UNIVERISITY OF PIRAEUS - DEPARTMENT OF INFORMATICS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

MSc «Cybersecurity and Data Science»

ΠΜΣ «Κυβερνοασφάλεια και Επιστήμη Δεδομένων »

MSc Thesis

Μεταπτυχιακή Διατριβή

Thesis Title: Τίτλος Διατριβής:	**Understanding and Mitigating GPS Spoofing Attacks in Shipping** Κατανόηση και Μετριασμός των Επιθέσεων GPS Spoofing στη Ποντοπόρο Ναυτιλία
Student's name-surname: Ονοματεπώνυμοφοιτητή:	**Niko Charitou** Νικώ Χαρίτου
Father's name: Πατρώνυμο:	**Vasileios** Βασίλειος
Student's ID No: Αριθμός Μητρώου:	ΜΠΚΕΔ2246
Supervisor: Επιβλέπων:	**Athanasios Papadimitriou, Assistant Professor** Αθανάσιος Παπαδημητρίου, Επίκουρος Καθηγητής

January 2025/Ιανουάριος 2025

3-Member Examination Committee

ΤριμελήςΕξεταστικήΕπιτροπή

Athanasios Papadimitriou **Assistant Professor**	**Michael Psarakis** **Associate Professor**	**Panagiotis Kotzanikolaou** **Professor**
Αθανάσιος Παπαδημητρίου Επίκουρος Καθηγητής	Μιχαήλ Ψαράκης Αναπληρωτής Καθηγητής	Παναγιώτης Κοτζανικολάου Καθηγητής

Acknowledgements

I would like to express my deepest gratitude to the supervisor of this thesis, mr Athanasios Papadimitriou, as his guidance and expertise input, throughout my research and writing process; along with his insights and intuition were instrumental in shaping this thesis and bringing it to completion. I take this opportunity to convey my Special thanks to my professor Kontzanikolaou Panagiotis and mentors at the University of Piraeus, Department of Informatics. As without their continuous support and will to help me achieve my goals this thesis would have a different perspective on research, one that I might not have loved so much. I would also like to thank my PhD peers in the MSc «Cybersecurity and Data Science» programs for their constructive discussion and support, which enriched my research experience. This journey would have not been possible without continuous support from family and friends. Their continuous support, patience and belief in my work have been the source of strength throughout this journey. Finally, this work is dedicated to all maritime professionals who strive for safety and security in an ever-increasing complex technological landscape.

Abstract

As cyber crises in the maritime sector become more evident and GPS Spoofing attacks more common, this thesis aims to better the knowledge of the reader on the topic of "Understanding and Mitigating GPS Spoofing in Maritime Navigation". This, while emphasizing the impact of the implications imposed on the industry in the event of a successful Spoofing attack. This study will provide a detailed analysis of the mechanisms, methodologies and software and hardware approaches available to counter-react to a GPS Spoofing attack; and classifies them by implementation, feasibility and cost. Further examination delves into the practical side of the available countermeasures while identifying the challenges imposed and applying them to the maritime sector. The thesis continues with a discussion of using neural network training techniques for GPS Spoofing detection and prevention while emphasizing the benefits and limitations of integrating machine learning in signal analysis and real-time monitoring. The conclusion incorporates key findings on GPS Spoofing mechanisms, countermeasures and practical applications in the maritime industry. The suggested future research directions include hybrid navigational systems, advanced regulatory frameworks and enhanced signal processing techniques that all aim to bolster maritime cybersecurity and resilience.

Περίληψη

Καθώς οι κρίσεις στον κυβερνοχώρο στον τομέα της ναυσιπλοΐας γίνονται όλο και πιο εμφανείς και οι επιθέσεις GPS Spoofing όλο και πιο συχνές, η παρούσα διατριβή αποσκοπεί στην καλύτερη γνώση του αναγνώστη σχετικά με το θέμα «Κατανόηση και μετριασμός του GPS Spoofing στη θαλάσσια ναυσιπλοΐα». Και αυτό, δίνοντας παράλληλα έμφαση στον αντίκτυπο των επιπτώσεων που επιβάλλονται στον κλάδο σε περίπτωση επιτυχούς επίθεσης Spoofing. Η παρούσα μελέτη θα παράσχει λεπτομερή ανάλυση των μηχανισμών, των μεθοδολογιών και των προσεγγίσεων λογισμικού και υλικού που είναι διαθέσιμες για την αντιμετώπιση μιας επίθεσης GPS Spoofing- και τις ταξινομεί με βάση την εφαρμογή, τη σκοπιμότητα και το κόστος. Περαιτέρω εξέταση εμβαθύνει στην πρακτική πλευρά των διαθέσιμων αντιμέτρων, ενώ προσδιορίζει τις προκλήσεις που επιβάλλονται και την εφαρμογή τους στον ναυτιλιακό τομέα. Η διατριβή συνεχίζει με μια συζήτηση σχετικά με τη χρήση τεχνικών εκπαίδευσης νευρωνικών δικτύων για την ανίχνευση και την πρόληψη του GPS Spoofing, ενώ υπογραμμίζει τα οφέλη και τους περιορισμούς της ενσωμάτωσης της μηχανικής μάθησης στην ανάλυση σήματος και την παρακολούθηση σε πραγματικό χρόνο. Το συμπέρασμα ενσωματώνει τα βασικά ευρήματα σχετικά με τους μηχανισμούς GPS Spoofing, τα αντίμετρα και τις πρακτικές εφαρμογές στη ναυτιλιακή βιομηχανία. Οι προτεινόμενες μελλοντικές ερευνητικές κατευθύνσεις περιλαμβάνουν υβριδικά συστήματα πλοήγησης, προηγμένα ρυθμιστικά πλαίσια και βελτιωμένες τεχνικές επεξεργασίας σήματος, οι οποίες αποσκοπούν στην ενίσχυση της ασφάλειας και της ανθεκτικότητας στον κυβερνοχώρο της ναυτιλίας.

Contents

Table of Contents: Images

Table of Contents: Tables

1. Introduction

This thesis makes an endeavour to provide a detailed assessment on the estimating risks against available GPS spoofing and the available countermeasures in merchant maritime industrial settings. The research will be analytic, and theoretical work will provide a review of works based on both literature, and the technological advancements, as well as strategic frameworks for countering the GPS Spoofing attacks. The set aim is to broaden the view of the reader on potential vulnerabilities and determine the impact level for spoofing events with reference to existing countermeasures. (Safety4Sea, 2020)

1.1 Overview of GPS and GNSS

As defined by The EU Space Programme; the Global Navigation Satellite System (GNSS) refers to any satellite constellation that provides global positioning, navigation, and timing services for multi-modal use. It consists of user receivers, one or more satellite constellations, ground segments and a control organisation with facilities to monitor and control the worldwide conformity of the signals processed by the user receivers to predetermined operational performance standards. (EUSPA - European Union Agency for Space Programme, 2024)

Several GNS Systems are currently available, such as the following:

Galileo (EU)
GPS (USA)
GLONASS (Russia)
BeiDou (China)

These systems are using space originated signals in order to transmit range and time data to the GNSS receivers. These receivers later use the data give so as to determine location (Christopher, 2017). More specifically and in the case of the current thesis, the Navigation Center of United States Coast Guard under the U.S. Department of Homeland Security institutes the Global Positioning System (GPS) as a part of GNSS and is a satellite-based radio-navigation system developed and operated by the U.S. Department of Defense (DOD) (U.S. Department of Homeland Security - Navigation Center). Full operational capability (FOC) of GPS was achieved in 1995 and a modernisation programme between 2002 and 2010, that followed the improved system's performance. Moreover, GPS enables users on land, sea, and air to determine their three-dimensional position, velocity, and time with high levels of precision and accuracy. This capability is available 24 hours a day, in all weather conditions, anywhere in the world thus making GPS superior to other radio-navigation systems available today or in the foreseeable future.

As noted by Ahmed El-Rabbany on his "Introduction to GPS: The Global Positioning System"; GPS is composed of three main segments: the Space Segment, the Control Segment, and the User Segment. (El-Rabbany, 2002)

- Space Segment

The Space Segment is composed of of a constellation of a minimum of 24 operational satellites that are arranged in six circular orbits at an altitude of 20,200 kilometres (10,900 nautical miles) above the Earth, with an inclination angle of 55 degrees. Each satellite completes one orbit, in approximately 11 hours and 58 minutes. Most frequently, these satellites are typically positioned in such a way that at least six satellites are visible to users anywhere on Earth at any given time, even though it is not required by any Authority involved (FURUNO, FURUNO FLEETBROADBAND, n.d.). This configuration ensures continuous and reliable

coverage for GPS users around the globe. However, coverage issues can be evident when a vessel nears land and is near coastal areas. A solution to which will be covered later on in this thesis.

- Control Segment

The Control Segment handles the operation and maintenance of the GPS satellite constellation. It consists of a master control station located in Colorado Springs, supported by five monitor stations and three ground antennas distributed around the world. The monitor stations track all visible GPS satellites, collecting ranging data from the satellite broadcastsThen the data are sent to the master control station, where precise satellite orbits are calculated. The updated navigation information gets formatted into messages and transmitted back to the satellites via the ground antenna. Thus, as these antennas also do handle the transmission and reception of satellite control and monitoring signals, ensuring the system's integrity and accuracy.

- User Segment

The User Segment encompass the receivers, processors, and antennas that enable operators on land, sea, or air to receive GPS satellite broadcasts and compute their precise position, velocity, and time. GPS receivers use the concept of satellite ranging to determine their location on Earth, since by measuring the distance from a group of satellites in space, users can accurately pinpoint their position. Each GPS satellite, then, transmits a signal that withholds its precise position and the current time. The user's receiver measures the time delay for the signal to reach it, which directly correlates to the distance from the satellite. By processing signals from at least four satellites simultaneously, the receiver can calculate the three dimensions of position (latitude, longitude, and altitude), velocity, and time.

This sophisticated system of satellite ranging and precise timekeeping allows GPS to provide unmatched accuracy and reliability, making it an indispensable tool for navigation and positioning across various domains, including military, commercial, and civilian applications.

1.2 Potential Compromisation of GPS Systems

Application in real life scenarios shows that the available GPS Systems are not shielded completely by any potential threats. These threats will be mentioned later on in this thesis, however a shore note at this stage ought to be made. Signal jamming, signal interferences, locking of counterfeit signals, blocking, and software or hardware weaknesses and spoofing. GPS Spoofing, as it will be fully examined later on, can have severe implications, as it can misdirect vehicles, ships, or aircraft and compromise the safety and security of individuals and assets (Bluegoatcyber). Although GPS systems offer tremendous convenience and utility, their vulnerabilities to the known threats present serious risks that cannot be ignored. These kind of threats pose significant challenges across various sectors and to individuals. However, by recognizing these vulnerabilities and proactively implementing effective countermeasures (Sunny Arora & Amit Tuteja - Guru Kashi University, Talwandi Sabo, 2021), users can be reasured that GPS technology remains a reliable and secure tool for the future

1.3 Thesis Contribution

Referencing the contribution of this thesis, the key contributions made are the following. A systematic review of GPS as a system and its mechanisms and challenges in the marine sector. A classification of the available countermeasures and an evaluation of the mitigation techniques

rated by feasibility, cost and easy of implementation; available for the stakeholders of marine navigation for their insight. A practical implementation side mentioning the hardware and software based countermeasures uniquely structured around real-life shipping operations. An introduction of applications of neural networks and machine learning based systems as an approach to detect and prevent Spoofing attacks in real time.

Moreover, the thesis contributes by providing recommendations for the use of multi-source verification procedures and hybrid approaches into acts against GPS Spoofing attacks.

1.4 Thesis Structure

This thesis is structured by an Introduction to the GNSS systems with an overview on GPS, while noting its critical role in the maritime industry. Followed by an approach of the methods and mechanisms of GPS Spoofing attacks and the available case studies on the same. Afterwards, sections 4 and 5 overview the existing hardware and software based countermeasures, with an emphasis on anomaly detection and cryptographic methods and an evaluation on dual band and multi-constellation GPS receivers. Subsequently, section 7 follows the application of neural networks for GPS spoofing detection and prevention and the real life challenges that come up during daily operations in the maritime industry. This thesis' structure is concluded by the key findings and the recommendations and future directions for the emerging threats and the latest advanced mitigation technologies.

2. The Critical Role of GPS2.1 The Importance of GPS for Merchant Marine Vessels

The critical role of GPS (Global Positioning System) and GNSS (Global Navigation Satellite System) in merchant marine vessels can be highlighted while examining the severe implications that GPS spoofing has on maritime operations in the event of any availability, integrity or confidentiality issue arises. These technologies are integral to modern maritime navigation, safety, efficiency as well as regulatory compliance, making them essential components in the industry.

2.1.1 Navigation and Route Planning

The GPS, as a part of GNSS, provides unparalleled accuracy in navigation, thus enabling merchant marine vessels to determine their precise positions at sea. This attained precision is crucial for plotting courses across the ocean, ensuring vessels' safe navigation through congested shipping lanes and avoiding hazards such as reefs and shallow waters. The accomplished accuracy of these systems significantly reduces the risk of groundings and collisions and thereby enhancing the overall safety of maritime navigation. Thus, any compromise in this precision can lead to catastrophic navigational errors, endangering all at once the vessel, its cargo, the seamen on board as well as the environment. It is worth mentioning that in shipping any potential fault on the operation of GPS directly ensures economical aftermath. Furthermore, the information carried by GPS is found embedded within a system known as the Automatic Identification System (AIS) transmission. The AIS is used for vessel traffic control around busy seaways and is endorsed by the International Maritime Organization. The provided services are important for navigation and is also increasingly used to bolster the security of ports and waterways by providing governments with greater situational awareness of commercial vessels and their cargo.

2.1.2 Safety and Collision Avoidance

In addition to its navigational use, GPS fortifies the safety levels reached at sea through its role in collision avoidance systems. These collision avoidance systems continuously monitor the positions and movements of nearby vessels, providing alerts for potential collision risks to both the vessel and her company. Also, due to the fact that the ship's GPS position is embedded in these transmissions, all essential information about vessel movements and unique identification information can be uploaded automatically to electronic charts. Moreover, the safety and security of vessels using this system is significantly enhanced as it allows for timely evasive actions from ship borne personnel, crucial for preventing accidents. In emergency situations, such as distress calls or man overboard scenarios, accurate location data is invaluable for coordinating search and rescue operations. However, GPS spoofing can undermine these safety measures, delaying rescue efforts and increasing the risk of loss of life.

In the new role of GNSS, when the aim is for increased safety at sea; maritime safety is of paramount importance. Supplying the master of a vessel and those responsible for the safety of shipping ashore with modern, proven tools to make marine navigation and communications more reliable is most critical issue. These tools would help on reducing errors, especially those with the potential to cause equipment damage, pollution harm to the marine environment, injury and loss of life. Maritime safety in this case means to address the needs of enhancing the prevention of collisions and groundings. According to statistics (Pilatis, Pagonis, Serris, Peppa, & Kaltsas, 2024), the number of ship collisions and groundings has not appreciably changed over the last ten years despite the growing technology. Notably, serious concerns, about the secondary disasters resulting from collisions and groundings, for example, loss of human life and oil spills, are evident. (Rosario La Pira, 2010)

2.1.3 Operational Efficiency and Cost Savings

Furthermore, operational efficiency in the maritime industry is significantly enhanced by GPS technology as it enables shipping companies to optimise routes and schedules based on real-time data, including weather conditions, ocean currents, and traffic patterns. Besides, by adjusting courses to take advantage of favourable conditions, shipping companies can maximise their earnings by reducing vessels' fuel consumption, lowering operational costs, and minimising any possible environmental impact. On top of that efficient route planning also contributes to shorter transit times, improving the reliability and profitability of shipping services. However, GPS spoofing can disrupt these optimised routes, leading to increased fuel consumption, higher operational costs and delays. When GPS data is compromised, vessels may burn more fuel due to less efficient routing, leading to higher emissions and a larger carbon footprint. This not only contradicts global efforts to combat climate change but also exposes shipping companies to stricter environmental regulations and potential sanctions.

