mathematics

MDPI

Article

Detection and Mitigation of GNSS Spoofing Attacks in Maritime Environments Using a Genetic Algorithm

Saravjeet Singh [1], Jaiteg Singh [2,*], Sukhjit Singh [3], S. B. Goyal [4,*], Maria Simona Raboaca [5,*], Chaman Verma [6] and George Suciu [7,*]

1 Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Chandigarh 140401, Punjab, India
2 Department of Computer Applications, Chitkara University Institute of Engineering and Technology, Chitkara University, Chandigarh 140401, Punjab, India
3 Department of Data Science and Mathematics, Wilfrid Laurier University, Waterloo, ON N1048, Canada
4 Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia
5 ICSI Energy Department, National Research and Development Institute for Cryogenics and Isotopic Technologies, 240050 Ramnicu Valcea, Romania
6 Faculty of Informatics, University of Eötvös Loránd, 1053 Budapest, Hungary
7 R&D Department Beia Consult International Bucharest, 041386 Bucharest, Romania
* Correspondence: jaiteg.singh@chitkara.edu.in (J.S.); sb.goyal@city.edu.my (S.B.G.); simona.raboaca@icsi.ro (M.S.R.); george@beia.ro (G.S.)

Abstract: Due to the high reliance of daily activities on the Global Navigation Satellite System (GNSS), its security is one of the major concerns for research and industry. Most navigation and mobile-driven location-based services use GNSS to render services. Due to the low power and easy access of GNSS signals, these signals are vulnerable to spoofing and other types of attacks. Recently many GNSS spoofing attacks have been identified in road- and maritime-based environments. This study provides a technique to detect and counter the GNSS spoofing attack in the maritime environment. This technique uses the Receiver Autonomous Integrity Monitoring (RAIM) model with Least Square Estimation (LSE) and Proportional Integral Derivative (PID) Control to detect the spoofing attack. The proposed technique is based on the concept of a genetic algorithm and navigation devices, such as inertial sensors and pilot options for the ship. A case study using the AIS dataset and simulation using MATLAB and NS3 is provided to validate the performance of the proposed approach. Nine different voyages from the AIS dataset were considered to check the accuracy and performance of the proposed algorithm. The accuracy of the proposed technique was analyzed using the correctly identified attack. The result shows that the proposed technique identifies spoofing attacks with an average value of 90 percent. For result analysis the considered nine routes were traversed multiple times. Root mean square error is used to calculate the positional mismatch (error rate). Based on the combined results analysis, the average value of RMSE is 0.28. In a best-case scenario, the proposed approach provides an RMSE value of 0.009.

Keywords: inertial sensor; maritime vehicles; intelligent transportation; marine resources; rudder angle; fitness function

MSC: 68W50

check for updates

Citation: Singh, S.; Singh, J.; Singh, S.; Goyal, S.B.; Raboaca, M.S.; Verma, C.; Suciu, G. Detection and Mitigation of GNSS Spoofing Attacks in Maritime Environments Using a Genetic Algorithm. *Mathematics* **2022**, *10*, 4097. https://doi.org/10.3390/math10214097

Academic Editors: Ioannis G. Tsoulos and Ripon Kumar Chakrabortty

Received: 27 September 2022
Accepted: 25 October 2022
Published: 3 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Maritime transport (also termed a blue economy) has a huge impact on economic and social life [1]. Sea routes not only provide space for spices, but also create opportunities for tourism, transport, and sailing. Coastal regions have many benefits for economic development and Gross Domestic Product (GDP) growth due to the increasing use of maritime transport. The blue economy has recently emerged as the in-demand source of transport and economic development [1]. Maritime ships highly depend on digitization

and informational and operational technologies for navigation purposes. These supporting technologies are highly dependent on the internet, which makes them a potential target for cyber-attacks. According to the World Economic Forum's Global Risks Report 2020 and 2021, cyber risk is among the top ten risks. Security of ships and risks associated with ships was ranked fifth in the World Economic Forum's Global Risks Report 2020 [2,3]. According to a Maritime Insight report, cyber-attacks on ships increased by 900 times in the last three years. Denial of operational technology is the primary risk associated with any cyber-attack intended for maritime machinery [4].

Many cyber security attacks have occurred in maritime environments; their details and severity level are presented in Table 1. Due to weak GNSS signals, a small interference source can easily spoof GNSS signals with false data. Deliberate failure of GNSS signal by replacing it with a false signal is known as spoofing. GNSS spoofing and jamming are one of the operational technology attacks that have been faced by ships for years. Spoofed signals cause the wrong estimation of position and subsequently take the shipping vessel onto the wrong path [5]. GNSS spoofing can have severe consequences, and may even result in economic losses.

Table 1. Types of attack in maritime environment.

Sno	Risk Name	Information	Severity Level (Low:1, Medium:2, High:3)
1	Blind vision/Fake Vision	Blocks the camera of vehicles or provides misleading visual outputs	1/3
2	Jamming	Jams the signals of LiDAR or Radar and leads to poor performance.	1
3	Hidden/Fake objects	Attacker generates wrong signals to either hide objects or create fake objects.	3
4	Spoofing	Replaces GNSS signal with false signal	3
5	Jamming	Blocks the GNSS signal	1
6	Eavesdropping	Leaks the data of the system	2
7	Denial of Service	Blocks the services of the system	1

In the last few years, many GNSS spoofing and jamming attacks were faced by maritime transport. A GNSS spoofing attack on the Black Sea and Malacca Strait are an example of GNSS attacks on maritime transport [6,7]. Apart from the above-mentioned attack, many other attacks also happened on maritime transport due to spoofed GNSS signals [8]. Due to these GNSS-based attacks and the security of GNSS, many GNSS spoofing detection and mitigation techniques came into existence. Most of the spoofing detection and mitigation techniques are based on signal characteristics and cryptography, which are totally based on hardware devices. Thus, the performance of these techniques was directly dependent on the associated hardware and signal characteristics. Further, the hardware-based techniques for detecting spoofing may become obsolete with time and technological upgrades [9–12].

