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021. [CrossRef]
13. Rødseth, Ø.J.; Christensen, M.J.; Lee, K. Design challenges and decisions for a new ship data network. In Proceedings of the International Symposium on International Symposium Information on Ships (ISIS), Berlin, Germany, 27–28 September 2011; pp. 149–168.
14. BBC News. Suez Blockage Is Holding Up \$9.6 bn of Goods a Day. 2021. Available online: <https://www.bbc.com/news/business-56533250> (accessed on 17 March 2023).
15. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing Cyber Challenges of Maritime Navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [CrossRef]
16. IEC. *Maritime Navigation and Radiocommunication Equipment and Systems—Digital Interfaces—Part 450: Multiple Talkers and Multiple Listeners—Ethernet Interconnection* (IEC 61162-450:2018); International Electrotechnical Commission (IEC): Geneva, Switzerland, 2018.
17. Warner, J.S.; Johnston, R.G. *GPS Spoofing Countermeasures*; Technical Report LAUR-03-6163; Vulnerability Assessment Team, Los Alamos National Laboratory: Los Alamos, NM, USA, 2003.
18. Ranganathan, A.; Ólafsdóttir, H.; Capkun, S. SPREE: A Spoofing Resistant GPS Receiver. In Proceedings of the Conference on Mobile Computing and Networking (MobiCom), New York, NY, USA, 3–7 October 2016; pp. 348–360. [CrossRef]
19. Medina, D.; Lass, C.; Marcos, E.P.; Ziebold, R.; Closas, P.; García, J. On GNSS Jamming Threat from the Maritime Navigation Perspective. In Proceedings of the 22th International Conference on Information Fusion (FUSION), Ottawa, ON, Canada, 2–5 July 2019; pp. 1–7. [CrossRef]
20. Caprolu, M.; Pietro, R.D.; Raponi, S.; Sciancalepore, S.; Tedeschi, P. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Commun. Mag.* **2020**, *58*, 90–96. [CrossRef]
21. Awan, M.S.K.; Al Ghamdi, M.A. Understanding the Vulnerabilities in Digital Components of An Integrated Bridge System (IBS). *J. Mar. Sci. Eng.* **2019**, *7*, 350. [CrossRef]

22. Burgess, M. When a Tanker Vanishes, All the Evidence Points to Russia. 2017. Available online: <https://www.wired.co.uk/article/black-sea-ship-hacking-russia> (accessed on 17 March 2023).
23. Wu, J.; Thorne-Large, J.; Zhang, P. Safety First: The Risk of Over-Reliance on Technology in Navigation. *J. Transp. Saf. Secur.* **2021**, *14*, 1220–1246. [CrossRef]
24. Maritime Safety Committee (MSC). *Resolution MSC.915(22)–Revised Maritime Policy and Requirements for a Future Global Navigation Satellite System (GNSS)*; MSC 915(22); International Maritime Organization (IMO): London, UK, 2001.
25. Zalewski, P. GNSS Integrity Concepts for Maritime Users. In Proceedings of the European Navigation Conference (ENC), Warsaw, Poland, 9–12 April 2019; pp. 1–10. [CrossRef]
26. Department of Homeland Security. Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework Version 2.0. 2022. Available online: https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf (accessed on 20 April 2023).
27. Warner, J.S.; Johnston, R.G. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *J. Secur. Adm.* **2002**, *25*, 19–27.
28. Coulon, M.; Chabory, A.; Garcia-Pena, A.; Vezinet, J.; Macabiau, C.; Estival, P.; Ladoux, P.; Roturier, B. Characterization of Meaconing and its Impact on GNSS Receivers. In Proceedings of the Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+), Online, 21–25 September 2020; pp. 3713–3737. [CrossRef]
29. Lenhart, M.; Spanghero, M.; Papadimitratos, P. DEMO: Relay/replay attacks on GNSS signals. *arXiv* **2022**, arXiv:2202.10897. [CrossRef]
30. Key, E.L. *Techniques to Counter GPS Spoofing. Internal Memorandum*; MITRE Corporation: Mclean, VA, USA, 1995.
31. Brown, R.G. Receiver Autonomous Integrity Monitoring. In *Global Positioning System: Theory and Applications*; Parkinson, B., Spilker, J., Eds.; AIAA Inc.: Washington, DC, USA, 1996; Volume 2, Chapter 5, pp. 143–165.
32. Scott, L. Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems. In Proceedings of the Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), Portland, OR, USA, 9–12 September 2003; pp. 1543–1552.