2.1.4 Regulatory Compliance

On another note, regulatory compliance is heavily dependent on GPS and GNSS international maritime regulations, such as those by the International Maritime Organization (IMO), which often require vessels to be equipped with satellite navigation systems so as to meet safety and traffic management standards. As these regulations are designed to enhance the safety of life at sea and protect the marine environment; GPS and GNSS provide the reliable positioning data needed to meet these regulatory requirements, avoiding penalties and ensuring clear access to international ports and shipping lanes. Thus, Spoofing attacks can lead to non-compliance, legal

penalties, and restricted access to critical maritime infrastructure. In addition, IMO has also recognized the importance of cybersecurity in the maritime sector. At this point it is worth noting that as of June 18, 2024 IMO created the “International Maritime Cyber Security Organisation (IMCSO)” and its mission is to enhance cybersecurity risk assessment across the maritime industry (IMSCO - INTERNATIONAL MARITIME CYBER SECURITY ORANISATION, 2024). On that point, IMO has agreed that recommendations for cybersecurity risk management should be integrated into existing management procedures and complement security management practices already in place. Consequently, the PDCA (Plan, Do, Check, Act) process should be implemented. The first step is to define security objectives, taking into account the requirements of both the IMO and other stakeholders. Based on these objectives, an implementation plan should be developed by shipping companies to eliminate suitable obstacles. The next step is to continuously monitor the effectiveness of cybersecurity measures and thus corrective and preventive actions should be implemented based on the findings of internal and external audit reports (DNV, 2021).

Additional guidelines and standards introduced by IMO include:

a) Guidelines for cybersecurity on ships issued by BIMCO, ICS, INTERCARGO, INTERTANKO, etc., which analyze threats, vulnerabilities, probability assessment, impact assessment, as well as the development of protection and detection measures.43

b) ISO/IEC 27001:201844 standard concerning Information Technology, Security Techniques, Information Security Management Systems published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and

c) the Framework for Improving Critical Infrastructure Cybersecurity of the National Institute of Standards and Technology (NIST Framework), which more specifically mentions the functional elements for effective cyber threat management, used for understanding, detecting, and prioritising actions to reduce risk

The European Union Agency for Cybersecurity (ENISA) published in 2011 the first EU report on the challenges of cybersecurity in the Maritime Sector. This report highlights basic knowledge as well as existing initiatives as the basis for cybersecurity. Finally, high-level recommendations are given for addressing these risks. (First EU-report on Maritime Cyber Security, 2022) This publication is also one of the few services to develop recommendations for cybersecurity in ports. In 2020, it published guidelines to provide port operators with a set of best practices to assist in identifying and evaluating cyber risks and determining appropriate security measures. ENISA's new guidelines - Cyber Risk Management for Ports were drafted in collaboration with several ports in EU member states (ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2020). The Network and Information Security Directive (NIS Directive46) is the first EU attempt to legislate cybersecurity and applies to all EU countries. This legislation includes critical sector agencies that largely rely on information networks and are referred to as Operators of Essential Services (OES). In these sectors is shipping as well as transport, energy sectors, etc. As OES of the shipping sector are defined shipping companies, port authorities, port facilities, and ship traffic services. Furthermore, the Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce cyber and physical infrastructure risks. It connects stakeholders across industry and government, providing resources, analyses, and tools to help them establish their own cybersecurity, communications, and physical security and resilience. CISA also oversees the Maritime Sector Coordinating Council (Maritime SCC), which facilitates emergency preparedness and coordinates response efforts between the domestic maritime sector and the government (CISA - CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY).

2.1.5 Cargo Tracking Application

Another critical application of GPS in the maritime industry is cargo tracking. The available technologies on cargo tracking allow for real-time monitoring of cargo movement from origin to destination, while enhancing supply chain management by providing stakeholders with the ability to track the status and location of shipments. Positively, improved cargo tracking facilitates better inventory management, reduces theft or loss risks, and enhances logistics coordination are managed. On top of the potential for GPS spoofing to obscure the true location of cargo presents significant risks to supply chain integrity and security; GPS facilitates the automation of the pick-up, transfer, and placement process of containers by tracking them from port entry to exit. While millions of container shipments are being placed in port terminals annually, the use of GPS has managed to greatly reduce the number of lost and/or misdirected containers and lowered associated operation costs. Finally it is worth noting, that efficiency in cargo tracking can be achieved by using block chain technologies. Same seems to be becoming noticeable lately as its use was boosted lately by big shipping companies like DNV (DNV, 2023)

2.2. Implications of Loss of Availability and Integrity of GPS for Merchant Marine Vessels

Loss of availability and integrity of GPS represents a profound challenge for the vessels, with far reaching implications across multiple sectors of marine operations. Nowadays, the GPS is a cornerstone of modern navigation and operational efficiency; as a disruption on it's reporting can lead to severe consequences that impact safety, economic performance, regulatory compliance, as well as environmental stewardship.

2.2.1 Navigational Errors and Increased Risk of Accidents

Modern integrated bridge systems fundamentally depend on the data supplied by a vessel's GNSS receivers, presuming that the position fixes obtained from surrounding GNSS signals are both accurate and dependable. However, this assumption is significantly undermined in cases of GNSS spoofing since during such incidents, spoofed receivers transmit erroneous position data manipulated by an attacker through fraudulent GNSS signals. This enables the attacker to alter the ship's actual along-track and cross-track positions by providing the autopilot system or bridge crew with positions that are intentionally misaligned with the vessel's true location. The ramifications of GNSS spoofing go beyond mere system-level interference, impacting specific navigation and collision avoidance instruments. Systems such as the automatic radar plotting aid (ARPA), the automatic identification system (AIS), the dead reckoning system integrated into the ship's electronic chart display and information system (ECDIS), and the satellite compass are all vulnerable to producing dangerously misleading information during a GNSS spoofing incident. Any possible jeopardisation of these systems underscores the urgent necessity for effective countermeasures against GNSS spoofing to maintain the integrity and reliability of navigation systems. This situation eventually manages to highlight the pressing need for robust countermeasures against GNSS spoofing to ensure the integrity and reliability of navigation systems.

2.2.2 Economic Impact and Operational Disruptions

Another critical domain reliant on the availability and reliability of GPS is its operational efficiency. Contemporary merchant marine vessels, along with weather reporting agencies, utilize GPS technology to enhance their routing and scheduling by incorporating real-time information regarding weather patterns, ocean currents, and maritime traffic. This strategic optimization leads to a reduction in fuel consumption, operational expenses, and transit durations, thereby enhancing the overall profitability and sustainability of shipping operations. In instances where GPS data is either unavailable or unreliable, vessels are compelled to navigate in a less efficient manner, often resulting in extended voyages, increased fuel usage, higher emissions, and escalated operational costs. The economic ramifications of such inefficiencies can be significant, especially for shipping firms that operate with narrow profit margins. Additionally, cargo tracking is profoundly impacted by the absence of GPS availability and integrity. GPS facilitates real-time monitoring of shipments, offering stakeholders timely updates on the location and condition of cargo. This level of transparency is essential for effective supply chain management, enabling improved coordination, inventory oversight, and logistical planning. Interruptions in GPS data can obscure the actual whereabouts of cargo, leading to delays, misdeliveries, and heightened risks of theft or loss. Such disruptions can erode customer trust and satisfaction, potentially damaging the reputation and competitive edge of shipping companies.

2.2.3 Compliance with International Maritime Regulations

Furthermore, disruptions in GPS technology also significantly affect another vital aspect, this of the regulatory compliance. Numerous international maritime regulations, particularly those established by the International Maritime Organization (IMO), mandate that vessels be equipped with GPS or comparable satellite navigation systems to guarantee safety and adherence to traffic management protocols. A failure in GPS availability or integrity can lead to violations of these regulations, placing shipping companies at risk of legal repercussions, fines, and limitations on port access. Furthermore, non-compliance heightens the likelihood of maritime accidents, thereby exacerbating the associated legal and financial consequences. Consequently, the loss of GPS availability and integrity, particularly due to a spoofing attack, poses a serious challenge for merchant marine vessels, impacting navigation safety, operational efficiency, cargo tracking, regulatory adherence, environmental considerations, and the progress of maritime technology. It is imperative for the maritime industry to prioritize the implementation of effective countermeasures and contingency strategies to address the risks linked to GPS disruptions, thereby safeguarding the ongoing safety, efficiency, and sustainability of global shipping operations.

3. GPS Spoofing Attacks: Mechanisms and Execution

3.1 What is GPS Spoofing?

When defining GPS spoofing, - one can refer to it, as GPS signal spoofing or GNSS (Global Navigation Satellite System) spoofing - it is noted to be a method employed by attackers to alter or fabricate GPS signals, and thereby misleading GPS receivers, including those utilized on maritime vessels such as ships and boats. The ramifications of this practice can be significant, affecting navigation, safety, and security in maritime operations. Vessel specific GPS spoofing entails the transmission of fraudulent GPS signals to mislead a vessel's GPS receiver. These deceptive signals can cause the receiver to inaccurately perceive its location, speed, or direction of travel. To mitigate the risks associated with GPS spoofing in the maritime domain, a range of countermeasures can be adopted.

Figure 1: GPS Display at Vessel's Bridge (JRC)

There are three primary methods to compromise a GPS receiver:

- Blocking

Blocking refers to the act of obstructing the satellite signal from reaching the receiver's antenna. This can be achieved through physical means, such as damaging or removing the antenna. The result of blocking is a disruption in GPS signal reception, which prevents the receiver from accurately determining its position.

- Jamming

Jamming involves overwhelming a GPS receiver with noise or other signals, thereby hindering its ability to track legitimate GPS signals. This form of attack is commonly known as a denial of service (DoS) attack. Jamming interferes with the receiver's capacity to lock onto and process authentic satellite signals, ultimately leading to a total loss of GPS functionality.

- Spoofing

Spoofing, which is the primary focus of this analysis, entails an attacker substituting the genuine satellite signal with a fraudulent one. In contrast to blocking or jamming, spoofing is a covert attack that misleads the GPS receiver into calculating an erroneous position based on the counterfeit signal. This technique is more advanced and discreet compared to the more overt tactics of blocking and jamming.

3.2 How Spoofing Attacks Are Executed

For a spoofing attack to be executed, spoofed signals are required. These required spoofing signals can be generated using satellite simulators, which are advanced pieces of equipment available today. These simulators can create counterfeit signals that mimic the characteristics of genuine GPS signals. Practically, for a spoofing attack to be successful, it is crucial that the received power of the spoofing signal exceeds that of the legitimate signal. This is because the GPS receiver tends to lock onto the strongest signal it receives. Therefore, by overpowering the legitimate signal, the spoofing signal effectively jams the authentic GPS signal, leading the receiver to operate with the forged signal as its input. Consequently, the GPS receiver computes the location based on the falsified information induced by the spoofer. At this point, it is worth noting that for all the above to take place a “Spoofing device” oughts to be created. Even though it’s creation can be of a cost on the lower side if the GPS receiver to be attacked is quite small, it is its deployment on the field that can be extremely expensive so that for all the above and below conditions to be able to be met. The process of executing a spoofing attack can be quite sophisticated. For instance, an adversary could "invert" the navigation solution it wishes to impose on the target GPS receiver. This inversion involves estimating the positions of the satellite constellation and then configuring the corresponding NAV message values to reflect these falsified positions. Beyond the straightforward manipulation of time data, such as falsifying the time or the week to influence the receiver's internal clock, the adversary can undertake more nuanced alterations of NAV message parameters. These parameters include the mean anomaly at reference time, which describes the angular offset between the satellite's position at the reference time and its perigee, the satellite's eccentricity, and the rate of right ascension (Schmidt, A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures, 2016).

On top of direct signal generation, spoofed signals can also be created based on previously received GNSS signals. In this method, the adversary records authentic NAV messages and later re-transmits them. Alternatively, the adversary may synthesise new messages by combining parts of the recorded messages. This type of attack, known as meaconing a specific form of replay attack, involves the deliberate recording and subsequent re-broadcasting of GNSS signals, causing the GPS receiver to compute its position based on outdated or manipulated data (Papadimitratos, 2008). This can subsequently lead to significant navigation errors. The ability to generate and manipulate spoofing signals highlights a significant vulnerability in GNSS systems. The techniques involved in spoofing and meaconing demonstrate the complexity and potential impact of these attacks. The sophistication required to carry out such attacks indicates that adversaries need considerable technical expertise and resources. Nonetheless, the availability of satellite simulators and the knowledge of GNSS signal structures make these attacks feasible for well-equipped adversaries (Hengqing Wen, Countermeasures for GPS Signal Spoofing, 2005).

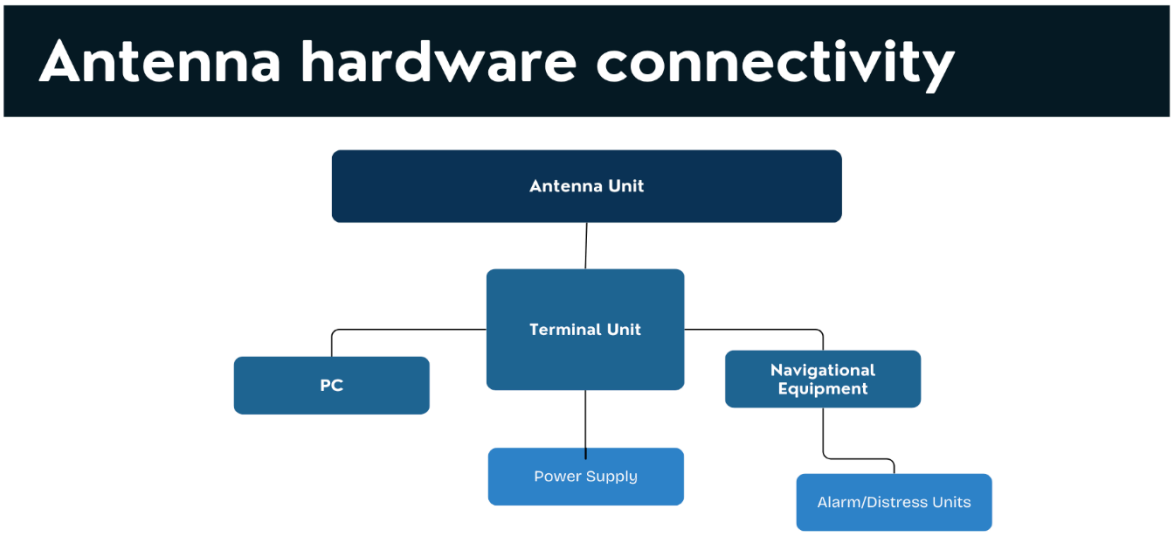

Figure SEQ Figure * ARABIC 2: Antenna hardware connectivity example

The primary objective of GPS spoofing is to deceive the receiver by providing it with a misleading signal. This causes the receiver to utilise these counterfeit signals in its positioning calculations and thus resulting in an erroneous position solution. In other words, the GPS P-code, used primarily for military purposes, is heavily encrypted, making it difficult to spoof. In contrast, the civilian GPS signal uses a code, known as the C/A code, that is highly susceptible to spoofing attacks. This vulnerability arises because the signal structure, spread spectrum codes, and modulation methods of the C/A code are publicly accessible, allowing attackers to replicate and manipulate these signals. However, one ought to note that by Flag requirements, onboard there are two antennas and two GPS Systems to prevent navigational issues in case of hardware failure of one of the systems. This would mean that for the Spoofing attack to be successful, the attacker would have to feed both antenna receivers with the counterfeit and alternated signals. Both antennas still do receive signals from the same source, e.g. satellite, ground source, but proceed with calculations of their own.

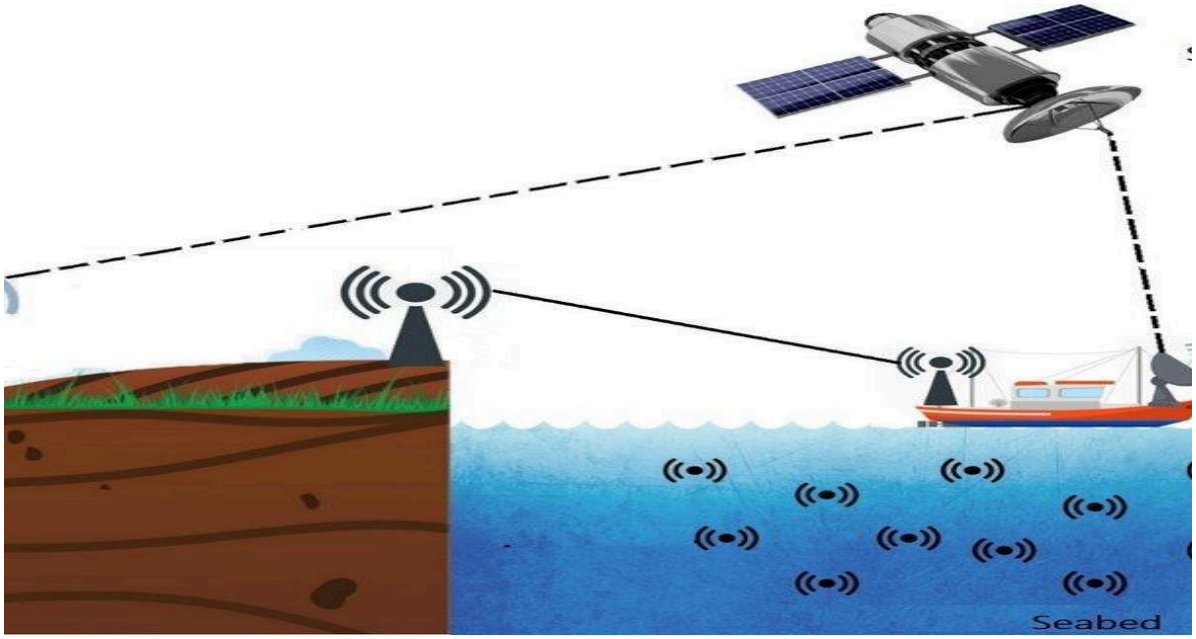

Figure SEQ Figure * ARABIC 4: Satellite-Vessel-Ground Antennas Connectivity

On the practical implementation of Spoofing attacks, the adversary targets the GPS receiver. The attacker uses a simulator to generate and transmit false signals to the GPS receiver, thereby manipulating the reported position and speed of the vessel. For a spoofing attack to be effective, several conditions must be met (Schmidt, A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures, 2016):

- Interception of the Antenna Signal: The genuine signal from the GPS satellite must be intercepted or broken off, allowing the counterfeit signal to dominate.