Due to the low power and easy access of GNSS signals, these signals are vulnerable to spoofing and other types of attacks. Recently, many GNSS spoofing attacks were identified in road- and maritime-based environments. According to the studied literature, most of the GNSS spoofing detection and mitigation algorithms in maritime environments use the concept of cryptography, signals interference, and hardware devices. Very few studies are based on the concept of software-based solutions. In this study, an attempt was made to detect and mitigate a GNSS spoofing attack using genetic algorithms. A software-based approach to detect and correct any spoofing attack could potentially help in the mitigation of spoofing attacks. Further, software-based solutions are much easier to upgrade, finetune, and customize in comparison to any hardwired system. These techniques and a study of the literature are presented in the next section. We propose an approach that uses an auxiliary navigation component with Receiver Autonomous Integrity Monitoring, and a genetic algorithm to detect and mitigate the GNSS spoofing attack. The genetic algorithm

was originally developed for optimality problems but we identified that this method can also provide the correct route after detecting the spoofing attack. This technique uses the Receiver Autonomous Integrity Monitoring (RAIM) model with Proportional Integral Derivative (PID) Control to detect the spoofing attack. Novel contributions of this study are presented as below:

- GNSS spoofing detection using RAIM and PID
- GNSS spoofing mitigation using a genetic algorithm
- Use of Dynamic Time Wrapping (DTW) Algorithm with sensor reading and rudder angle for fitness function

Firstly, GNSS signals with inertial sensors and pilot options are used to model the ship movement model. Based on the ship movement model, inertial sensors, and diversion threshold, true spoofing and false spoofing were identified. Ship trajectory, actual route, and intermediate waypoints with a dynamic time wrapping algorithm were used to calculate the fitness score. A case study using a simulation tool was also undertaken to check the performance and accuracy of the proposed method. After the simulation and result analysis, we present the conclusion and future scope.

2. Literature Survey

GNSS spoofing and security gained attention due to the increased dependence of human activities on GNSS. Low power, public accessibility/availability and easy usage of GNSS signals make it possible for low power interface devices to easily jam or spoof GNSS signals. Warner and Johnson undertook the first experiment to detect GNSS spoofing using the GS720 satellite on-road navigation [13]. Subsequently, many different techniques were designed to detect and counter spoofing attacks. Spoofing detection techniques are categorized into four parts, namely: cryptographic approaches, signal feature-based, auxiliary navigation based spatial, and geometrical based. Table 2 provides brief details about these techniques.

Table 2. Categories of GNSS Spoofing Techniques.

Category	Details	Ref.
Cryptographic based approaches	Effective way to identify the GNSS spoofing. Pseudo-Random Noise (PRN) code of signal was used to detect the spoofing. Secret key encryption is used. Sender and receiver have the information of a secret key.	[14–16]
Signal feature based	Signal features like signal strength, signal components, phase-aligned, Nulling etc., are used to detect the spoofing. Correlation function with help of clock rate/bias or Automatic Gain Control (AGC) value, is used to identify the distortion.	[17–19]
Auxiliary navigation based	Position, Velocity and Time (PVT) of GNSS with WiFi, Inertial Sensors, and cellular systems are used to identify the spoofing attack	[20–23]
Spatial and geometrical based	Signal spatial and geometrical properties like number of satellites, direction of signal, count of signal, or angle of arrival are used to identify the spoofing attack.	[24–26]

In the past few years, GNSS-based attacks have become quite popular. To counter any GNSS-based spoofing attack, numerous anti-spoofing techniques have been developed. A non-cryptographic method using two independent GNSS receiving antenna was proposed to detect the GNSS spoofing. Three-dimensional GNSS fixes on both antenna were synchronously monitored to identify the spoofing [27]. Apart from additional hardware, signal encryption, cryptographic methods for sender and receiver, spectrum security methods,

and signal authentication methods were used to detect the GNSS spoofing attacks. GNSS signal interference was also identified using signal strength, distance correlation matrix, and frequency modulation techniques. All of these techniques were based on hardware, GNSS signal frequency, and GNSS transition modes [15,16].

Anomalies in ship movement were identified using the trajectory data and patterns. Ship trajectories were considered a predictor for wrong vessel movement and recorded anomalies in routes selected by ships [24]. Ship type, number of stoppages, speed, and pattern of the movement were also used to identify the trajectory anomalies [28]. AIS is used by maritime authorities to manage the ships' movement to help identify the location based on the information (such as speed, type, number, etc.) transferred by AIS. Due to the open and self-reporting nature of AIS, many ships' spoofing activities were based on the AIS system. Many AIS-based spoofing detection techniques were developed by the research community, which are based on RADAR data, distance calculation methods, AIS position estimation, speed, and AIS data emission patterns, etc. [29–34].

According to studied literature following are the key challenges and research gaps for the identified research area:

- In order to detect GNSS spoofing, the primary challenge is to differentiate the true GNSS spoofing attack and diversion from the actual path due to errors in calculations.
- Most of the GNSS spoofing techniques are based on signal behaviors, signal geometrical/spatial features, and cryptography.
- One such approach is based on the auxiliary navigation component, which uses additional navigation devices like a cellular network, Wi-Fi, an inertial sensor, etc. to detect the spoofing attack.

In this experiment, the GNSS spoofing detection and mitigation have been done using two different procedures, GNSS spoofing is detected using RAIM and Inertial sensors whereas Spoofing mitigation has been done using the AIS data, current system state, and a genetic algorithm. A detailed description of the proposed approach and simulation is provided in the next sections.