33. Kerns, A.J.; Wesson, K.D.; Humphreys, T.E. A blueprint for civil GPS navigation message authentication. In Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 5–8 May 2014; pp. 262–269. [CrossRef]
34. Wen, H.; Huang, P.Y.R.; Dyer, J.; Archinal, A.; Fagan, J. Countermeasures for GPS signal spoofing. In Proceedings of the Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS), Long Beach, CA, USA, 13–16 September 2005; Volume 5, pp. 13–16.
35. Akos, D.M. Who's Afraid of the Spoof? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *Navigation* **2012**, *59*, 281–290. [CrossRef]
36. Konovaltsev, A.; Cuntz, M.; Haettich, C.; Meurer, M. Autonomous spoofing detection and mitigation in a GNSS receiver with an adaptive antenna array. In Proceedings of the Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+), Nashville, TN, USA, 16–20 September 2013; pp. 2937–2948.
37. McDowell, C.E. GPS Spoof and Repeater Mitigation System Using Digital Spatial Nulling. U.S. Patent 7,250,903, 31 July 2007.
38. Nielsen, J.; Broumandan, A.; Lachapelle, G. Spoofing Detection and Mitigation with a Moving Handheld Receiver. *GPS World* **2010**, *21*, 27–33.
39. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS spoof countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 181–191. [CrossRef]
40. Li, J.; Zhu, X.; Ouyang, M.; Shen, D.; Chen, Z.; Dai, Z. GNSS spoofing detection technology based on Doppler frequency shift difference correlation. *Meas. Sci. Technol.* **2022**, *33*, 095109. [CrossRef]
41. Chu, F.; Li, H.; Wen, J.; Lu, M. Statistical Model and Performance Evaluation of a GNSS Spoofing Detection Method based on the Consistency of Doppler and Pseudorange Positioning Results. *J. Navig.* **2019**, *72*, 447–466. [CrossRef]
42. Zeng, Q.; Li, H.; Qian, L. GPS spoofing attack on time synchronization in wireless networks and detection scheme design. In Proceedings of the Military Communications Conference (MILCOM), Orlando, FL, USA, 29 October–1 November 2012; pp. 1–5. [CrossRef]
43. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoof. In Proceedings of the Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS), Savannah, GA, USA, 16–19 September 2008; pp. 2314–2325.
44. Lo, S.C.; Enge, P.K. Authenticating aviation augmentation system broadcasts. In Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS), Indian Wells, CA, USA, 4–6 May 2010; pp. 708–717. [CrossRef]
45. Lo, S.; De Lorenzo, D.; Enge, P.; Akos, D.; Bradley, P. Signal authentication: A secure civil GNSS for today. *Inside GNSS* **2009**, *4*, 30–39.
46. Phelts, R.E. Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality. Ph.D. Theses, Stanford University, Stanford, CA, USA, 2000.
47. Pini, M.; Fantino, M.; Cavalieri, A.; Ugazio, S.; Presti, L.L. Signal Quality Monitoring Applied to Spoofing Detection. In Proceedings of the Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS), Portland, OR, USA, 20–23 September 2011; pp. 1888–1896.

48. Miralles, D.; Bornot, A.; Rouquette, P.; Levigne, N.; Akos, D.M.; Chen, Y.H.; Lo, S.; Walter, T. An Assessment of GPS Spoofing Detection Via Radio Power and Signal Quality Monitoring for Aviation Safety Operations. *IEEE Intell. Transp. Syst. Mag.* **2020**, *12*, 136–146. [[CrossRef](#)]
49. White, N.A.; Maybeck, P.S.; DeVilbiss, S.L. Detection of interference/jamming and spoofing in a DGPS-aided inertial system. *IEEE Trans. Aerosp. Electron. Syst.* **1998**, *34*, 1208–1217. [[CrossRef](#)]
50. Wei, X.; Aman, M.N.; Sikdar, B. Light-Weight GPS Spoofing Detection for Synchrophasors in Smart Grids. In Proceedings of the International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 16–19 December 2020; pp. 1–4. [[CrossRef](#)]
51. Psiaki, M.L.; O’hanlon, B.W.; Powell, S.P.; Bhatti, J.A.; Wesson, K.D.; Humphreys, T.E. GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase. In Proceedings of the Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), Tampa, FL, USA, 8–12 September 2014.