- Locking onto the Counterfeit Signal: The GPS receiver must be deceived into locking onto the counterfeit signal instead of the true satellite signal. This requires the fake signal to mimic the characteristics of the legitimate signal closely. The only detectable differences between legitimate satellite signals and spoofed ones may be in discrepancies in timing, signal direction, strength, doppler shift (relative speed between satellite/spoofer and receiver), and signal-to-noise ratio.

- Proximity of the Attacker: The attacker must be in relatively close proximity to the target to ensure the fake signals are strong enough to override the authentic satellite signals. Broadcasting of fake GPS signals must occur from a location near the target to maintain the integrity and strength of the spoofed signals.

By fulfilling these conditions, an attacker can effectively manipulate the GPS receiver, leading to incorrect position calculations and potentially hazardous navigation errors (MITRE, 2022).

Scientifically, each GPS satellite broadcasts two distinct signals: a military signal and a civilian signal. The vast majority of GPS users, including most Department of Defense (DoD) users, can only utilise the civilian code GPS signal. This civilian code is also used by merchant marine vessels and consists of two main data signals and a carrier wave, as depicted in Figure 1.

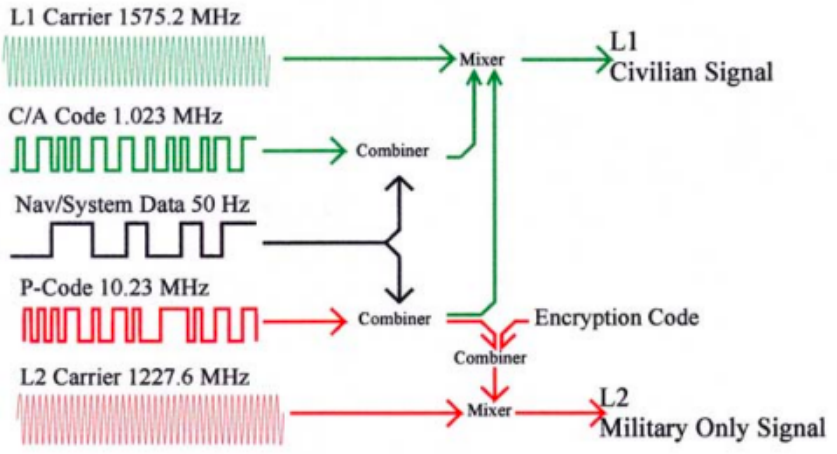

Figure SEQ Figure * ARABIC 5: GPS Carrier Waves CITATION Jon03 \l 1033 *(Jon S. Warner, 2003)*

The Nav/System data provides the GPS receiver with critical information regarding the position of the satellites and precise timing data derived from the atomic clocks aboard the satellites. Each satellite is assigned a unique identification code, known as the C/A code, which repeats every millionth of a second. The Nav/System information is combined with the C/A code and then modulated within a carrier wave.

The GPS receiver simultaneously locks onto signals from several GPS satellites. For simplicity, we will focus on the process of locking onto a single satellite. The receiver is pre-programmed with the C/A identification string associated with each satellite. It continuously listens for the GPS signals from space, and upon detecting a satellite signal, it refers to the C/A code to identify the satellite. The receiver then generates an internal C/A code that matches the satellite's code. This internally generated code is compared against the repeating C/A code from the satellite, allowing the receiver to determine the signal's travel time (ΔT), as illustrated in Figure 2.

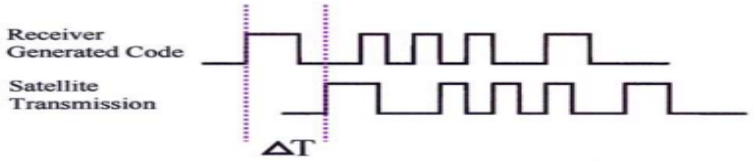

Figure SEQ Figure * ARABIC 6: Example of GPS signal time delay CITATION Jon03 \l 1033 *(Jon S. Warner, 2003)*

Once the travel time (ΔT) is determined, the receiver calculates its distance to the satellite using the formula: Distance = ΔT x Speed of Light. However, knowing the distance to a single satellite is not sufficient for accurate positioning. Even with precise knowledge of the satellite's position, this information only indicates that the receiver is somewhere within a fixed distance from the satellite.

Accurate positioning requires the receiver to determine distances from multiple satellites simultaneously, usually four. As shown in Figure 3, the ranges measured by the GPS receiver from different satellites typically do not converge at a single point. This discrepancy is due to

clock errors in the GPS receiver, which is less precise than the atomic clocks on the satellites. The area of overlap between the incorrect ranges indicates the receiver's approximate position.

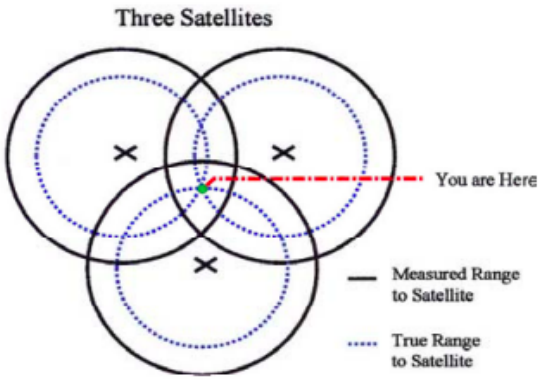

Figure SEQ Figure * ARABIC 7: 2-D representation of finding a position CITATION Jon03 \l 1033
(Jon S. Warner, 2003)

The GPS receiver then interpolates this overlap area to find the centre, providing two crucial pieces of information: the receiver's position and the clock error. The more satellites involved in this process, the smaller the overlap area, resulting in a more accurate position fix. Initially, the position is determined in an X, Y, Z Earth-centred/Earth-fixed coordinate frame, and subsequently converted to latitude, longitude, and altitude coordinates. If the above is executed properly, it means that the attacker can modulate the ship's true along-track and cross-track positions by feeding apparent positions to the ship's autopilot system or to its bridge crew that are falsely offset from the ship's true position and thus successfully completing his intended attack.

3.3 Assets

In accordance with Chapter V of the SOLAS Convention, vessels engaged in navigation are required to comply with specific standards aimed at ensuring the safety and efficiency of maritime operations. The latest edition of SOLAS 2020 delineates these requirements, which include vital provisions for navigational equipment and procedures. The primary provisions, deemed essential for effective navigation, are typically situated on the vessel's Bridge and include the following:

- Nautical Charts and Publications: It is imperative for vessels to carry nautical charts and publications to aid in the planning and visualization of the ship's intended route. These materials are vital for accurately plotting and tracking positions during the voyage, thereby facilitating informed decision-making and promoting safe navigation.

- Electronic Chart Display and Information System (ECDIS): The Electronic Chart Display and Information System (ECDIS) is recognized as a compliant alternative to the traditional paper charts mandated by SOLAS Chapter V. ECDIS offers a digital solution that provides extensive navigational data and improves situational awareness for mariners.

- Backup Arrangements: When electronic systems are employed for navigational tasks, vessels must implement backup arrangements. These contingencies are crucial for

maintaining the continuity of navigational functions and fulfilling operational requirements, thus reducing the likelihood of system failures or malfunctions.

- Global Navigation Satellite System (GNSS) Receiver: Vessels are required to be equipped with a receiver for a global navigation satellite system (GNSS), a terrestrial radionavigation system, or other appropriate means capable of automatically determining and updating the ship's position. This stipulation ensures dependable positioning and navigation capabilities throughout the voyage, thereby enhancing navigational precision and safety.

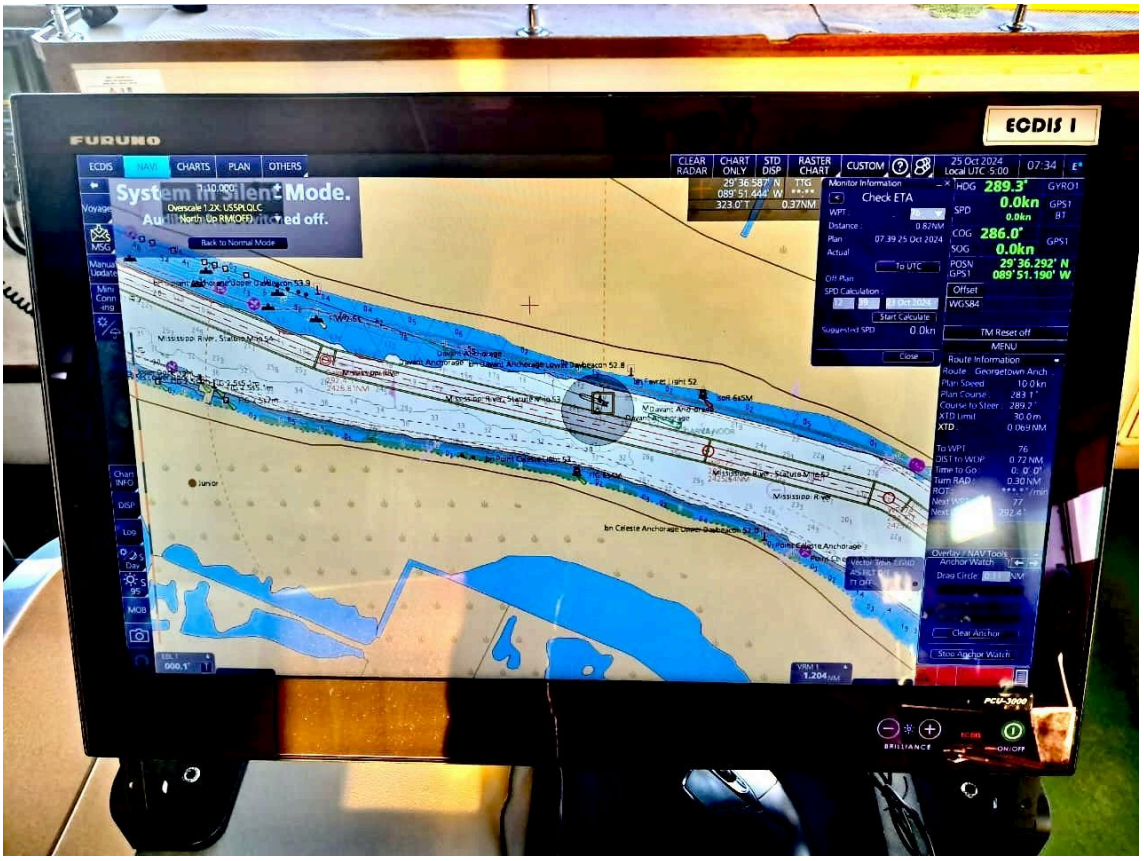

Figure 8: ECDIS Display at Vessel's Bridge

The provisions specified in SOLAS Chapter V highlight the paramount importance of these requirements in safeguarding maritime operations. Ultimately, by adhering to these requirements, vessels can uphold the highest standards of navigational safety and operational efficiency, thereby contributing to the overall safety and security of maritime transportation (IMO - SAFETY OF LIFE AT SEA, 2020).

Basis on the above and already established knowledge on GPS Spoofing equipment one can derive the below as assets of a GPS Spoofing Attack are involved:

- Spoofing Device: The fundamental component of a GPS spoofing attack is the spoofing device, which is designed to produce fraudulent GPS signals, e.g. an Antenna. This

device plays a crucial role in delivering misleading positional data to the navigation systems of the targeted vessel. The spoofing device should be fully capable of generating and transmitting counterfeit signals. Same can be supported by software and programs that can generate fake signals as well.

- Signal Source: To fabricate counterfeit GPS signals, the attacker must have access to a dependable signal source. This may involve altering legitimate GPS signals or generating entirely fictitious signals from the ground up using specialized tools or software. In other words, a mobile platform is needed; from where the spoofing device can operate. This, while taking into notice that the closer the proximity of the attacker to his target, the higher the control he has over his attack. Also, a system with signal transmission capability is required, so as to overpower the authentic satellite signals that are received by the vessels.

- Knowledge and Expertise: The effective implementation of a GPS spoofing attack necessitates a deep understanding of GPS technology, signal modulation, and navigation systems. The attacker must have the requisite knowledge and skills to manipulate GPS signals proficiently while evading detection. Knowledge not only of GPS signal manipulation, but also of vessels' operation. As familiarity with the way a vessel operates, e.g. within port, can differentiate between success and failure of the attack.

- Access to Target Vessel's Navigation Systems: The attacker must gain access to the navigation systems of the target vessel to successfully inject counterfeit signals. This may require physical access to the vessel's GPS receiver or exploiting weaknesses in its communication protocols to remotely introduce spoofed signals. The access to the vessel's Nav systems can be direct but can also be indirect, by using available knowledge on vessel's navigation configuration and set up, e.g. available GPS antennas, electronic charts, ECDIS, autopilot, as well as on board sensors.

- Timing and Location Information: Precise timing and location data regarding the target vessel and its environment are essential for synchronizing the spoofed signals with authentic GPS signals, e.g. using AIS. This synchronization enhances the believability of the spoofed signals. A monitoring mechanism could be real-time feedback loop as it would allow the attacker to dynamically adjust the parameters of his attack.

- Monitoring and Feedback Mechanism: Throughout the attack, the attacker may need a monitoring and feedback system to evaluate the effectiveness of the spoofing in real-time. This could be done by using AIS tracking or even by visual observation

- Concealment Measures: To prevent detection and attribution, the attacker might implement concealment strategies such as encryption or anonymizing their communications. These strategies assist in obscuring the identity and location of the attacker during the operation.

- Backup Plans and Contingencies: In the event of failures or unforeseen circumstances, the attacker should have alternative strategies and contingency plans in place. This could include alternative methods of spoofing or escape routes to evade capture.

By leveraging the abovementioned assets, an attacker can effectively execute a GPS spoofing attack by manipulating the navigation systems of the target vessel and potentially causing navigational errors or safety hazards as mentioned previously.

3..4 Examples of GPS Spoofing Incidents in Maritime Industry

Figure SEQ Figure * ARABIC 9: Furuno GNSS Bridge Display CITATION FUR \l 1033 *(FURUNO, n.d.)*

3.4.1 The University of Texas Exercise: The White Rose

In July 2013, a pivotal GPS spoofing experiment was conducted by researchers from the University of Texas. An experiment which has since been recognized as a significant case study in maritime security. Utilizing equipment valued at a mere $3,000, they successfully took command of the navigation system of a highly valuable mega-yacht, estimated to be worth $80 million. This yacht was equipped with state-of-the-art digital systems and operated by a skilled and well-trained crew. It is noteworthy that only the captain and the owning company were aware of this exercise, which ensured the integrity of the experimental conditions. The operation specifically occurred in June 2013, involving a yacht named White Rose of Drachs, which was en route from Monaco to Rhodes. While the yacht was navigating international waters, approximately 30 miles off the Italian coast, students Jahshan Bhatti and Ken Pesyna, guided by Assistant Professor Todd Humphreys, commenced the spoofing operation. They transmitted a weak yet precisely calibrated GPS signal from their spoofing device to the yacht's two GPS antennas. The counterfeit signals produced by the team gradually overpowered the authentic signals from the GPS satellites, allowing the researchers to surreptitiously seize control of the yacht's navigation system.