3. Proposed Approach

The proposed approach uses an auxiliary navigation component with Receiver Autonomous Integrity Monitoring (RAIM) and a genetic algorithm to detect and mitigate the GNSS spoofing attack. Major steps involved in this approach are shown in Figure 1 and their description is provided as below:

Data Preparation:

For this study, Automatic Identification System (AIS) data, Sensor readings, ship data, source, and destination points are considered. AIS data provides the details of the available ship tracks in maritime environments. Ships have integrated bridge systems for navigation, routing, and surveillance at sea. This bridge system comprises of pilot options, data sources, sensors, and inertial data sources. Data sources comprise of spatial data elements like GPS, Automatic Radar Plotting Aid (ARPA), and Automatic Identification System (AIS). These data sources act as a base for navigation. GPS provides a real-time location of the ship. APRA processes the Radar data and uses it for avoiding collisions. AIS provides a map to the ship and allows the ship to adjust the speed, heading, and rudder angle. Sensor data includes compass, gyroscope, inertial sensor, and dead reckoning elements. Compass and gyroscope are used to identify the direction and position corresponding to obtained longitude and latitude information. Inertial Sensors and Dead Reckoning are used to identify the ship's relative position. These elements provide the position estimation in case of the absence of GPS. Climate sensors include different elements to provide weather and climate information.

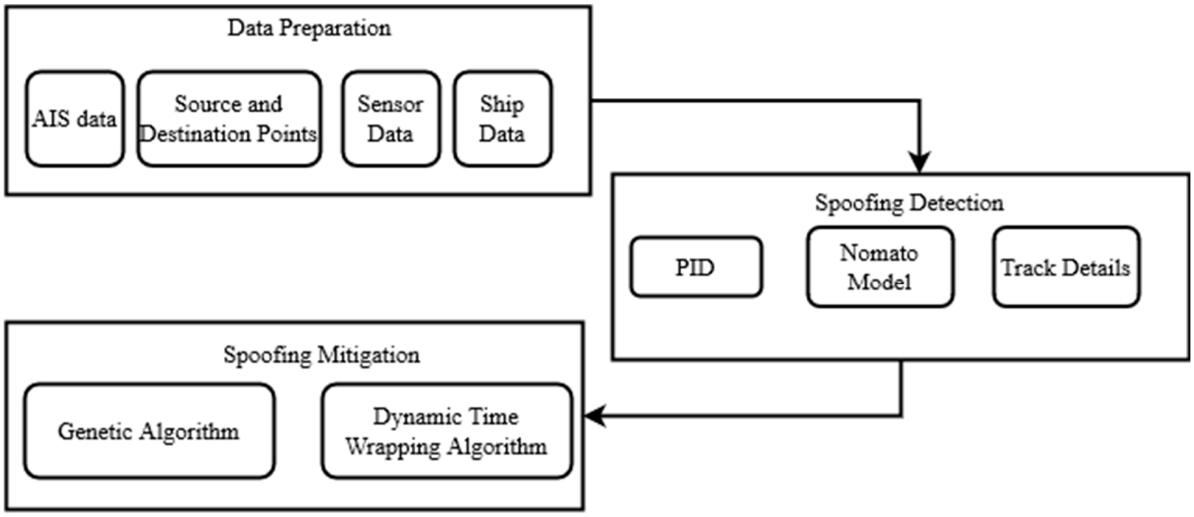


Figure 1. Steps involved in proposed approach.

Spoofing Detection:

RAIM model with PID Control to detect the spoofing attack. The RAIM model is used to assess the integrity of the GNSS signal in maritime and aviation environments. The RAIM model uses the pseudo-range measurement of GNSS signals received from different satellites to identify the faults in GNSS. The RAIM model computes various position fixes corresponding to available GNSS signals. Based on these position fixes and pseudo-range, the RAIM model identifies faulty GNSS signals. The RAIM model uses a minimum of five satellite signals to check the integrity of the GNSS signal [35]. PID is a control mechanism, which is based on the loop and feedback concept. It is used to identify the error rate by continuously monitoring the measured value and desired value of the parameters. Based on the identified error rate, PID controls the error rate and makes changes in the system by using proportional, derivative, and integral gain.

Spoofing Mitigation:

The proposed spoofing mitigation algorithm is based on the concept of genetic algorithms. For fitness function location information of spoofing detection point, the location of a recent GNSS receiver set point, route information, Dynamic Time Wrapping Algorithm (DTW), and Heading information are used. The genetic algorithm was initially developed for optimality problems, but we identified that this method could provide the correct route after detecting the spoofing attack. DTW is a technique to compare two time-variant data series. This technique finds the distance between all points of two series. A cost function is used to identify the similarity between two points. An accumulative matrix is used to calculate the global cost of two time series. A lower value of global cost signifies the more similarity between two series. For the considered spoofing scenario, ship trajectory and planned route act as data series. Each location in both series act as data points for the DTW.

4. System Description and Methodology

Ships have integrated bridge systems for navigation, routing, and surveillance in maritime environments. This bridge system comprises of pilot options, data sources (like GPS, Automatic Radar Plotting Aid (ARPA), and an Automatic Identification System (AIS)), sensors (compass, gyroscope, climate sensor, inertial sensor, and dead reckoning), and inertial data sources.

4.1. Spoofing Detection Model

Ship dynamic model and track information are very important for spoofing detection. In this study, the Nomato Model was considered to model the ship's dynamic for the position estimation and anomaly detection [14,36–38].

$$S_c \frac{dT_r}{dt} + T_r = R_g\theta + E_N \tag{1}$$

$$E_N = \frac{(\lambda T)^n}{n!} e^{-\lambda T} \tag{2}$$

According to the simple Nomato model, ship dynamics (as shown in Equation (1)) can be described using the different variables such as: time constant corresponding to the selected ship (S_c), turn rate of the ship in radian per second T_r, helm (rudder gain) (1/s) to rudder the ship R_g, rudder angle θ, and environmental disturbances E_N. Figure 2 shows the relationship between the helm and rudder angle. The helm provides information of turns taken by the ship to maintain the rudder angle. Similarly, Equation (2) describes the environmental disturbances in term of the Poisson process. According to Poisson distribution, n is a random variable for events in T interval time. Whereas λ is a rate parameter for the Poisson process and expresses the event per time in a given interval.