52. Dasgupta, S.; Rahman, M.; Islam, M.; Chowdhury, M. A Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 23559–23572. [[CrossRef](#)]
53. Lemieszewski, Ł. Transport safety: GNSS spoofing detection using the single-antenna receiver and the speedometer of a vehicle. *Procedia Comput. Sci.* **2022**, *207*, 3181–3188. [[CrossRef](#)]
54. Olieri, G.; Sciancalepore, S.; Ibrahim, O.A.; Di Pietro, R. GPS spoofing detection via crowd-sourced information for connected vehicles. *Comput. Netw.* **2022**, *216*, 109230. [[CrossRef](#)]
55. Nighswander, T.; Ledvina, B.; Diamond, J.; Brumley, R.; Brumley, D. GPS Software Attacks. In Proceedings of the International Conference on Computer and Communications Security (CCS), Raleigh, NC, USA, 16–18 October 2012; pp. 450–461. [[CrossRef](#)]
56. Zalewski, P. Real-time GNSS spoofing detection in maritime code receivers. *Sci. J. Marit. Univ. Szczec.* **2014**, *38*, 118–124.
57. Laverty, D.; Kelsey, C.; O’Raw, J. GNSS Time Signal Spoofing Detector for Electrical Substations. In Proceedings of the IEEE Power & Energy Society General Meeting (PESGM), Denver, CO, USA, 17–21 July 2022. [[CrossRef](#)]
58. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. Novelty-based Intrusion Detection of Sensor Attacks on Unmanned Aerial Vehicles. In Proceedings of the ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet), Alicante, Spain, 16–20 November 2020; pp. 23–28. [[CrossRef](#)]
59. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. UAV Attack Dataset. 2020. Available online: <https://ieee-dataport.org/open-access/uav-attack-dataset> (accessed on 23 April 2023).
60. Singh, S.; Singh, J.; Singh, S.; Goyal, S.B.; Raboaca, M.S.; Verma, C.; Suciu, G. Detection and Mitigation of GNSS Spoofing Attacks in Maritime Environments Using a Genetic Algorithm. *Mathematics* **2022**, *10*, 4097. [[CrossRef](#)]
61. Lee, D.K.; Miralles, D.; Akos, D.; Konovaltsev, A.; Kurz, L.; Lo, S.; Nedelkov, F. Detection of GNSS Spoofing using NMEA Messages. In Proceedings of the European Navigation Conference (ENC), Dresden, Germany, 23–24 November 2020; pp. 1–10. [[CrossRef](#)]
62. Olieri, G.; Sciancalepore, S.; Ibrahim, O.A.; Di Pietro, R. Drive Me Not: GPS Spoofing Detection via Cellular Network: (Architectures, Models, and Experiments). In Proceedings of the Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Miami, FL, USA, 15–17 May 2019; pp. 12–22. [[CrossRef](#)]
63. Johnson, G.; Swaszek, P.; Alberding, J.; Hoppe, M.; Oltmann, J.H. The Feasibility of R-Mode to Meet Resilient PNT Requirements for e-Navigation. In Proceedings of the Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), Tampa, FL, USA, 8–12 September 2014; pp. 3076–3100.
64. Koch, P.; Gewies, S. Worldwide Availability of Maritime Medium-Frequency Radio Infrastructure for R-Mode-Supported Navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 209. [[CrossRef](#)]
65. Grundhöfer, L.; Rizzi, F.G.; Gewies, S.; Hoppe, M.; Bäckstedt, J.; Dziewicki, M.; Galdo, G.D. Positioning with medium frequency R-Mode. *NAVIGATION J. Inst. Navig.* **2021**, *68*, 829–841. [[CrossRef](#)]
66. Naus, K.; Waż, M.; Szymak, P.; Gucma, L.; Gucma, M. Assessment of ship position estimation accuracy based on radar navigation mark echoes identified in an Electronic Navigational Chart. *Measurement* **2021**, *169*, 108630. [[CrossRef](#)]
67. Hagen, O.K.; Ånonsen, K.B. Using Terrain Navigation to Improve Marine Vessel Navigation Systems. *Mar. Technol. Soc. J.* **2014**, *48*, 45–58. [[CrossRef](#)]
68. Kelso, T.S. Frequently Asked Questions: Two-Line Element Set Format. Celestrak, Satellite Times. 2004. Available online: <http://celestrak.com/columns/v04n03/> (accessed on 17 March 2023).
69. Oszczak, B. GNSS positioning algorithms using methods of reference point indicators. *Artif. Satell.* **2014**, *49*, 21–23. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.