This technique of GPS spoofing is markedly different from GPS jamming. After gaining control of the navigation system, the researchers employed a strategy of subtly modifying the yacht's course through gradual maneuvers. These maneuvers redirected the yacht only a few degrees from its original path at a time, making the changes almost imperceptible to the crew. Whenever the navigation system reported a discrepancy in the yacht's location, the crew, following standard operating procedures, initiated a course correction. However, each course correction, unbeknownst to the crew, actually compounded the deviation from the intended route. Eventually, after several manoeuvres of such kind, the yacht had been deceived into following a

parallel trajectory that was hundreds of metres away from its originally planned course. This sophisticated manipulation demonstrated the efficacy of GPS spoofing in altering a vessel's course without the crew's awareness, showcasing a significant vulnerability in maritime navigation systems.

3.4.2 GPS Spoofing Incidents in Shanghai: Incident Involving M/V Manukai

As reported on the article published at "Safety4Sea", in 2019, investigations revealed a significant prevalence of GPS spoofing that impacted numerous vessels in Shanghai (SAFETY4SEA, 2020). This surge in incidents highlighted the growing global threat posed by GPS spoofing. Despite thorough inquiries, the identities of those responsible for these spoofing attacks and their ultimate intentions remain unclear. Various theories have been suggested to account for these occurrences. One credible hypothesis indicates that smugglers may be utilizing such tactics to avoid detection and facilitate illicit operations. Another theory suggested that the Chinese government could be conducting extensive tests of a new electronic weapon, potentially in preparation for its deployment in contentious areas like the South China Sea. In July 2019, the container ship M/V Manukai was navigating towards the busy port of Shanghai via the Huangpu River, a significant tributary of the Yangtze River. The ship's captain, while observing the navigation displays, noticed another vessel traveling at approximately seven knots within the same channel. Abruptly, the other vessel vanished from the screen, only to reappear moments later, appearing to be docked. This occurrence repeated several times, leading the captain to visually verify the position of the other vessel, which remained stationary at the dock throughout the incidents. As the M/V Manukai was preparing to approach its assigned berth, the bridge was suddenly inundated with multiple alarms. The ship's GPS systems lost their signals, the Automatic Identification System (AIS) transponder malfunctioned, and an emergency system reliant on GPS failed to provide accurate positioning. Despite these obstacles, the M/V Manukai successfully docked. The captain subsequently submitted a report to the United States Coast Guard Navigation Center. A nearby vessel encountered a similar problem, where its true position and speed were replaced by erroneous coordinates. Such spoofing incidents can result in navigation errors, collisions, or groundings. On the same day that the M/V Manukai encountered these difficulties, an intense interference was recorded, affecting nearly 300 ships. Data examined by C4ADS (The Center For Advanced Defense Studies Inc) regarding the Shanghai incidents revealed a different pattern compared to previous hacking instances observed in Russian waters, where ships were spoofed to a single point. In Shanghai, ships appeared to "jump" to different locations every few minutes, forming rings on the eastern shore of the Huangpu River. These attacks impacted all GPS-reliant devices on the ships, rather than the ships themselves (CENTER FOR ADVANCED DEFENCE STUDIES).

3.4.3 Recent Incidents: Incidents in coastal areas and ports

The last few years a series of GPS spoofing incidents have been occurring around the world and their reports show the rise of global security issues. These notable series of spoofing incidents need to be investigated further so as for those involved to gain better understanding on this uprising issue. Some cases involving GPS Spoofing attacks are the following:

- People's Republic of China

In 2020, numerous GPS spoofing incidents were reported in coastal areas and ports of the People's Republic of China. The Center for Advanced Defense Studies (C4ADS) discovered that hundreds of vessels, particularly in Shanghai and the Huangpu River, were affected over several months. These incidents involved false GPS signals being broadcast to mislead ships' navigation systems, causing significant disruptions in maritime operations. The widespread and persistent nature of these spoofing activities raised concerns about the security and reliability of navigation systems in one of the world's busiest maritime regions, indicating potential motives ranging from commercial interference to strategic military advantages (SAFETY4SEA, 2020).

- Eastern and Central Mediterranean, Suez Canal

  The US Maritime Administration (US MARAD) reported significant GPS interference incidents in the Eastern and Central Mediterranean, including the Suez Canal. These disruptions led to lost GPS signals, adversely affecting navigation and operations in critical maritime routes. Notably, the areas between Libya and Malta, Port Said in Egypt, and near Cyprus were identified as hotspots for such interference. The interference not only posed risks to commercial shipping but also threatened regional maritime security and safety, highlighting the vulnerabilities of GPS-dependent navigation systems in geopolitically tense areas.

- Strait of Hormuz

  The Strait of Hormuz has been identified as a hotspot for GPS spoofing, where commercial vessels faced severe navigation issues due to false GPS signals. These spoofing attacks contributed to a series of high-profile incidents, including attacks on ships, the downing of drones, and the seizure of the UK-flagged 'Stena Impero'. The region's strategic importance as a major oil transit route made it a target for such activities, reflecting broader geopolitical tensions and the use of GPS spoofing as a tool for regional power struggles. These incidents underscored the critical need for enhanced navigation security in one of the world's most vital maritime chokepoints. (Lott, 2022)

- Russian Federation

  Reports from the Center for Advanced Defense Studies (C4ADS) revealed that the Russian Federation has been extensively using GNSS (Global Navigation Satellite System) spoofing, posing significant threats to maritime navigation. Analysis indicated that GNSS spoofing patterns were prevalent in Russia, Crimea, and Syria, suggesting both tactical and strategic applications of this technology. These activities included misleading navigation systems of vessels, potentially for military and security purposes, to protect sensitive areas or disrupt foreign operations. The systematic use of GNSS spoofing by Russia highlighted the growing use of this technology as a tool for strategic advantage in modern geopolitical conflicts.

- Black Sea Incident

  In 2017, a significant GPS spoofing attack in the Black Sea affected approximately 20 vessels, misleading their GPS receivers. The disruption was confirmed when a shipmaster in the Black Sea reported the issue to the US Coast Guard Navigation Center (NAVCEN). The spoofing attack caused the ships' navigation systems to display incorrect locations, posing serious risks to maritime safety and navigation. This incident brought international attention to the vulnerabilities of GPS systems and the potential for malicious actors to exploit these weaknesses, prompting calls for improved resilience and countermeasures in maritime navigation technologies (Safety4Sea, 2020).

- As per report of the Australian Transport Safety Bureau (ATSB) (ATSB - AUSTRALIAN TRANSPORT SAFETY BUREAU, 2022), on the 4th of May 2022, a near grounding of a Bulk carrier during her transit through Hydrographers Passage under the conduct of a coastal pilot. The pilot on board suddenly noticed that one of the ship’s 3 GPS units began outputting incorrect positional data. The vessel’s position was then incorrectly displayed on the electronic chart display and information system (ECDIS), radars and automatic identification system. The pilot ordered a timely heading change and the ship’s course was altered away without further incident. In this case, though no GPS Spoofing was proven to be the cause of GPS malfunctioning, this incident showcases the major issues that come up once antennas face issues of any kind.

4. Countermeasures Against GPS Spoofing Attacks for Merchant Marine Vessels: Hardware and Software Solutions

Nowadays, the maritime industry increasingly relies on GPS for navigation, safety, and operational efficiency. Consequently, the threat of GPS spoofing attacks where malicious entities transmit false GPS signals to deceive receivers poses a significant risk to the integrity and safety of maritime operations (Michael A. Lombardi, 2001). To mitigate these risks, a comprehensive approach involving both hardware and software countermeasures is essential. This section will explore the various strategies and technologies that can be used and applied accordingly so as to protect merchant marine vessels from GPS spoofing attacks. Typically, existing countermeasures against spoofing attacks can generally be categorised into two classes: cryptographic techniques and anomaly detection at the signal level (Hengqing Wen, Countermeasures for GPS Signal Spoofing, 2005).

TEST STATISTIC	FUNCTION	LIMITATION
Absolute signal power	Limit the spoof signal power	Antenna attitude and environment related
Signal power changing rate	Detect stationary spoof station	Antenna attitude and environment related
Relative signal strengths on all carriers	Detect spoofing single carrier	Affected by ionosphere refraction
Range rate	Bound the phase and code range rate	Related to GPS receiver's moving direction
Doppler shift	Detect spoof that uses one transmitter to spoof all satellites	None
Correlation peaks	Correlate L1/L2 binary message	Low performance on Y-code
GPS signal after removing all navigation data	Recover authentic data	Requires low spoof/authentic signal power ratio
Range differences; phase/code, L1/L2	Identify signal source	Needs to be L1/L2 receiver
Ephemeris data	Verify ephemeris data including satellite position	None
Signal power and data	Jump detection	None

Table 1: Signal based countermeasures Classification

4.1 Hardware-Based Countermeasures

The threat of GPS spoofing in the maritime industry necessitates a multifaceted defense strategy incorporating both hardware and software countermeasures. Multi-frequency and multi-constellation receivers, advanced antennas, signal authentication, inertial navigation systems, and signal strength monitoring are critical hardware solutions that enhance the resilience of GPS against spoofing attacks. The hardware based countermeasures are complemented by are software-based strategies, including advanced signal processing algorithms, cross-referencing with alternative data sources, cryptographic verification, real-time anomaly detection, crowd-sourced data validation, and regular firmware updates. The implementation of these countermeasures collectively ensures a robust defence against GPS spoofing, safeguarding the integrity of navigation, operational efficiency, cargo tracking, regulatory compliance, and the overall safety of merchant marine vessels. As technology evolves and the maritime industry continues to adopt more advanced navigation systems, the integration of these countermeasures will be crucial in maintaining the security and reliability of GPS-based operations.

4.1.1 Multi-Frequency and Multi-Constellation Receivers

One of the most effective hardware countermeasures is the use of multi-frequency and multi-constellation GPS receivers. These receivers can process signals from multiple satellite constellations (such as GPS, GLONASS, Galileo, and BeiDou) and across different frequency bands (Shinya Kowada, 2022). This way by comparing signals from different sources, the receiver can identify discrepancies indicative of spoofing, since the redundancy provided by multiple constellations makes it significantly harder for attackers to spoof all signals simultaneously. However, it is worth noting that such systems are expensive to be bought and installed, as well as keep maintenance of.

4.1.2 Antenna Enhancements (CRPAs, Phased-Array Antennas)

Advanced antenna technologies can also play a crucial role in mitigating spoofing attacks. Controlled reception pattern antennas (CRPAs) and phased-array antennas are capable of detecting and rejecting signals coming from unexpected directions. These antennas use beamforming techniques to focus on signals from legitimate satellites while ignoring signals from other sources. Additionally, anti-jamming antennas can help reduce the impact of both jamming and spoofing by maintaining the integrity of received signals even in the presence of interference (E. Key).

4.1.3 Signal Authentication

Another important hardware based countermeasure is the use of signal authentication methods. For example, the U.S. military employs encrypted GPS signals that are more resilient against spoofing attacks. While such methods are not yet widely available for civilian use, ongoing research and development aim to introduce similar capabilities for commercial and civilian applications (Musumeci L. &.-1., 2014). Signal authentication involves embedding cryptographic signatures in GPS signals, allowing receivers to verify the authenticity of the signals and reject those that fail verification. However, even if encrypted GPS signals become available for commercial applications, the cost of their system installation and maintenance is something that could be appalling to shipping companies.

4.1.4 Inertial Navigation Systems (INS)

Inertial Navigation Systems (INS) provide an independent means of navigation that can be used to crosscheck GPS data. INS relies on bridge equipment, such as accelerometers and gyroscopes to track the position, velocity, and orientation of the vessel. While INS data can drift over time due to accumulated errors, it is highly reliable over short durations (Musumeci L. &.,

2014). By comparing GPS data with INS outputs, discrepancies can be detected, indicating potential spoofing. Integrating INS with GPS ensures continuous, reliable navigation even when GPS data is suspect, as they are also supported by simple visual configuration, which is possible even at night using constellation navigation.

4.1.5 Signal Strength Monitoring

Hardware solutions can also include monitoring the strength of incoming GPS signals. Legitimate GPS signals from satellites are relatively weak when they reach the Earth's surface. Spoofed signals, which are typically stronger, can be identified through signal strength monitoring (Warner, 2012). If a receiver detects an unusually strong signal, it can raise an alarm or switch to alternative navigation methods, such as INS or dead reckoning, to avoid being misled by spoofed data.

4.1.6 Dual Band GNSS Signal Reception

On the topic of countering GPS/GNSS Spoofing attacks, one cannot fail to mention dual band signal reception. As both Spoofing and noise, due to wireless receipt of signals, interfere with signal reception; dual band receivers can eliminate these challenges. Single band receivers, as already mentioned, use only L1 frequency band (1575.42 MHz). However, dual band receivers can receive signals on L5 band (1176.45 MHz) in addition to L1 band. This way, in the event that the signal reception of L1 is interrupted, L5 band takes over and ensures continuity of signal reception. Another positive aspect of Duals bands is that it is easy to install on board and inexpensive to purchase.

4.2 Software-Based Countermeasures

4.2.1 Signal Processing Algorithms

As previously examined, advanced signal processing algorithms are critical for detecting and mitigating spoofing attacks. Most commonly used algorithms in GPS Systems are two, Kalman filter and velocity renovation, both of which can be used in conjunction with GPS as a basis for location tracking. These algorithms manage to analyse various characteristics of incoming GPS signals, such as time delay, Doppler shift, and signal strength, to identify anomalies (Zahaby, 2009). By exploiting their abilities, theses algorithms are able to detect sudden changes in signal strength as well as unexpected variations in signal timing that are characteristic of spoofing.

4.2.2 Cross-Referencing with Alternative Data Sources

Software solutions are also commonly used so as to involve cross-referencing GPS data with alternative data sources, such as radars, Automatic Identification System (AIS), and visual data from vessel’s cameras. This way by comparing GPS positions with those derived from other sensors available on board, inconsistencies can be identified and thus indicate any potential spoofing. For example, if GPS indicates a sudden and implausible change in the vessel’s position that is not supported by the available AIS data or the radar image, the system can flag the GPS data as potentially spoofed (Jon S. Warner, 2003). However, this has only theoretical application, since on board the vessel’s AIS, radar and GPS are all receiving signals from the same source.

Figure SEQ Figure * ARABIC 10: Radar Display at Vessel's Bridge

4.2.3 Cryptographic Verification

Furthermore, the implementation of cryptographic verification methods in software can enhance the security of GPS signals. When a GPS receiver does receive a signal, it can use the established cryptographic verification methods to verify the cryptographic signature against a trusted public key. The available digital signatures and public key infrastructure (PKI) can be used to authenticate GPS data, thus ensuring that the received signal has not been tampered with (Do Alexis Sanou, 2013). However, in the event that the signature does not match, the signal can be rejected as potentially spoofed and respective alarm is to be raised. At this point, it should be noted that this requires frequent updates to both satellites and receivers.

4.2.4 Real-Time Anomaly Detection

Software-based real-time anomaly detection systems continuously monitor GPS data for signs of spoofing. These systems use statistical and machine learning models to detect deviations from expected GPS behaviour. For example, a vessel's speed and heading should change gradually; sudden, unexplained changes can indicate spoofing. This way the possible real time anomaly detection can ensure that alerts will be raised and that countermeasures will take place with immediate force such as for the crew to alternate on the used navigation methods, while updating vessel's master accordingly. This type of countermeasures will be analysed on chapter 10 using real-life cases of such systems.

4.2.5 Crowd-sourced Data Validation

Another possible approach on the Software side would be Crowd-sourcing data validation. This way it would be possible for the vessels to share their GPS data with nearby ships and shore-based stations at the closest port in order to create a network of cross-verified positions. While comparing position data from multiple sources, the system can identify inconsistencies that suggest spoofing and so succeed in enhancing the reliability of GPS data, as it would become more difficult for attackers to spoof multiple receivers simultaneously. Though this countermeasure applicable on the cybersecurity side, it seems highly unlikely on the shipping side.

4.2.6 Firmware Updates and Patch Management

As per usual practice in both marine and cyber sectors, regular firmware updates and patch management are essential to address known vulnerabilities in GPS receivers. This enables manufacturers to release patches so as to improve the robustness of receivers against possible spoofing attacks and thus ensuring that GPS receivers on merchant marine vessels are kept up to date with the latest security enhancements is a vital aspect of maintaining their integrity and reliability.

4.2.7 Signal Interference Mitigation

On the topic of signal Interference Mitigation used as a counter reaction to a GPS Spoofing attack it is usual that a vessel's GPS antenna, when the vessel nears land, by default is redirecting and picking up signals from the available land antennas. However, so as to avoid and prevent any possible attack in case the land antennas' signal has been compromised; the manufacturers should instead ensure that the vessel's antenna exclusively receives signals from satellites at all times. There are several technical strategies and considerations that can be implemented for this case, consisting of hardware design, antenna positioning, signal processing techniques as well as regulatory compliance (Roddy, 2006).