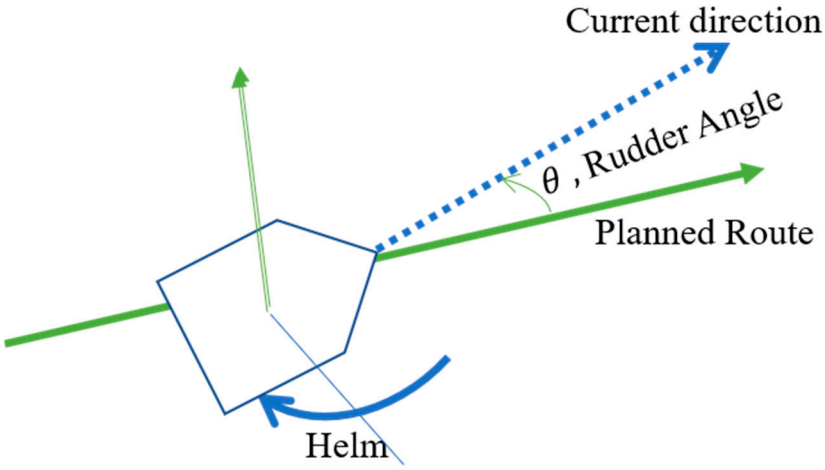


Figure 2. Relation between helm and rudder angle.

Ship headings can be defined using the kinematics of the ship as shown in Equations (3)–(5); where h is the heading of the ship (in radian), T_r is the turn rate of the ship in radian per second, N and M are the north and east positions of the ship, respectively.

$$\frac{dh}{dt} = T_r \tag{3}$$

$$\frac{dN}{dt} = V \cos h + E_N \tag{4}$$

$$\frac{dM}{dt} = V \sin h + E_M \tag{5}$$

where V is the velocity (in meters per second) of the ship in the water, E_N, E_M (in meters per second) are the drift error due to environmental conditions, water flow, and other disturbances.

The ship is directed using the autopilot mode for controlling heading and course. To control the heading h of the ship, autopilot uses PID law and maintains the required heading angle (h_r). Equation (6) is used to suppress the effect of noise and to control the rudder angle θ_t at a time (t).

$$\theta_t = A_i \int_0^t [h_r - c_t]dt + [h_r - c_t]A_p - [A_d gr_t + A_d OS_t] \tag{6}$$

where A_i is integral gain, c_t is compass reading at time t, gr_t is gyroscope reading at time t, OS_t is the reading of other inertial sensors, and A_p *and* A_d are the proportional and derivative gain calculated using the auto pilot control system (considering PID). By

considering η_c as the Nomato constant, η as natural frequency, ξ as the relative damping ratio, and S_c as time constant corresponding to the selected ship, Equations (7)–(9) are used to calculate A_i, A_p *and* A_d for ship motion.

$$A_i = \frac{\eta^3 S_c}{10\eta_c} \tag{7}$$

$$A_p = \frac{\eta^2 S_c}{\eta_c} \tag{8}$$

$$A_d = \frac{2\xi\eta\ S_c - 1}{\eta_c} \tag{9}$$

$$ATP = (N - N_0)\cos\theta_0 + (M - M_0)\sin\theta_0 \tag{10}$$

$$CTP = (M - M_0)\cos\theta_0 - (N - N_0)\sin\theta_0 \tag{11}$$

Both direct human or mechanical methods can be used to manage course/track by using the course autopilot in the outer control loop. The position of the ship in the sea in reference to global position can be estimated using heading angle, start position, and distance covered. Equations (10) and (11) can be used to calculate the along (ATP) or cross the track position (CTP). Where N_0 *and* M_0 are the global start position, M and N being the ship's current position, and θ_0 is the rudder angle with respect to N_0 *and* M_0. CTP with GNSS readings are added to the feedback mechanism of PID to estimate the position. The relationship between cross/along track readings with turn angle and heading angle is shown in Figure 3.

$$h_r(t) = \theta_0 - A_i{}' \int_0^\tau e(\tau)d(\tau) - A\prime_p CTP(t) \tag{12}$$

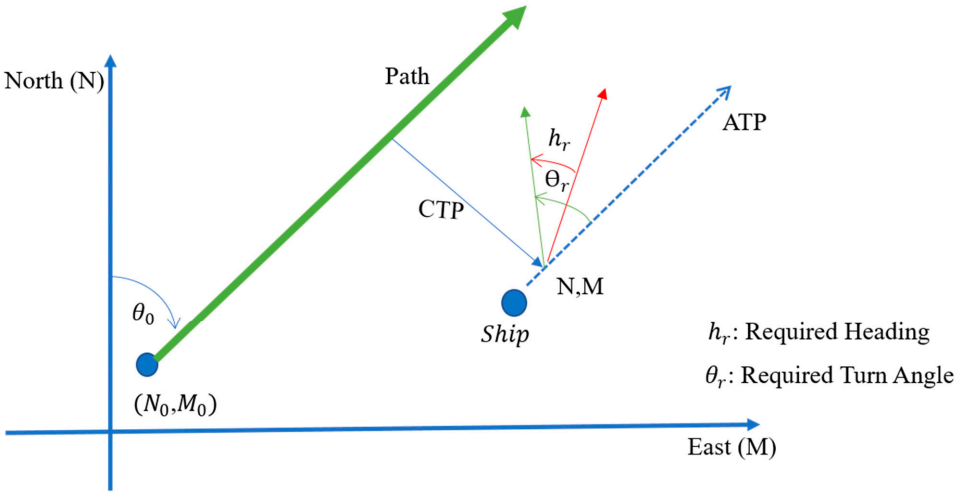


Figure 3. Along Track and Cross Track relationship in maritime navigation system.

Now using the Equation (12), the required heading angle (h_r) can be optimized with the help of PID, GNSS, and *CTP(t)* at time t using the equation, where $h_r(t)$ is optimized required heading angle at time t, $A_i{}'$ is integral gain, $e(\tau)$ is GNSS readings, $d(\tau)$ is the derivative variable, $A\prime_p$ is proportional gain of PID, and θ_0 is the rudder angle with respect to N_0 *and* M_0 (that is, with respect to the global start position). According to least square estimation algorithm, the state vector and mapped GNSS fix depend on *CTP(t)*. Thus, *CTP(t)* is further used to identify the spoofing detection.

4.2. GNSS Spoofing Detection Technique

The above stated terms and cumulative values of inertial sensors, pilot options, and GNSS receive output to identify the spoofing attack. Deviation from the actual route cannot

always be the spoofing attack, this deviation can be due to some error in the calculation and processing. The spoofing detection approach is based on two hypotheses that are given:

- H_0 = Null hypothesis means normal working of routing algorithms. Minor deviation in the path can be due to an error in the position estimation.
- H_1 = Alternate hypothesis means the working situation of routing is very different from the normal operating conditions. The deviation from the actual path is not due to an error in the position estimation, but it is due to some other reasons. This condition is also considered as a spoofing attack.

It is assumed that the attacker will divert the ship from the track with a minor CTP shift. The attacker will change the ship's path with limited speed and rudder angle and try to mislead the ship. After time t (0,1,2 . . .) a spoofing detection test is performed based on LSE RAIM model readings. At the beginning (time t = 0), the null hypothesis will be true, but with the passage of time an attacker can launch the attack so that situation can transition from the H_0 to the H_1 hypothesis. The sample situation is shown in Figure 4. According to LSE RAIM, the spoofing in GNSS signals can be identified using residual vector (RV) and attack statistics q that are shown in Equations (13) and (14). The RV depends on inertial sensor and GNSS readings. The weighted position estimation $S\hat{V}_b$ uses CTP reading for the position estimation. Similarly, the batch form of $e(\tau)$ uses CTP for the estimation.

$$\mathrm{RV} = e(\tau)_b - OM_b S\hat{V}_b \tag{13}$$

$$q = RV^T EE_b^{-1} RV \tag{14}$$

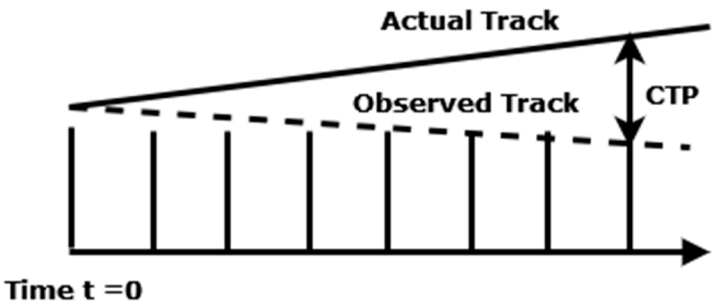


Figure 4. Sample situation of spoofing attack using cross-track positions. An attacker will make minor changes in the GNSS receiver reading so that it can be easily identified. However, the RAIM continuously analyzes the location deviation and error statistics in the GNSS and INS readings. The CTP over time interval t helps to identify the spoofing attack.

$e(\tau)_b$, OM_b, $S\hat{V}_b$, and EE_b^{-1} are batch measurement readings, batch observation readings, weighted position estimation, and inverse of the batch form of an error covariance matrix, respectively. $e(\tau)_b$, OM_b, $S\hat{V}_b$, and EE_b^{-1} can be calculated using GNSS and sensor readings.

If $T\delta$ is the threshold value to identify the spoofing attack with respect to error static q, then if $T\delta < q$ then H_0 will be true and if $T\delta \geq q$ then H_1 will be true. The GNSS receiver will continuously provide the location reading (gn) and state information over t time interval is sn. Then H_0 will be centrally chi-square distributed in non-spoofing conditions. Similarly, H_1 will be inverse non-centrally chi-square distributed under both spoofing and non-spoofing conditions.

4.3. Spoofing Mitigation Technique

Based on the q statistics of the RAIM algorithm, if a spoofing attack is detected then the system will generate the alarm and reset the GNSS receiver and other sensor readings. Considering Figure 2, N, M can be the position of the ship after detecting the spoofing attack. After spoofing detection, the new path needs to be planned to take the ship to the actual route. For the considered problem, before the spoofing detection point, it is assumed that ship is moving on the correct path. In this algorithm, it is assumed that the pilot option

reset the GNSS receiver after a certain time interval (that is reset time). When the GNSS receiver was reset to its original value the algorithm will store the position of the ship (RP_t).

The proposed spoofing mitigation algorithm (Algorithm 1) is based on the concept of a genetic algorithm and the core of the genetic algorithm is the fitness function. For Algorithm 1, the fitness function uses location information of spoofing detection point (SP), location of recent GNSS receiver set point (RP_t), route dataset (R), and after point RP_t, Dynamic Time Wrapping Algorithm (DTW), Rudder and Heading information, and GNSS receiver readings. A detailed description of the fitness function is shown in Algorithm 2. The main steps of the proposed technique are as below and shown in Figure 5.