- Antenna Design and Selection

a. Directional Antennas:

One of the primary strategies is to use highly directional antennas. Directional antennas, such as parabolic dishes or helical antennas, are designed to focus their reception in a narrow beam aimed at the satellite. This would help minimise the reception of off-axis signals, including those from terrestrial sources (Balanis, 2015).

b. Installation of a Low-Noise Block Downconverter (LNB):

The LNB can be mounted at the focal point of the parabolic dish and thus minimising interference. High-quality LNBs with narrow beamwidths are less susceptible to picking up signals from unintended sources.

- Antenna Positioning and Stabilization

a. Azimuth and Elevation Control:

Modern maritime satellite antennas are equipped with motors that continuously adjust their azimuth (horizontal angle) and elevation (vertical angle) to keep the antenna precisely pointed

at the satellite. This is of crucial importance on a moving vessel where the orientation constantly changes due to waves and frequent course adjustments.

b. Stabilised Antenna Platforms:

These platforms use gyroscopes (GYRO) and accelerometers to counteract the motion of the vessel, ensuring the antenna maintains continuously a steady aim at the satellite even in rough seas.

- Frequency Selection and Filtering

a. Frequency Bands:

Satellite communication typically uses specific frequency bands (such as C, Ku, and Ka bands) that are less congested and less likely to overlap with terrestrial signals. Ensuring the vessel's communication system operates exclusively within these bands.

b. Bandpass Filters:

Implementing bandpass filters can significantly reduce the reception of unwanted signals. These filters allow only the desired frequency band to pass through, blocking out signals from terrestrial sources that typically operate on different frequencies.

- Advanced Signal Processing

a. Beamforming:

Beamforming technology can be used to steer the reception pattern of the antenna electronically. By adjusting the phase and amplitude of the signals received from multiple antenna elements, the system can focus on signals coming from the satellite and nullify signals from other directions.

b. Adaptive Filtering:

Adaptive filtering techniques continuously analyze the incoming signal and dynamically adjust the filter parameters to minimise interference by enabling the system to distinguish between the satellite signal and terrestrial interference. Moreover, leveraging constellations of satellites, such as those used in VSAT (Very Small Aperture Terminal) systems, ensures continuous coverage and allows the system to switch between satellites if one is experiencing interference from terrestrial sources (Elbert, 2008). As for the possible regulatory and operational considerations, operators should be aware of the vessel's location and the proximity to coastal areas where terrestrial signals are stronger. This so that they are able to adjust the communication system's parameters or temporarily suspend certain operations while near land can minimise interference.

As a conclusion, by employing a combination of the aforementioned strategies, a vessel's antenna can effectively avoid picking up terrestrial signals and focus exclusively on satellite communications. Thus ensuring a reliable and high-quality connectivity which is essential for a vessel’s safe navigation, communication and operational efficiency at all times.

5. Classification and Feasibility of GPS Spoofing Countermeasures

5.1 Classification of GPS Spoofing Countermeasures

The below classification table provides insight into the varying degrees of complexity and financial investment associated with implementing countermeasures against GPS spoofing attacks. By understanding the relative ease and cost of each countermeasure category, stakeholders and shipping companies can make informed decisions regarding the selection and deployment of appropriate defence mechanisms for protecting merchant marine vessels from spoofing threats.

COUNTERMEASURE	EASE OF IMPLEMENTATION	COST	DESCRIPTION
1. Firmware Updates and Patch Management	Easy	Low	Regular updates to GPS receivers to address known vulnerabilities. Need for minimal hardware changes, as primarily involves software patches
2. Signal Strength Monitoring	Easy	Low	Monitoring signal strength to detect anomalies can be integrated into existing systems with relatively simple software updates.
3. Dual Band GNSS Signal Reception	Easy	Low	Using L1 band and L5 band to ensure continuity of signal reception. Installation of the equipment is simple and cost is minimal.
4. Real-Time Anomaly Detection	Moderate	Low to Moderate	Uses statistical and machine learning models to detect deviations from expected GPS behaviour. Requires software development but no significant hardware changes.
5. Cross-referencing with Alternative Data Sources	Moderate	Moderate	Involves integrating data from radar, AIS, and other sensors. Requires some hardware integration and software development for data fusion.
6. Crowd-sourced Data Validation	Moderate	Moderate	Utilises data sharing and cross-verification among multiple vessels and shore stations. Requires

			network setup and data processing capabilities.
7. Signal Processing Algorithms	Moderate to Hard	Moderate	Advanced algorithms analysing signal characteristics to detect spoofing. Requires significant software development and enhanced processing capabilities.
8. Inertial Navigation Systems (INS)	Moderate to Hard	Moderate to High	Provides independent navigation using accelerometers and gyroscopes. Installation involves adding new hardware and integrating it with existing systems.
9. Cryptographic Verification	Hard	Moderate to High	Involves implementing cryptography for signal authentication. Requires changes at both the transmitter (satellites) and receiver ends, along with secure key management.
10. Antenna Enhancements	Hard	High	Involves deploying advanced antenna technologies like CRPAs, phased-array antennas, and anti-jamming antennas. Requires significant hardware upgrades and installation
11. Multi-frequency and multi-constellation Receivers	Hard	High	Uses receivers that process multiple satellite signals across various constellations and frequencies. Requires advanced hardware and integration with existing navigation systems.

Table 2: Classification of GPS Spoofing Countermeasures by Implementation and Cost

5.2 Feasibility and Realistic Application of GPS Spoofing Countermeasures

As proven in the previous chapters, countermeasures to GPS spoofing attacks are indeed realistic and have practical applications, all while providing solutions to address known vulnerabilities while continuing to improve the security of GPS receivers. This is supported by the use of the latest technological capabilities and ongoing research efforts aimed at enhancing the security of available GPS systems. A simple counter reactive technique as signal strength monitoring can be applied to existing GPS receivers with relatively minor modifications, as it provides a simple but effective way to detect anomalies that indicate spoofing attacks. Additionally, advances in signal processing and machine learning enable real-time anomaly detection in GPS data. Furthermore, integrating data from multiple sources such as radar, AIS and inertial sensors is a feasible approach to validate GPS information and detect spoofing.

Moreover, advances in signal processing algorithms enable more complex analysis of GPS signals to detect spoofing attacks, while they may require additional computing resources. Furthermore, it is worth noting that the Inertial Navigation Systems (INS) can be used in independent navigation using on-board sensors and is usually used in conjunction with GPS for redundancy and reliability. The integration of INS with GPS receivers achieves enhanced resilience against spoofing attacks, while cryptographic techniques offer strong protection against spoofing by providing authentication and verification of the integrity of GPS signals. In addition, advanced antenna technologies, such as Controlled Signal Reception Antennas (CRPAs) and anti-jamming antennas, are available to reduce the effects of spoofing and jamming attacks. However, their use and implementation often comes with higher costs and specialised facilities, even though they are now practical for applications that require high levels of security. Finally, receivers that can process signals from multiple frequencies and satellite constellations offer increased resilience against spoofing attacks. These receivers are already available in commercial and military navigation systems, proving their practical application. Overall, while some countermeasures may require more extensive hardware upgrades or computing resources, all are based on existing technologies and research developments. With continued advances in GPS security and navigation technology, these countermeasures are becoming increasingly standard practice to protect against GPS spoofing attacks in real-world situations.

5.2.1 Technical Feasibility

Various approaches have been proposed and tested to enhance the resilience of GPS receivers against spoofing. A distinguished method is the use of multi-GNSS systems. This includes integrating signals from multiple satellite systems (eg, GPS, GLONASS, Galileo, and BeiDou) to increase complexity for potential attackers and enhance the reliability of received signals. In addition, signal authentication techniques, such as cryptographic authentication and wideband signals, are available to ensure that the signals received by GPS receivers actually originate from legitimate satellites. A different approach involves using array antenna processing. In this method, multiple antennas are used to sense the direction of incoming signals to detect inconsistencies in signal directions, which are key indicators of spoofing attempts. The algorithms used can analyze large data sets to distinguish between genuine and counterfeit signals, enabling real-time detection and response. However, it should be noted that the mentioned technological advances require rigorous testing and verification to ensure their effectiveness in different operational environments, and in our case, maritime environments.

5.2.2 Economic Viability

Reffering to the economic viability of implementing GPS spoofing countermeasures, this involves a cost-benefit analysis that takes into account both the financial costs of developing these technologies, as well as the potential losses associated with spoofing incidents. Initial costs include research and development, the procurement of advanced GPS receivers, and the integration of multi-system and signal authentication techniques on board ships. Ongoing

operational costs such as maintenance, updates and staff training must also be taken into account. However, these investments, made by ship owners and/or managers, are justified by the significant financial and operational risks posed by GPS spoofing. This justification is strengthened by the fact that in the shipping industry, spoofing can lead to navigational errors, collisions and course deviations, resulting in significant economic losses and environmental damage. Additionally, the tarnished reputation of shipping companies and the potential increase in insurance premiums add to the economic rationale for investing in countermeasures. Thus, economic viability is further enhanced by the scalability of these technologies, as with increased production and application, costs are likely to decrease due to economies of scale. Also, the international regulations and standards, such as those of the International Maritime Organization (IMO), can encourage widespread adoption, further reducing costs and enhancing the economic rationale of these investments. Therefore, while the initial financial investment may be significant, the long-term benefits and potential risk reduction make GPS spoofing countermeasures economically viable.

5.2.3 Real-World Implementation and Case Studies

Confirming the effectiveness of known GPS spoofing countermeasures and identifying best practices to adopt is directly linked to their application in the real world. This is the reason why several case studies can provide insight into the practical challenges, such as the 2017 Black Sea incident where several ships experienced GPS spoofing. Some of these ships, equipped with multi-system GNSS receivers and advanced signal processing capabilities, have been able to effectively detect and mitigate spoofing attacks. This incident highlighted the importance of robust detection systems and the need for continuous monitoring and real-time response capabilities. Another notable case is the implementation of GPS spoofing countermeasures by the US military, which uses advanced cryptographic techniques and signal integrity checks to protect against spoofing in critical operations. The shipping industry has also seen pilot projects where shipping companies have integrated advanced GPS receivers with anti-spoofing technologies that have demonstrated significant improvements in navigational accuracy and operational security, enhancing the value of investing in these countermeasures. Real-world implementation also involves overcoming accounting and regulatory challenges, such as ensuring compliance with international standards and coordinating with multiple stakeholders. These case studies highlight the feasibility and effectiveness of GPS spoofing countermeasures in real-world settings, offering valuable lessons for wider adoption and continued improvement of these technologies.

6. Differences and Common Ground between GPS Spoofing on Vessels and Generic GPS Spoofing Attacks

After this study it is clear that GPS spoofing attacks carry significant risks in a variety of contexts, but there are distinct differences between attacks targeting commercial marine vessels and those targeting other applications. These differences arise from the unique operational environments, consequences and technological requirements associated specifically with maritime navigation. The broad and open operating environment, critical security and economic impacts, as well as the need for sophisticated detection and mitigation technologies establish GPS spoofing as a particularly serious threat to maritime navigation. Understanding that these differences are essential to developing targeted countermeasures that address the unique vulnerabilities and requirements of commercial marine vessels compared to other applications of GPS technology is of high importance while aiming for better results and counter reactions

6.1 Unique Challenges in the Maritime Environment

GPS spoofing on ships presents unique challenges that differ significantly from general GPS spoofing attacks encountered in other sectors. These challenges arise from the distinct operational and environmental conditions inherent in the shipping sector.

6.1.1 Harsh and Variable Environmental Conditions

The marine environment is characterised by adverse and often unpredictable weather conditions. Ships operate in open seas where factors such as heavy storms, large waves and heavy fog can significantly affect the reception and reliability of GPS signals. These environmental variables add an additional layer of complexity to the detection and mitigation of GPS spoofing attacks, as the system must differentiate signal anomalies caused by natural conditions from those caused by malicious actions.

6.1.2 Limited Infrastructure

Unlike urban or land-based settings, maritime operations lack extensive land-based infrastructure. In many cases, ships are located far from land-based reference stations or alternative navigational aids. This isolation means that ships rely almost exclusively on satellite navigation systems, making them more vulnerable to spoofing attacks. The absence of complementary systems to cross-verify GPS data complicates the detection of spoofing.

6.1.3 Dynamic and Large Operational Area

Ships operate in extensive and dynamic areas, often crossing international waters and different sea zones. This wide operational scope makes maintaining consistent and reliable GPS signals difficult. Spoofing attacks can exploit these extended areas, as monitoring and securing such large areas is inherently difficult. The dynamic movement of ships also requires GPS systems to be highly adaptive, which can be an exploit for sophisticated spoofing techniques.

6.1.4 Navigation and Safety Systems Interdependency

Marine navigation relies on an integrated set of systems, including radar, Automatic Identification Systems (AIS), Electronic Charting and Information System (ECDIS) and GPS. Spoofing attacks that compromise GPS signals can lead to failures or errors in these interconnected systems. This interdependence means that a successful spoofing attack can have far-reaching effects on the overall navigation and safety of the ship, potentially leading to serious incidents such as collisions or grounding.

6.1.5 Regulatory and Compliance Pressures

The shipping industry operates under strict international regulations and compliance standards, mainly set by organizations such as the International Maritime Organization (IMO). These regulations mandate the use of reliable navigation systems to ensure safety at sea. GPS spoofing poses a direct threat to regulatory compliance, as altered navigation data can lead to violations of these standards. Non-compliance not only jeopardizes the operation of the ship but also exposes managers & shipowners to legal and financial implications.

6.1.6 Human Factors and Training

The effectiveness of GPS spoofing detection and mitigation also depends on the human factor. Seafarers must be trained to recognize the signs of spoofing and respond accordingly. The unique maritime context requires specialized training programs focused on spoofing detection and navigation resilience. However, varying levels of expertise and awareness among crew members can prevent early recognition and response to spoofing incidents.

Overall, GPS spoofing on ships presents unique challenges, compared to more common spoofing attacks on cars or fixed antennas, due to the adverse and changing conditions of the marine environment, limited infrastructure, dynamic operational areas, interconnected navigation systems, regulatory pressures and human factors. Addressing these challenges requires a comprehensive approach that incorporates advanced technological solutions, rigorous training and robust regulatory frameworks to ensure the integrity and safety of maritime operations.

6.1.7 Specific Operational Considerations

Commercial marine vessels operate in a vast, open ocean environment where GPS is critical for navigation due to the lack of physical reference points. The marine environment is subject to adverse weather conditions and requires constant, accurate positioning. Therefore, operational complexity is greater as marine vessels must navigate through busy shipping lanes, avoid hazards such as reefs and shoals, and comply with international shipping regulations. On the high seas, GPS signals are less likely to be jammed by physical obstacles, making them more vulnerable to direct spoofing attacks. In contrast, general GPS applications take place in a variety of environments, including urban, rural, and aviation environments. Each setting presents unique challenges, such as multipath effects in urban canyons or obstructions from buildings and natural features. The complexity of using GPS can vary widely. For example, car navigation systems are simpler compared to aviation or military applications that have more stringent requirements. In non-maritime environments, GPS signals can be blocked by buildings, terrain or other infrastructure, which can affect the success and detection of spoofing attempts.

6.1.8 Differences in Detection and Response

Ships need real-time detection and response capabilities because of the immediate dangers created by navigational errors at sea. This includes automated systems to alert the crew and initiate corrective actions. Detection and response systems must be integrated with other navigational aids and communication systems to provide a coordinated defence against spoofing. Another key fact is that in many GPS Spoofing attacks, the attacker is required to be very close to the ship that is the victim of the spoofing; in this regard, the difficulty of non-visual detection of the attacker is remarkable. In general applications, the required response time to spoofing attacks can vary. Personal navigation devices may tolerate small detection delays, while aviation or military applications require immediate responses. In many general applications, GPS spoofing detection may not be as deeply integrated with other systems, especially in consumer devices.

6.2. Common Ground between GPS Spoofing on Vessels and Generic GPS Spoofing Attacks

While GPS spoofing attacks on commercial marine vessels have unique characteristics due to the maritime environment, the underlying principles, detection techniques, mitigation strategies, and impacts have significant similarities to general GPS spoofing attacks. These commonalities underscore the importance of a coordinated approach to developing countermeasures and maintaining the integrity of GPS systems in all applications. Recognizing these similarities can help build strong, flexible defences against GPS spoofing that will benefit both maritime and wider applications.

6.2.1 Shared Techniques and Mitigation Strategies

Anomaly detection in signals is a critical method in both contexts. This includes detecting unusual patterns in signal strength, time deviation and frequency. Sudden changes in signal strength or the appearance of signals that do not match the expected parameters can indicate spoofing. Additionally, using receivers capable of processing multiple frequencies and signals from multiple satellite constellations helps cross-verify the authenticity of GPS data. Both marine and general applications benefit from the redundancy and cross-verification capabilities offered by such receivers. By comparing GPS data with independent data sources, inconsistencies can be identified that indicate a possible spoofing attack.