Step 1. This approach resets the GNSS receiver after a certain interval and stores the location of the GNSS reset point ($RP = RP_1, RP_2, \ldots .. RP_t$) where RP_1 is the first GNSS resent point and RP_t is the recent resent point. Reset helps to reduce the route length. Ship trajectories and previous history are also recorded by the system.

Step 2. Fetch actual route (R) between recent GNSS resent point (RP_1) and destination. If the destination is far away then the algorithm can select the in-between waypoint to reduce the path length. Waypoints are the milestones between source and destination position. These waypoints also act as sub destinations for the complete route.

Step 3. Fetch part of the trajectory between RP_t, and spoofing detection point. This sub trajectory will act as the base of the fitness function and will be used to optimize the result using a genetic algorithm.

Step 4. R acts as an initial population for the genetic algorithm. A genetic algorithm extracts two chromosomes of the same size from the initial population.

Step 5. To find the best fit and for the evaluation of the genetic algorithm, perform ordered crossover and mutation on the chromosomes

Step 6. Identify fitness score using fitness function, based on the fitness function, the algorithm provides a route to the destination.

Algorithm 1 GNSS Spoofing Mitigation Algorithm

Input: AIS data *A*, Starting Point S, Ending Point *E*, inertial sensor readings, GNSS receiver output *F*, Ship trajectory information *T*, Spoofing detection point (*SP*), recent GNSS receiver set point (*RPt*)

Output: Optimal Route after detecting GNSS Spoofing

Start

1. Set t = 0;
2. Identify route dataset (*R*) between point *RPt* and *E*
3. Extract dataset T' from *T* between *RPt* and *Sp*
4. *TSize = Size of* T'
5. *RP*[1] . . . *RP[N]* are the nodes of *R*, where *N* is no of the nodes in *R*.
6. Select individual *I1* (of size *ISize*) from the initial population
7. Do
8. Select *I2* of *ISize* from the initial population
9. Crossover on *I1* and *I2* keeping same order
10. Perform Mutation and Replacement Retaining the data element order
11. Calculate matching score using fitness function between *I1* and *I2* using T'
12. *I1* = Best among *I1* and *I2* using fitness function (call Algorithm3 (*I1*,*I2*, T',*SP*))
13. While (fitness score optimized)

End

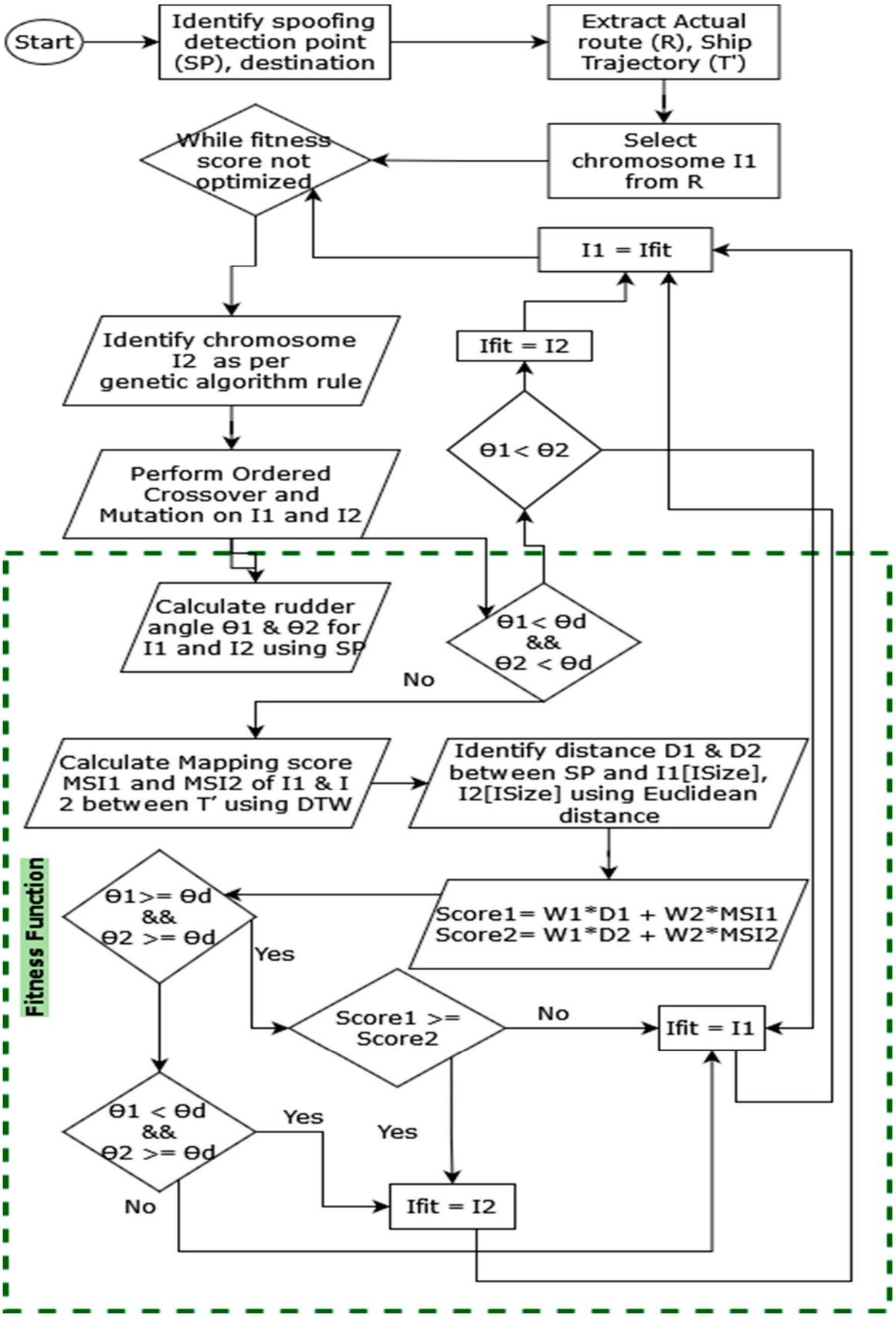


Figure 5. Flow chart of GNSS Spoofing detection technique using the genetic algorithm.

Algorithm 2 Fitness Function

Input: Ship trajectory information T, Spoofing detection point (SP), $I1$ and $I2$ chromosomes. $W1$ and $W2$ are weight factors.

Output: Best among $I1$ and $I2$

Calculate Mapping $MSI1$ score of $I1$ and T' using DTW
Calculate mapping $MSI2$ Score of $I2$ and T' using DTW
Identify distance $D1$ between SP and $I1[ISize]$ using Euclidean distance
Identify distance D2 between SP and $I2[ISize]$ using Euclidean distance
Calculate required rudder angle $\theta 1$ between SP and $I1[ISize]$
Calculate required rudder angle $\theta 2$ between SP and $I2[ISize]$
If ($\theta 1 < \theta d$ && $\theta 1 < \theta d$)
If ($\theta 1 > \theta 2$)
  $FitI = I1$
Else
  $FitI = I2$
Else
If ($\theta 1 >= \theta d$ && $\theta 2 < \theta d$)
Calculate decision score $Score1 = W1*D1 + W2*MSI1$;
  $FitI = I1$
If ($\theta 2 >= \theta d$ && $\theta 1 < \theta d$)
Calculate decision score $Score2 = W1*D2 + W2*MSI2$;
$FitI = I2$
If ($\theta 1 >= \theta d$ && $\theta 2 >= \theta d$)
Calculate decision score $Score1 = W1*D1 + W2*MSI1$;
Calculate decision score $Score2 = W1*D2 + W2*MSI2$;
If ($Score1 > Score2$)
$FitI = I1$
Else
$FitI = I1$
Return $FitI$

End

5. Simulation and Result Analysis

This section provides the experimental details of the proposed GNSS spoofing detection and mitigation algorithm. MATLAB and Network Simulator (NS-3) tools were used to simulate the GNSS spoofing, maritime traffic, and routing. Simulink tool was used with MATLAB to model the ship's environment. In addition to this, the "Sensor Fusion and Tracking Toolbox" of MATLAB was used to model the inertial sensors and GNSS. Sea Clutter Simulation was also added to set the physical environment variable of the sea. These environmental variables include wave speed, wave slope and height, wind speed, etc. The spoofing attack and spoofing detection calculations were simulated using Monte Carlo simulations. Signals carrier frequencies and baseband are considered to be 2.4 GHZ, with bias of 400 HZ and 1.5 KHZ, respectively. The speed of the ship was kept in the range of 1–15 knots. Sea disturbances were generated using the Monte Carlo simulation on Poisson Distribution in the range of 3 km/h to 100 km/h. Sensor readings and GNSS readings were considered to establish the Nomoto Ship movement model, RAIM environment, and Cross-track spoofing attack. A complete MATLAB simulated environment was integrated with NS-3 to establish the movement of ships. In this experiment, a ship course was created using the AIS dataset. Route nodes were based on the course data of the AIS [39].

Produced sea environment data in MATLAB were read as data files in NS-3 to represent the sea conditions and location information. Nine different voyages (details shown in Table 3) from the AIS dataset were considered to check the performance of the proposed algorithm. AIS details were processed using the JOSM tool to set the map-specific variables.

Table 3. Maritime Route Specification.

Route No	Latitude/Longitude: Start Port	Latitude/Longitude: Destination Port
1	21.6835°/72.49651°	15.81373°/52.21973°
2	2.02514°/45.33757°	21.6835°/72.49651°
3	2.02514°/45.33757°	−14.899°/50.28152°
4	17.69595°/83.2873°	12.641°/101.3025°
5	14.249°/80.13°	13.0587°/100.8948°
6	2.02514°/45.33757°	14.50437°/49.11537°
7	10.00767°/105.0788°	16.93134°/82.30579°
8	14.249°/80.13°	19.43268°/93.55493°
9	17.69595°/83.2873°	16.795°/96.17998°

The considered AIS data includes different fields like ship details, movement information, position information, dimension of the ship, data source type, and some other course-specific information.

5.1. Result Analysis Metrics

The accuracy of the proposed approach depends on different factors like positional accuracy to calculate the ship position, to identify the error due to normal condition or spoofed condition, diversion error from the predefined route, spoofing detection, spoofing mitigation, etc. To analyze the correctly identified GNSS spoofing attack and their mitigation. The following metrics were considered for the accuracy analysis:

- The ratio of Correct Detection (*RCD*): *RCD* is the ratio of the correctly identified GNSS spoofing attacks to the total launched GNSS spoofing attacks (the simplified formula is shown in Equation (15) below).

$$RCD = I/N \tag{15}$$

  where I is the number of correctly identified GNSS spoofing attacks and N denotes the total launched GNSS spoofing attacks.
- Average Positional Error (*APE*): *APE* identifies the average difference between the proposed route and actual obtained route after mitigating the spoofing attack. *APE* can be calculated by Equation (16):

$$APE = \sum_{i=1}^{n} SV_i - OP_i \tag{16}$$

  where SV are positional points on the proposed route, and OP are points on the obtained route, assuming that routes consist of n points.
- Positional Accuracy: The positional accuracy of the calculated position of the ship can be calculated using the Root Mean Square Error (*RMSE*) and Normalized Mean Square Error (*NMSE*), Mean Error (*ME*), and Per Point Positional Error (*PPPE*)
- Per Point Positional Error (*PPPE*): *PPPE* is the difference between the obtained position of the ship and the actual position of the ship with respect to the selected course as given in Equation (17).

$$PPPR = \sqrt{\left((ObtainX - ActualX)^2 + (ObtainY - ActualY)^2 \right)} \tag{17}$$

ObtainX and *ObtainY* are the obtained location of the ship. Similarly, *ActualX* and *ActualY* are the assumed actual positions of the ship with respect to the selected course.