Also, cryptographic verification methods are critical in both contexts to ensure the authenticity of signals. Embedding cryptographic signatures in GPS signals allows receivers to verify the legitimacy of the data, thus rejecting spoofed signals. Real-time systems that continuously monitor GPS data for anomalies are essential for early detection and response. These systems use statistical models and machine learning algorithms to detect deviations from expected GPS behaviour and alert users to possible spoofing. Leveraging data from multiple receivers to validate GPS information is an effective mitigation strategy. Sharing and comparing GPS data across a network of users or devices helps detect spoofing by highlighting inconsistencies between received signals.

6.2.2 Technological Needs

Both require a combination of advanced hardware and sophisticated software to effectively counter spoofing attacks. This includes multi-frequency receivers, advanced antennas, signal processing algorithms and real-time tracking systems. Continuous development and implementation of updates and improvements are necessary to stay ahead of evolving spoofing techniques. Regular updates to firmware, algorithms and hardware ensure systems remain resilient against new spoofing methods.

6.2.3 Regulatory and Compliance Issues

Compliance with regulatory standards is critical in both marine and general applications. For merchant ships, this includes international shipping regulations, while for other applications it may include aviation standards, automotive regulations or telecommunications standards. Adherence to industry standards and guidelines helps maintain the integrity and security of GPS systems in various fields. Applying best practices and following guidelines from organisations such as the International Maritime Organization (IMO) or the Federal Aviation Administration (FAA) is essential.

6.2.4 Cross-Industry Lessons and Insights

In both marine and general applications, the basic principle of GPS spoofing involves transmitting false GPS signals to trick receivers into accepting incorrect position, speed, and time data. Attackers generate fake signals that mimic legitimate satellite signals, but with altered information to mislead the target receiver. The main goal is to cause the receiver to calculate an incorrect position or timing solution, leading to navigation errors, service disruption, and potential security risks. Whether targeting a ship, an aircraft, or a personal navigation device, the attacker seeks to manipulate the recipient's understanding of location and time.

7. Preventing GPS Spoofing with Neural Network Training

7.1 The Role of Machine Learning in Signal Analysis

While mentioning Cyber security and Spoofing attacks the goal while aiming for best practices is the need for fast action against the moves of each probable attacker.. At this point, Machine learning techniques come in the picture, so as to be explored and applied to address the various challenges posed by GPS spoofing; as GPS spoofing is a deliberate manipulation of GPS signals deceiving GPS receivers about their true location. This can have serious implications in various domains, including maritime navigation. With this initiative, Machine Learning and Neural networks come to create new paths in controlling the navigational environment of the vessel for GPS spoofing detection as well as mitigation representing a cutting-edge approach in cyber security aimed at safeguarding against the increasingly sophisticated threats posed by spoofing attacks. Some key aspects of neural networks applications for GPS spoofing could be the following:

- Detection of Spoofing Signals: Neural networks are employed to detect anomalous signals that indicate GPS spoofing. Traditional methods often struggle with the complexity and variability of spoofing signals, but neural networks excel in learning complex patterns and identifying deviations from legitimate GPS signals.

- Pattern Recognition: Neural networks can be trained using vast datasets of both legitimate and spoofed GPS signals. By learning the intricate patterns inherent in these signals, neural networks become proficient at distinguishing between genuine GPS signals and spoofed ones

- Adaptability and Learning: One of the key strengths of neural networks is their ability to adapt and learn from new data. As spoofing techniques evolve, neural networks can be continually trained with updated datasets to improve their accuracy in detecting new types of spoofing attacks.

- Real-time Detection: Depending on the architecture and implementation, neural networks can operate in real-time, providing immediate feedback on the authenticity of GPS signals. This capability is crucial for preventing spoofing attacks from impacting critical systems and operations.

- Challenges: Despite their effectiveness, neural networks for GPS spoofing detection also face challenges. These include the need for extensive and diverse training data to ensure robust performance across different environments and conditions. Moreover, there can be computational challenges in deploying neural networks in resource-constrained environments typical of many GPS-enabled devices.

- Research and Development: Research in this area is ongoing and aims to enhance the resilience of GPS systems against spoofing attacks. This includes advancements in neural network architectures, optimization techniques for real-time operation, and integration with existing GPS receivers and navigation systems.

7.2 Potential Benefits of Neural Network Training

On the topic of detection of spoofingattacks using machine learning based on multi-layer neural network in single-frequency GPS receivers it was noted that on one hand neural networks can be used in pattern recognition tasks, which is crucial for distinguishing between genuine GPS signals and spoofed signals as they can learn complex patterns associated with spoofing attacks, enabling more accurate detection. On the other hand, neural networks are also capable of learning and adapting to new types of spoofing attacks that may evolve over time. This adaptability can be proven essential as spoofing techniques become more sophisticated, thus allowing detection systems to stay effective against emerging threats. Moreover, compared to traditional rule-based or heuristic approaches; neural networks are able to achieve higher detection accuracy by leveraging the nonlinear relationships within GPS signal data. This leads to fewer false positives and false negatives and thereby improving the reliability of spoofing detection systems (Shafiee, 2018).

Furthermore, the real-time processing of GPS signals for spoofing detection is slowly becoming a true possibility as technology advances. This capability is of high importance especially for maritime navigation. Neural networks can also be used to identify which features are most relevant for detecting spoofing e.g., signal strength variations, timing discrepancies, thereby reducing the manual effort required for system tuning. Also, neural networks are able to be used as spoofing detection systems that can eventually be integrated with existing GPS receivers and navigation systems without significant hardware modifications. This would ensure adoption in various domains, including merchant shipping.

7.3 Challenges and Limitations of this Approach

Even though by employing neural network training for GPS spoofing detection actions can be completed faster and with high accuracy and automation; several challenges and limitation can also present themselves. While training neural networks for spoofing detection, large, diverse, and accurately labelled datasets of GPS signal data are required. Obtaining such datasets can be challenging due to privacy concerns within the industry, so the availability of data can become a challenge. Also, the variability in real-world spoofing scenarios, and the need for ground truth annotations can wither the quality of gathered datasets and thus the data quality becomes an issue.. Another challenge comes up from the computation resources demanded for real time calculations; as such couldpotentially limit the scalability and deployment of neural network-based solutions in resource-constrained environments.

Moreover, neural networks are often considered as "black box" models, making it difficult to interpret their decisions and understand the underlying features driving spoofing detection. This lack of interpretability may hinder trust and acceptance of neural network-based systems in safety-critical applications. Furthermore, neural networks trained on specific datasets may struggle to generalise to unseen spoofing techniques or environmental conditions not adequately represented in the obtained training data. Ensuring robustness and generalizability of neural network models remains a significant research challenge. It is also worth noting that neural networks are vulnerable to adversarial attacks, where malicious actors can manipulate GPS signals to evade detection by the trained model. Adversarial robustness techniques must be integrated into neural network architectures to mitigate such threats effectively. This means that the models would have to be trained after each new available spoofing attack case meaning which would as a result mean that implementation and maintenance costs associated with data collection, model training, hardware infrastructure, and ongoing updates would be sky high. This eventually would lead the Organisations and Shipping companies to assess the cost-effectiveness and long-term sustainability of adopting such technologies; as expensive systems would have to be installed on board and part of the vessel would be solemnly physically used for the new systems.

7.4 Enhanced Satellite Signal Reception and Terrestrial Interference Mitigation

This chapter will explore the integration of machine learning (ML) techniques into maritime antenna systems to enhance their capability to exclusively receive satellite signals while minimising interference from terrestrial sources. This topic evidently came up when our research was examining ways to minimise the possible Spoofing attacks by avoiding for the receivers to change over from receiving signals originated from the satellites available to receiving signals from the terrestrial antennas in closest proximity. Therefore for this chapter the aim is to improve the directional accuracy, positioning stability, frequency selection, and signal processing of maritime antennas. The integration of ML into these systems would return with significant advancements in maritime communication reliability and efficiency, essential for navigation, safety, and operational performance. Modern satellite communication systems are capable of being equipped with ML-powered interference detection capabilities as these systems can analyze signal patterns in real-time, detecting interference and automatically applying mitigation techniques such as frequency hopping or beam steering. Machine learning enhances these systems by continuously learning from interference patterns and improving their response strategies.

As proven, maritime vessels rely heavily on satellite communications for navigation, weather updates, safety communications, and operational coordination; the reception of terrestrial signals can interfere with the clarity and reliability of satellite communications. Based on the design of directional antennas, such as parabolic dishes and helical antennas, machine learning by analysing extensive performance data, ML algorithms can be used to optimise the antenna's directional accuracy, ensuring a narrow focus on satellite signals and reducing the likelihood of receiving off-axis terrestrial signals. .Identification and filtering out of terrestrial resources can also be done using ML Furthermore, ML models can analyze the characteristics of received signals, distinguishing between desired satellite signals and unwanted terrestrial noise and ensure the antenna remains accurately aligned with the satellite, despite the constant changes in the vessel's position due to waves and course adjustments. Since satellite communications typically operate within specific frequency bands to avoid congestion and interference, machine learning models can be used to analyze the frequency spectrum in real-time, identifying and selecting the optimal frequency bands with the least interference from terrestrial sources. This dynamic selection process would ensure the vessel's communication system operates within the most reliable and interference-free bands. Adaptive filtering using machine learning can dynamically adjust bandpass filter settings based on the analysis of incoming signal characteristics so ML algorithms can learn to distinguish between satellite signals and terrestrial interference, allowing only the desired frequencies to pass through. This capability enhances the clarity and reliability of satellite communications.Furthermore on the topic of "Geographic and Operational Awareness" the use of ML models could predict areas of high terrestrial interference based on geographic data and historical signal patterns. Conclusively, this newly found info would actively enable the vessel's operators to adjust system parameters proactively when approaching such areas thus minimising any possible interference and optimising vessel's effectiveness in satellite communication.

7.5 Neural Networks Application and GPS Spoofing prevention

7.5.1 Cases of Neural Networks Application on GPS Spoofing prevention

The open source nature of ML and unecrypted characteristics of GPS signals have drawn the attention of adversaries aiming to exploit UAV system vulnerabilities. These adversaries could make use of ML techniques to manipulate GPS signal information, presenting significant challenges for conventional detection systems in identifying and mitigating such deceptive activities. Despite is, the advent of Adversarial Machine Learning (AML) has recently emerged as a significant threat to the effectiveness of such systems. An adversary can exploit

vulnerabilities in the ML algorithm or the trained ML model to compromise network defence. The attacks on UAV and other means will be analysed and thus conclude on whether same applications are possible on marine vessels and whether the available methods to counteract on such attacks are truly applicable on the marine sector.

Firstly there is the case of DeepPOSE (Peng Jiang, 2022), which is a system designed to detect GPS spoofing attacks using deep learning techniques, specifically deep recurrent neural networks (RNNs). GPS spoofing is a type of cyber-attack where a malicious entity sends counterfeit GPS signals to deceive a GPS receiver, causing it to report incorrect location information. This can have severe implications for navigation systems, autonomous vehicles, and other GPS-dependent applications.

The key concepts and components related to DeepPOSE are as follows:

- GPS Spoofing Attack: This involves transmitting fake GPS signals to trick a GPS receiver into believing it is at a different location. Attackers can use this method to mislead navigation systems, hijack drones, or disrupt the operations of location-based services.

- Recurrent Neural Networks (RNNs): These are a class of neural networks particularly suited for sequence data. RNNs maintain a hidden state that can capture information about previous inputs, making them effective for time-series data analysis, such as GPS signal patterns.

- Deep Learning for Anomaly Detection: Deep learning models, including RNNs, can be trained to recognize patterns in normal GPS signals and identify anomalies that indicate spoofing attempts.

- Components of DeepPOSE

Collecting GPS signal data from various sources under normal and spoofed conditions, serving as the foundation for training and evaluating the model.
Identifying and extracting relevant features from raw GPS signals, including signal strength, time of arrival, and other temporal characteristics.
Training deep recurrent neural networks (RNNs) on a labeled dataset that includes both normal and spoofed GPS signals to learn the patterns of legitimate signals.
Analyzing incoming GPS signals in real-time to detect deviations from learned patterns, flagging potential spoofing attacks.

Secondly on 2022, there was an approach on ML Spoofing attack detection on UAVs using PerDet (Wei X W. Y., 2022). This system classified the available data as the normal and the attacked so as they can be used along with algorithms for the model to be trained accordingly This followed by the evaluation of the trained model and choose an appropriate classifier as a PerDet detector. PerDet reads the unknown flight data, and then determines whether the UAV has been attacked and produces a detection report to record the detection process and results.

In another case, adversarial Machine Learning Models have also been used as defence on Spoofing attacks. An examination to strengthen the robustness of IDS through integration with

the GAN model was completed during this scenario. The goal was aimed at three-phase process (Alhoraibi L, 2024). Firstly with signal acquisition and dataset loading, followed by feature extraction processing and then dataset into training, testing, and validation sets. Finally, in the third phase, evaluated the robustness of the IDS classifier. However, it was noted that even though the proposed model did show encouraging results, the scarcity of openly available datasets for GPS signal attacks and threats restricted the proposed model's ability to fully comprehend the complexity of GPS signal attack behaviour in authentic settings. This since the obtained datasets were impeded by various factors, including privacy concerns, proprietary data ownership, and logistical challenges associated with data collection.

Furthermore, on the "Machine Learning-based GPS Jamming and Spoofing Detection" (Squatrito, 2024) the existence of a crossed model that has a spoofing lower detection rate than the local model due to the increased number of combinations of uncorrelated features being compared to one another in the crossed model, was examined by Squatrito. When features between varying signals received are compared against one another, the feature space increases significantly, and thus the self regions become larger so as to cover the increased variation in suspected correlation. This results in a lower detection rate because a spoofed signal may fall in this expanded self region. As more features are added to the model, spoofing detection rates would increase. This thesis progressively proposed an architecture that uses an Artificial Immune System and Support Vector Machine algorithm to create a Health Management System for the detection of potential GPS jamming and spoofing attacks. This machine learning system was validated using simulated GPS signal data, simulated GPS receiver output, and simulated GPS jamming and spoofing signals. The results eventually proved that the model can successfully differentiate between nominal and failure data with high accuracy.

On the study of "Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs" (Talaei Khoei T, 2022), a given dataset, data pre-processing, feature selection, were used. The dataset was built using real-time experiments and simulations so as to collect authentic and spoofed signals at different dates in several locations. A universal software radio peripheral (USRP), a front-end active GPS antenna, and an I5-4300U laptop with 8 G RAM running with Ubuntu 16.04.7 LTS version was used for the hardware set up, as the GPS attacks were simulated using MATLAB by considering three types of spoofing attacks with different complexity levels: simplistic, intermediate, and sophisticated. Each attack was inflicted on specific features of the GPS signals, p.e on the Doppler Shift Measurement, Receiver Time, and Pseudo Range. This was fake GPS signals, unsynchronized with the authentic signals, were generated. On one of the cases observed, higher Doppler Shift measurements were out of the normal range of ±20 Hz, leading to a signal drift. In these attacks, GPS spoofing signals are also transmitted at a higher power level, compared to that of authentic GPS signals, resulting in a higher Signal-to-Noise Ratio value and thus recognised and categorised accordingly. In the examined cases the attacker has a knowledge of UAV position and the intermediate attacker is able to control the generated GPS signals. In sophisticated attacks, the spoofer gains control over several channels of multiple synchronized antennas. This type of attack is the most threatening spoofing attack, due to the effect of multipath signals and the motion of the satellites and receiver.

On the case of ConstDet (Wei X S. C., 2022) selected features were used with the goal of speeding up ML processing and improving its accuracy. These features were selected through an analysis of the control semantics. The control semantics are the mechanism and theory about how to control UAVs using flight data. As for the application, the JSA method was used and implemented using the available dataset so that it could get compared with the ConstDet method.

The implementation and comparison took place as per hereunder:

- To implement the JSA method, first, the original data obtained from the flight log were preprocessed. The angular velocity and acceleration were selected as the features.
- The GPS data, including latitude, longitude, and altitude, were utilised to compute the distance between two positions as a feature.
- The sampling time was 0.2 s, which was the same value as our ConstDet approach.
- The model using the same optimised parameters provided by the JSA method was trained on given optimised parameters and on a comparison with the ConstDet approach.

All in all, it was calculated that the ConstDet approach had better performance than the JSA method,, even though the JSA method used the optimized model parameters. Thus it was concluded that the proposed ConstDet approach is better than the JSA method. Concluding, It is not difficult to implement GPS spoofing devices and these attacks can lead to catastrophic consequences. The original data are distinctly important in the control process and can affect the control ability. Thus, data features are analyzed and selected based on the control semantics. Final work shows that the control semantics have a crucial relationship with the flight data, which is effective for the detection of GPS spoofing attacks. One of the reasons for the low detection rates of some existing works is that they only consider part of the flight data, which cannot comprehensively represent the relationship between the position-related flight data.

Moreover, Semanjski (Semanjski S, 2020) on the case of GNSS Spoofing Detection by Supervised Machine Learning with Validation on Real-World Meaconing and Spoofing Data inherited three separated datasets:

(a) The GNSS spoofing dataset synthetically generated and radiated Over the Air (OTA) in a laboratory by means of manipulating receiver clock drift, via Pulse Per Second (PPS) output through programmed clock divergence with an increase in the Carrier-to-Noise Density ratio (C/N0) of 2 dB or more for each tracked satellite (hereafter called the synthetic dataset, comprised of three subsets, each reflecting a different programmed clock divergence);

(b) The real-world GNSS meaconing dataset produced by un-intentional re-radiation (leaked signal from laboratory) of the authentic signal (called the meaconing dataset);

(c) The real-world spoofing dataset generated by using the Software Defined Radio (SDR) LimeSDR (a low cost, open source, app-enabled SDR platform that can be used to support just about any type of wireless communication standard) and HackRF (an open source hardware for SDR) configuration with gps-sdr-sim (a software-defined GPS Signal Simulator that generates GPS baseband signal data streams, that can be converted to Radio-Frequency using Software-Defined Radio platforms, such as ADALM-pluto, bladeRF, HackRF, and USRP), radiated OTA and recorded by the target GNSS receiver (hereafter called the spoofing dataset).

In the paper of (Wei X S. C., 2022), two experiments were presented to tackle the possibility of training the supervised machine learning-based approach on real-world GNSS signal manipulation data. Firstly, a supervised machine learning-based approach (in our case, C-SVM) has a high potential to be successfully implemented for GNSS signal manipulation attempt detection, as the designed model achieved high success rates over the presented experiments. Secondly, the inclusion of the real-world meaconing event increased the complexity of the model more than the inclusion of the real-world spoofing event did. This was evident in the number of supporting vectors that resulted from the model training step. However, although the increased complexity was not a desired scenario, it resulted in valuable results, as the trained model was able to detect all the real-world spoofing attempt data points in the validation step. This was not the case when the training was conducted on the simulated dataset only. Hence, enrichment of training datasets with real-world examples seems to be a valuable contribution for

model creation in Safety-of-Life applications, such as the detection of GNSS signal manipulation attempts. Furthermore, if four experiments and the achieved results are examined, the ability to implement the developed approach in combined learning scenarios.

7.5.2 Common Ground

The afore mentioned cases address the detection of GPS Spoofing and signal manipulation attacks with the use of various Machine Learning techniques. Par Example, DeepPOSE utilizes Recurrent Neural Networks (RNNs) in order to detect anomalies and distinguish same from the normal behavior. Similarly PerDet uses ML algorithms so as to classify the data received into normal and attacked state. These systems also empathize on data collection and feature extraction with characteristics like signal strength, time of arrival. DeepPOSE extracts temporal characteristics of the GPS signals, and ConstDET focuses on extracting features critical for grasping the concept of control semantics, like angular velocity and acceleration. Dynamic feature selection, as seen in the studies by Talaei Khoei, allows for the removal of less important data attributes, enhancing model efficiency and accuracy.

PerDet and DeepPOSE are systems that are designed to operate in real-time operations. Their ability to analyze data in real-time ensures immediate detection and mitigation of the Spoofing attacks and thus minimizing their implications. These systems are also designed to be able to be retrained based on new datasets so as to constantly evolve their effectiveness. For example, dynamic selection techniques used in MOD/WMOD models are capable of adapting to changing patterns, whilst systems such as CONSTDET improve accuracy by leveraging control semantics, making them resilient against various types of attacks.

Another similarity across the systems created and studied was that the efficiency and effectiveness of the systems heavily depends on the quality and quantity of the datasets used. Computational resources are a significant challenge, especially for systems such as DeepPOSE, where deep learning models require significant processing power for real-time data analysis. Ensuring that these systems operate effectively on typical UAV hardware remains a concern. Balancing sensitivity and model specificity is a global challenge. High sensitivity can lead to false positives, while high specificity can lead to missed detections. Each of these studies reports the need to calibrate their systems to minimize both false alarms and missed attempts at falsification.

7.5.3 Dissimilarities in approach

Even though the studied cases showed similarities, differences in approach were also evident. DeepPOSE utilizes RNNs for processing time-series data enabling the model to understand temporal dependencies and sequences in GPS signals. On the other hand, PerDet uses classification and evaluates and selects the most appropriate classifiers for spotting the signal anomalies. Squatrito's system combines Artificial Immune Systems (AIS) with Support Vector Machines (SVMs) to create a hybrid model that mimics the immune system's ability to recognize and respond to threats, offering a different perspective on pattern recognition and anomaly detection. Semanjski's study employs a C-SVM supervised machine learning technique, emphasizing the use of real-world datasets to train models. Unlike purely simulated datasets, real-world examples add complexity and depth, making the model more robust in practical applications.

ASPECT	DESCRIPTION

Variation in Machine Learning Techniques	DeepPOSE: Utilizes Recurrent Neural Networks (RNNs) to process time-series data, effectively capturing temporal dependencies and sequences in GPS signals, which aids in anomaly detection.
	PerDET: Involves classification of flight perception data, focusing on evaluating and selecting appropriate classifiers to differentiate between normal and spoofed data.
	Squatrito's System: Combines Artificial Immune Systems (AIS) with Support Vector Machines (SVMs) to create a hybrid model that detects jamming and spoofing, drawing parallels to the immune system's ability to recognize and respond to threats.
	Semanjski's Study: Employs a C-SVM supervised machine learning technique, emphasizing the use of real-world datasets, which adds complexity and depth, making the model more robust in practical scenarios.
Diverse Data Sources and Experimentation	DeepPOSE: Relies on synthetic data generated through controlled experiments
	Semanjski's System: Uses a mix of real-world meaconing and spoofing data, combined with synthetically generated signals, enhancing the model's performance in practical applications.
	CONSTDET: Data derived from UAV flight logs, focusing on control semantics (mechanisms of UAV flight navigation), offering a domain-specific approach that emphasizes flight behavior over raw signal characteristics.
	Talaei Khoei's Research: Analyzes varying levels of attack complexity (simplistic, intermediate, sophisticated), enabling differentiation between low-level and advanced attackers, with each type exhibiting unique features.
Differences in Handling Real-World vs. Simulated Data	Semanjski: Stresses the importance of incorporating real-world data, noting that training models solely on synthetic data may be insufficient. Integrating real-world data introduces complexity but enhances accuracy by accounting for real-world signal variations

	Squatrito's System: Primarily relies on simulated data for validation, offering controlled environments that allow precise testing of specific scenarios, though it may not capture all complexities of real-world conditions.
Specificity of Attacks and Defense Mechanisms	Semanjski's Method: Capable of distinguishing between meaconing (unintentional re-radiation of authentic signals) and deliberate spoofing, enhancing the model's effectiveness by addressing various forms of signal manipulation.
	CONSTDET: Utilizes control semantics based on UAV flight behavior, analyzing aspects such as velocity and acceleration to detect deviations from expected flight paths, providing robust defense against navigation interference.

Table 3: Dissimilarities in ML based approaches

7.5.4 Application into Commercial Shipping

The cases examined were focused on application on UAVs, however just like UAVs, merchant marine vessels also heavily rely on GPS Systems for their navigational and multiple other systems as already proven. Implementing on board, systems like DeepPOSE and Constdet that are using real time GPS Spoofing detection, would ensure vessels' smooth operation at all times and under adverse conditions. Moreover, in the line of PerDet methodology, ML technologies could potentially be used to ensure safe movements within a congested port or sea route. Eventhough, on the contrary to UAVs, marine vessels have multiple sensors for navigation, including AIS, radar, and sonar. Systems like PerDet that use perception data can be adapted to fuse information from these sensors, providing a holistic view of the vessel's environment. By integrating data from various sources, the system could more effectively detect when a spoofing attempt is being made, as manipulating multiple sensors at once would be more challenging for an attacker. This could be particularly useful for vessels traveling through regions known for piracy or where GPS jamming is a common issue.

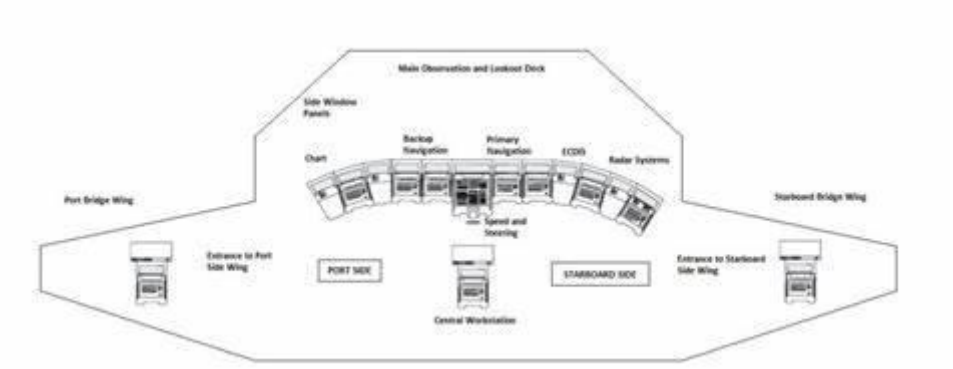

Figure SEQ Figure * ARABIC 11: Bridge Layout Example 1 CITATION Mar20 \l 1033
(Marine Insight, 2020)

Adopting a technique similar to Semanjski's, where real-world data is incorporated into the training process, could be deemed beneficial for marine systems, as vessels from all over the globe could possibly integrate data and thus enhance the system's capabilities on detecting and eventually preventing Spoofing attacks. Furthermore, techniques like those observed in Talaei Khoei's

dynamic feature selection could be particularly useful, as they allow the model to adjust which features are prioritized based on the operating environment. This is helpful taking into note the fact that merchant marine vessels operate on multiple conditions e.g. coastal areas, open seas, high piracy areas.

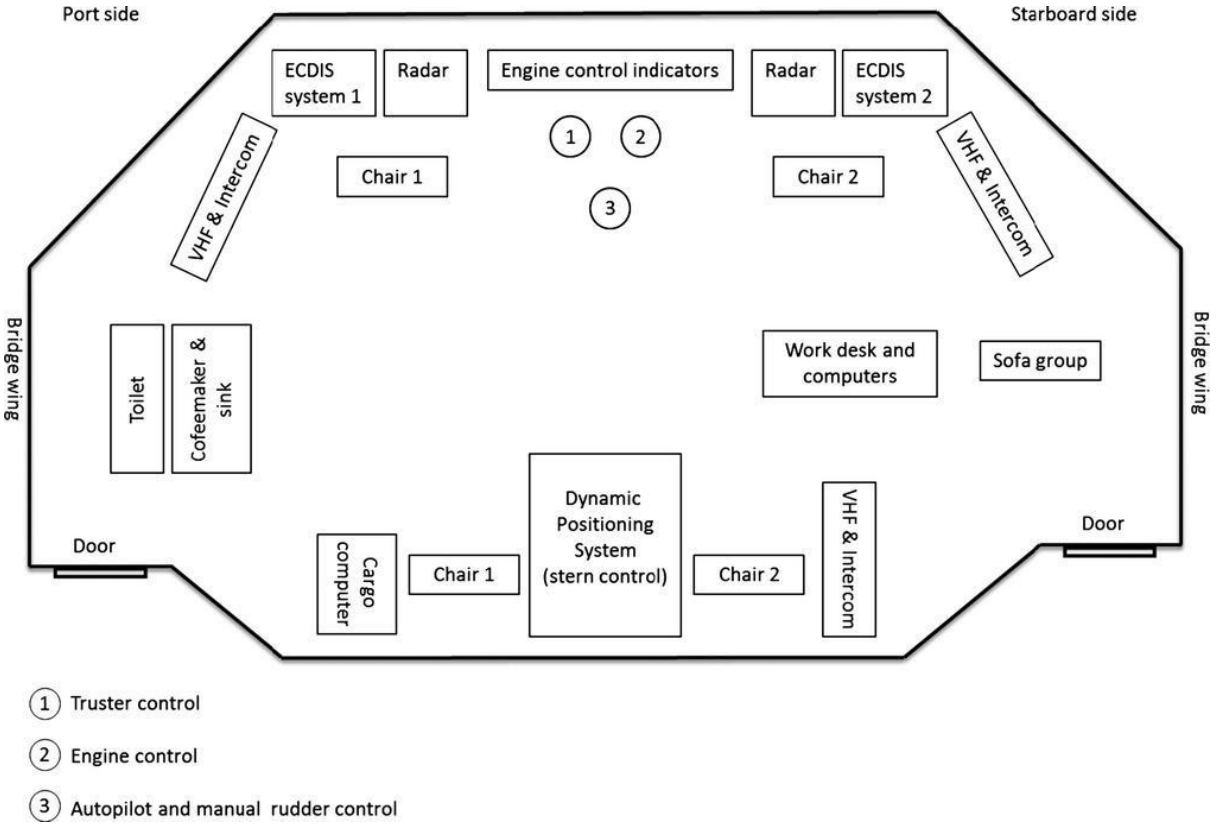

Figure SEQ Figure * ARABIC 12: Bridge Layout Example 2 CITATION htt \l 1033
(https://bpspsychub.onlinelibrary.wiley.com/doi/10.1111/joop.12111 , n.d.)

However, even though all of the above are indeed applicable, and as this thesis examines the shipping side of GPS Spoofing, it is important that the physical and practical application of the above mentioned systems is duly examined. To be more detailed, a vessel has a finite capacity available to be used by machinery. This means that practically the only available space for a new system to be installed, would be the vessel's bridge or the engine room. A machine that has the ability to operate real-time as DeepPOSE or PerDet would need to be supported by sufficient computer power, meaning a considerable part of the vessel would be used for this installation. Moreover, at this point it is worth mentioning the fact that vessels do not have access to the internet at all times. This due to the fact that they sail in open seas, and they usually sail under extreme weather and sea conditions. This fact would pause or interfere with data enquiry in most cases. Another issue is who would operate these new systems. On this topic a few questions arise. Should the company train the crew to be able to operate these Cyber Security assistive systems? Should the operators outsource the operation of these systems? Who would bear the cost of the installation of a system like this? Conclusively, the application of ML systems into the shipping industry is possible in theory, however solutions have to come up for a lot of practical problems in an industry that chronically refuses to change.

8. Conclusion

8.1 Summary of Key Findings

Navigating accurately and determining future routes is fundamental for maritime vessels, largely achieved through the use of GPS technology. However, GPS spoofing, a malicious activity where false GPS signals are broadcasted to deceive a receiver, has emerged the last few years as a significant threat. This results in GPS outages, potentially leading to major disruptions in the shipping industry by compromising safe navigation, paralyzing shipping lanes, collisions, and untraceable cargo. As noted, a GPS spoofing attack involves broadcasting fake GPS signals that mimic legitimate ones or using genuine signals recorded from other locations or times. This act tricks the GPS receiver into misinterpreting its actual location or the correct time, leading to severe navigational errors.

Eventually it comes down to the compromisation of three key components of the GPS System:

- Satellites: Functioning like constellations, satellites provide known positions at specific times.
- Ground Stations: These monitor and control the satellites, ensuring accurate positioning.
- Receivers: Devices that receive signals from satellites to determine precise locations.

In recent years, the maritime sector has faced a number of GPS spoofing incidents so to combat the dangers of GPS spoofing, it is crucial for maritime stakeholders to adopt several measures:

- Incident Reporting: Promptly report GPS disruptions with detailed information, including the vessel's location, date, time, and outage duration. Photographs or screenshots of equipment failures should be provided to aid analysis.
- Awareness and Training: Ensure navigators understand the differences between GPS jamming and spoofing and how these impact ship equipment. Navigators should be proficient in using alternative navigation methods and cross-checking the vessel's position.
- Use of Redundant Systems: Utilize a variety of position-fixing methods to verify the GPS location's accuracy.
- Caution in Sensitive Areas: Be informed of potential spoofing hotspots and exercise increased vigilance in these regions.

Highlighting the urgency of addressing GPS spoofing, global maritime organisations have urged the US Coast Guard to address deliberate GNSS signal interference at international forums, such as the IMO.

8.2 Future Directions for Research and Development

As GPS spoofing attacks continue to pose a significant threat to maritime navigation, it is imperative that future research and development focus on enhancing technologies for detecting and mitigating these attacks. The following initiatives represent key priorities for advancing the resilience and reliability of GPS systems in the maritime industry.

8.2.1 Advanced Signal Analysis

One of the foremost areas for future research is the development of advanced algorithms capable of distinguishing between genuine and spoofed GPS signals. By analysing signal characteristics, time discrepancies, and other anomalies, researchers can create more accurate and reliable detection systems. Innovative methods in signal processing and pattern recognition will be crucial to improving the effectiveness of these algorithms, ensuring that maritime vessels can identify and counteract spoofing attempts in real-time.

8.2.2 Multi-Source Verification

Integrating data from multiple GNSS constellations, such as GPS, GLONASS, Galileo, and BeiDou, offers a robust approach to cross-verifying positional information and detecting inconsistencies that may indicate spoofing. To this respect, future research should focus on refining this multi-constellation strategy to enhance its robustness and provide a comprehensive defence against increasingly sophisticated spoofing tactics.

8.2.3 Machine Learning

The application of machine learning (ML) detecting GPS spoofing is a promising area for future exploration. The development of systems that can learn from past spoofing incidents and adapt to new tactics will eventually enable real-time alerts and automatic adjustments to navigational systems. Thus research should prioritise leveraging advanced machine learning techniques, including deep learning and reinforcement learning, to improve the predictive accuracy and resilience of these systems.

8.2.4 Hybrid Navigation Solutions and Block chain Technology

To counteract the effects of GPS spoofing, research should also focus on developing more resilient navigation systems that integrate hybrid solutions. These could include combining traditional navigation methods with GPS and GNSS data to provide multiple layers of verification. Additionally, the implementation of block chain technology could ensure that any alteration or spoofing of navigational data is immediately detectable, providing a secure and trustworthy record of vessel movements.

8.2.5 International Policies and Regulatory Frameworks

Addressing the threat of GPS spoofing requires the development of international policies and regulatory frameworks. Future research could explore promoting global cooperation to establish standards for spoofing detection and response by sharing threat intelligence, best practices, and fostering collaborative efforts to combat GPS spoofing. This, including also the establishment of legal frameworks to penalise malicious GPS spoofing and protect maritime assets by evidently defining spoofing as a cybercrime and enforcing strict penalties will be crucial to deterring potential attackers.

Finally, by implementing mandatory compliance checks and regular audits of navigation systems on commercial vessels to ensure they meet anti-spoofing standards and establishing guidelines and protocols; these checks will manage to be essential for maintaining high levels of security.

8.2.6 Skill Enhancement and Awareness in the Maritime Sector

Improving the skills and awareness of maritime professionals is critical to mitigating GPS spoofing risks. By developing training modules focused on recognizing and responding to GPS spoofing incidents, including practical exercises and simulations the operators and managers would ensure that navigators, bridge crew and maritime IT professionals are well-prepared to handle spoofing scenarios is vital. Also, introducing certification programs that emphasise proficiency in handling GPS spoofing scenarios and arising awareness within the maritime industry about the dangers of GPS spoofing and the importance of robust navigational practices. Finally, informing all stakeholders about potential impacts and preventive measures can enhance overall industry resilience.

8.2.7 Real-Time Monitoring and Incident Reporting

Enhancing real-time monitoring and incident reporting capabilities can significantly reduce the impact of GPS spoofing. Future initiatives should prioritise establishing a network of monitoring stations equipped with advanced spoofing detection technologies to provide real-time data on spoofing activities worldwide. With the development of user-friendly platforms for the maritime community to report GPS spoofing incidents rapid reporting and dissemination of information to relevant authorities and stakeholders can be ensured. Also, by encouraging the sharing of spoofing incident data between maritime organisations and government agencies the ability build a comprehensive understanding of spoofing trends and tactics would constantly grow with all the collaborative efforts in data analysis and threat assessment; eventually reaching enhanced industry-wide preparedness.

8.2.8 Emerging Threats and New Spoofing Techniques

Ongoing research into emerging threats and new spoofing techniques is critical to staying ahead of potential risks. To this respect future research should focus on the continuous gathering and analysing data on new spoofing methods, tools, and attack vectors, the understanding evolving spoofing tactics and capabilities is essential for developing effective countermeasures. Focus should also be centered on conducting regular scenario planning exercises to evaluate the impact of different spoofing scenarios and develop robust countermeasures, as these exercises can help identify vulnerabilities and test the resilience of current systems. Since, partnering with universities and research institutions helps to explore innovative solutions and stay at the forefront of technological advancements in GPS spoofing detection and mitigation, academic research can then provide valuable insights and breakthroughs in this field.

8.2.9 Advancing Machine Learning for Maritime Antenna Systems

Future research should also prioritise the further development and refinement of machine learning models specifically for maritime antenna systems. Exploring advanced ML techniques, such as deep learning and reinforcement learning, will enhance signal processing and interference mitigation. Real-world testing and validation of these models on various types of vessels and in different maritime environments will be essential to fully realise the benefits of machine learning in this field. The continuous evolution of ML technologies promises to significantly improve maritime communication systems, ensuring reliable and efficient connectivity for the global maritime industry.

To conclude, by focusing on these future directions, the maritime industry can enhance its resilience against GPS spoofing, ensuring safe and secure navigation in increasingly complex and challenging environments. Continued investment in research, technology, policy

development, and education will be essential to protect maritime operations from the growing threat of GPS spoofing. Through collaborative efforts and innovative advancements, the industry can safeguard the integrity of its navigational systems, ensuring the continued safety and efficiency of global maritime trade.

8.2.10 Can merchant marine vessels by protected against GPS Spoofing attacks?

Eventually, one should seek an answer on the question on whether merchant marine vessels can be protected against GPS Spoofing attacks or not. The answer is yes. However, the reply is affirmative, providing that owners and operators, along with Marine Authorities, are willing to invest on the installation and implementation of systems on board that are able to counteract in the event of a GPS Spoofing attack. The commitment, of those involved, to invest in advanced systems capable of detecting and mitigating these threats, by employing a layered approach, can be truly fundamental in achieving a higher level of security against spoofing attempts on board. Even though current countermeasures manage to significantly reduce the risk of GPS spoofing, in reality a single solution cannot fully eliminate the threat of GPS Spoofing altogether. Each entity involved should evolve a multi-layered defense that integrates multiple strategies aiming to reach effectiveness and efficiency with minimal cost and consequences to the standard operations already enforced. Despite these high costs, the risks that materialize with Spoofing attacks — including collisions, misrouted or lost cargo and violations of regulatory compliance — make such investments indispensable. Thus, it all comes down to the fact that the decision to invest ultimately depends on a cost-benefit analysis by stakeholders within the maritime sector.

Βιβλιογραφία

Alhoraibi L, A. D. (2024). Detection of GPS Spoofing Attacks in UAVs Based on Adversarial Machine Learning Model. *Sensor Networks*. Ανάκτηση από https://www.mdpi.com/1424-8220/24/18/6156

ATSB - AUSTRALIAN TRANSPORT SAFETY BUREAU. (2022, MAY 04). Pilotage competency assurance safety recommendation after near grounding in Great Barrier Reef. Ανάκτηση από https://www.atsb.gov.au/media/news-items/2024/pilotage-competency-assurance-safety-recommendation-after-near-grounding-great-barrier-reef

Balanis, C. A. (2015). *Antenna Theory: Analysis and Design (4th ed.).* Wiley.

Bluegoatcyber. (χ.χ.). GPS System Vulnerabilities and Countermeasures. Ανάκτηση από https://bluegoatcyber.com/blog/gps-system-vulnerabilities-and-countermeasures/

CENTER FOR ADVANCED DEFENCE STUDIES. (χ.χ.). Ανάκτηση από https://c4ads.org/

Christopher, K. E. (2017). *Understanding GPS/GNSS: Principles and Applications.* Artech House.

CISA - CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. (χ.χ.). *Transportation - Maritime Modal Subsector Charter and Membership.* Ανάκτηση από https://www.cisa.gov/transportation-maritime-modal-subsector-charter-and-membership: https://www.cisa.gov/sites/default/files/2024-04/TSS-Maritime-SCC-Charter-2024-508.pdf

DNV. (2021). DNV ANNUAL REPORT. Ανάκτηση από https://www.dnv.com/publications/dnv-annual-report-2021-222310/

DNV. (2023, NOVEMBER 09). Cyber security enables safe digitalization for more efficient operations in container shipping. Ανάκτηση από https://www.dnv.com/expert-story/maritime-impact/cyber-security-enables-safe-digitalization-for-more-efficient-operations-in-container-shipping/

Do Alexis Sanou, R. J. (2013, MAY 22). Analysis of GNSS Interference Impact on Society and Evaluation of Spectrum Protection Strategies. *Positioning, Vol.4 No.2*. Ανάκτηση από https://www.scirp.org/journal/paperinformation?paperid=31514

E. Key. (χ.χ.). Techniques to Counter GPS Spoofing. Internal Memorandum. *MITRE Corporation*.

Elbert, B. R. (2008). *Introduction to Satellite Communication (3rd ed.).* Artech House.

El-Rabbany, A. (2002). *Introduction to GPS - The Global Positioning System.*

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. (2020, DECEMBER 17). Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk. Ανάκτηση από https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk

EUSPA - European Union Agency for Space Programme. (2024, July 03). What is GNSS. Ανάκτηση από https://www.euspa.europa.eu/eu-space-programme/galileo/what-gnss

FURUNO. (χ.χ.). Ανάκτηση από https://www.furuno.com/en/merchant/gnss/

FURUNO. (χ.χ.). Ανάκτηση από FURUNO FLEETBROADBAND: https://www.furuno.com/en/merchant/fleetbroadband/

FURUNO. (χ.χ.). *FURUNO FELCOM18* . Ανάκτηση από https://www.furuno.com/en/products/satellite_communications/FELCOM18#Options

Hengqing Wen, P. Y.-R. (2005). Countermeasures for GPS Signal Spoofing. *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, (σσ. 1285-1290). Ανάκτηση από https://www.ion.org/publications/abstract.cfm?articleID=6325

Hengqing Wen, P. Y.-R. (2005). Countermeasures for GPS Signal Spoofing. *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, (σσ. 1285-1290). Long Beach Convention Center .

IMO - SAFETY OF LIFE AT SEA. (2020). *SOLAS.* Ανάκτηση από https://www.samgongustofa.is/media/english/SOLAS-2020-Consolidated-Edition.pdf

IMSCO - INTERNATIONAL MARITIME CYBER SECURITY ORANISATION. (2024). IMSCO STANDARD. Ανάκτηση από https://imcso.org/Standard

Jon S. Warner, P. &. (2003). GPS Spoofing Countermeasures. Ανάκτηση από https://www.semanticscholar.org/paper/GPS-Spoofing-Countermeasures-Warner-Johnston/36e17f723bff8d429aca4714abe54500a9edaa49

Michael A. Lombardi, L. M. (2001). Time and Frequency Measurements Using the Global Positioning System (GPS). - *Proc. Measurement Science ConferenceMeasurement Science Conference.* Anaheim, CA. Ανάκτηση από https://tf.nist.gov/general/pdf/1417.pdf

MITRE. (2022, FEBRUARY 02). GPS spoofing detection techniques. Ανάκτηση από https://www.mitre.org/our-impact/intellectual-property/gps-spoofing-detection-techniques

Musumeci, L. &. (2014). Use of the Wavelet Transform for Interference Detection and Mitigation in Global Navigation Satellite Systems. *International Journal of Navigation and Observation*.

Musumeci, L. &.-1. (2014). Use of the Wavelet Transform for Interference Detection and Mitigation in Global Navigation Satellite Systems. *International Journal of Navigation and Observation*, σσ. 1-14.

Papadimitratos, P. &. (2008). Protection and Fundamental Vulnerability of GNSS. *Satellite and Space Communications, 2008. IWSSC 2008. IEEE International Workshop*, (σσ. 167-171). Ανάκτηση από https://www.researchgate.net/publication/224342594_Protection_and_Fundamental_Vulnerability_of_GNSS

Peng Jiang, H. W. (2022). DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network. *Digital Communications and Networks - Volume 8, Issue 5*, σσ. 791-803. Ανάκτηση από https://www.sciencedirect.com/science/article/pii/S2352864821000663

Pilatis, A., Pagonis, D.-N., Serris, M., Peppa, S., & Kaltsas, G. (2024). *Statistical Analysis of Ship Accidents (1990–2020) Focusing on Collision, Grounding, Hull Failure, and Resulting Hull Damage.* Ανάκτηση από https://doi.org/10.3390/jmse12010122

Roddy, D. (2006). *Satellite Communications.* McGraw-Hill Education.

Rosario La Pira. (2010). New role of GNSS in the Safety of maritime navigation. *Journal of the Spanish Institute of Navigation - Quarterly Technical Publication on Maritime, Air, Space and Land Navigation*, σσ. 17-25. Ανάκτηση από https://dialnet.unirioja.es/servlet/articulo?codigo=3313477

Safety4Sea. (2020, January 31). Understanding GPS spooding in shipping: How to stay protected. Ανάκτηση από https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/

SAFETY4SEA. (2020, JANUARY 02). Vessels navigating in China report GPS spoofing incidents. Ανάκτηση από https://safety4sea.com/vessels-navigating-in-china-report-gps-spoofing-incidents/

Schmidt, D. &. (2016, MAY). A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Computing Surveys*. Ανάκτηση από https://www.researchgate.net/publication/301798786_A_Survey_and_Analysis_of_the_GNSS_Spoofing_Threat_and_Countermeasures

Schmidt, D. &. (2016). *A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures.* ACM Computing Surveys. Ανάκτηση από https://www.researchgate.net/publication/301798786_A_Survey_and_Analysis_of_the_GNSS_Spoofing_Threat_and_Countermeasures

Semanjski S, S. I. (2020). GNSS Spoofing Detection by Supervised Machine Learning with Validation on Real-World Meaconing and Spoofing Data-Part II. *Sensors*. Ανάκτηση από https://www.researchgate.net/publication/340182303_GNSS_Spoofing_Detection_by_Supervised_Machine_Learning_with_Validation_on_Real-World_Meaconing_and_Spoofing_Data-Part_II

Shafiee, E. M. (2018). Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receiver. *Journal of Navigation*, σσ. 169-188. Ανάκτηση από https://www.cambridge.org/core/journals/journal-of-navigation/article/abs/detection-of-spoofing-attack-using-machine-learning-based-on-multilayer-neural-network-in-singlefrequency-gps-receivers/84BAC834ED5F8183497407A6FFF71A3D

Shinya Kowada. (2022). *High stability of 4.5ns (1sigma) using a single band GNSS timing receiver.* Furuno Electric Co., Ltd.). Ανάκτηση από https://www.furuno.com/en/products/gnss-module/GT-88

Squatrito, A. (2024). Machine Learning-based GPS Jamming and Spoofing Detection. *Doctoral Dissertations and Master's Theses*. Ανάκτηση από https://commons.erau.edu/edt/810/

Sunny Arora & Amit Tuteja - Guru Kashi University, Talwandi Sabo. (2021, MARCH). EXAMINING THE COUNTERMEASURES OF GPS SPOOFING ATTACKS. *Jurnal of Critical Review*. Ανάκτηση από https://www.jcreview.com/admin/Uploads/Files/6267eeb169fce0.35643295.pdf

Talaei Khoei T, I. S. (2022). Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs. *Sensors*(Special Issue Unmanned Aerial Vehicle (UAV)-Enabled Wireless Communications and Networking). Ανάκτηση από https://www.mdpi.com/1424-8220/22/2/662

U.S. Department of Homeland Security - Navigation Center. (χ.χ.). Global Positioning System (GPS) Overview. Ανάκτηση από https://www.navcen.uscg.gov/global-positioning-system-overview

Warner, J. J. (2012). A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. Ανάκτηση από https://www.semanticscholar.org/paper/A-Simple-Demonstration-that-the-Global-Positioning-Warner-Johnston/c49795beaec5dfea8b43d9b73a8573de2eb35f75

Wei X, S. C. (2022). CONSTDET: Control Semantics-Based Detection for GPS Spoofing Attacks on UAVs. *Remote Sensing*(Special Issue Satellite and UAV for Internet of Things (IoT)). Ανάκτηση από https://doi.org/10.3390/rs14215587

Wei X, W. Y. (2022). PERDET: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data. *Remote Sensing*. Ανάκτηση από https://www.mdpi.com/2072-4292/14/19/4925

Zahaby, M. &. (2009). Location tracking in GPS using Kalman Filter through SMS. *EURCON*, (σσ. 1707 - 1711). Ανάκτηση από https://www.researchgate.net/publication/224564437_Location_tracking_in_GPS_using_Kalman_Filter_through_SMS