For trajectory T, Root Mean Square Error ($RMSE$) and Normalized Mean Square Error ($NMSE$), Mean Error (ME) can be calculated using Equations (18)–(20).

$$ME = \frac{1}{T}\int_0^T PPPR(t)\cdot d(t) \tag{18}$$

$$RMSE = \sqrt{\frac{1}{T}\int_0^T PPPR^2(t)\cdot d(t)} \tag{19}$$

$$NMSE = \frac{T\cdot\sum_{t=i}^{T} PPPE(t)}{\sum_{t=i}^{T} Actual(t)\ \sum_{t=i}^{T} Obtain(t)} \tag{20}$$

- Covariance matrix: Covariance matrix provides the covariance between two random variables. Here, the covariance matrix is used to identify the true error and spoofed error. For two random vectors X and Y, the value at index [xy] gives the covariance between the x and y entry of vector X and Y respetivily.

5.2. Performance Analysis and Evaluation

Nine different routes based on the AIS data were considered to check the accuracy of the proposed approach. Spoofing attacks were launched using the Monte Carlo technique and the proposed approach was simulated using the NS-3 and MATLAB tools. RCD and APE scores for each route were calculated and are shown in Table 4. Accuracy analysis based on RCD and APE is shown in Figures 6 and 7, respectively.

The RCD score provides the efficiency of detecting true spoofing attacks. According to the RCD score, the maximum value of RCD is 1 which indicates 100 percent efficiency when detecting the spoofing attacks. On the selected nine routes, traversal was performed using the simulation and random attacks were also launched. Thus, based on the RCD score the minimum value of RCD is 0.75 and the average value is 0.90. Due to random attacks launched with the Monte Carlo random probability approach, the proposed approach was used to identify the rate of correct identifications of spoofing attacks for the maximum number of cases (that is, on average 90 percent of attacks were correctly identified by the proposed approach). The APE score identifies the difference between the actual route and the route obtained after mitigating the spoofing attack. The proposed approach uses the genetic algorithm-based approach to identify the correct route after detecting the spoofing attack. In the case of maritime navigation, ships cannot take sharp cuts, so to maintain the desired heading angle, an adequate rudder angle was selected. This genetic-based approach provides the best path with an average error of 1605.3 m considering current traffic and the sea environment. In the worst-case scenario, the deviation from the path was 3816 m. Overall, the mitigation approach provides good results.

Table 4. Accuracy analysis of proposed approach using RCD and APE metrics.

Route Number	Traversal Count	Number of Attacks Generated	Correctly Identified Attacked	RCD	APE in (Meters)
1	7	7	7	1	630
2	3	4	3	0.75	480
3	9	7	6	0.86	1470
4	11	10	9	0.9	3110
5	2	2	2	1	160
6	6	7	6	0.86	1778
7	8	4	4	1	1204
8	9	12	11	0.92	3816
9	12	15	12	0.8	1800
Average	67	68	60	0.90	1605.3

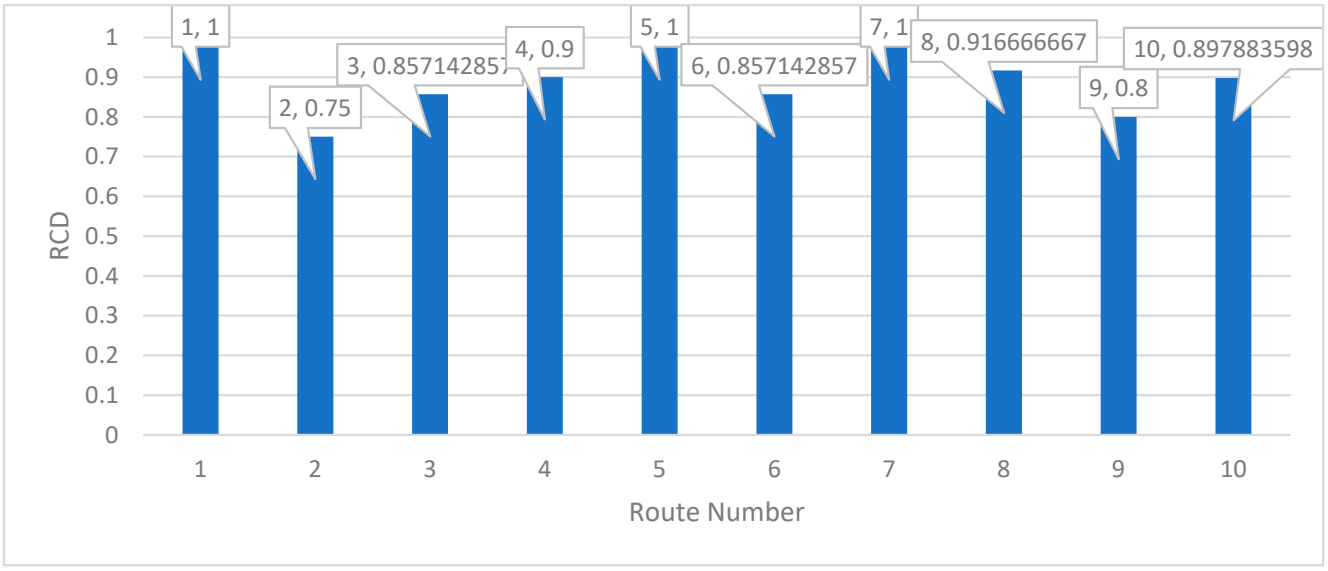


Figure 6. Performance comparison of proposed algorithm based on RCD values.

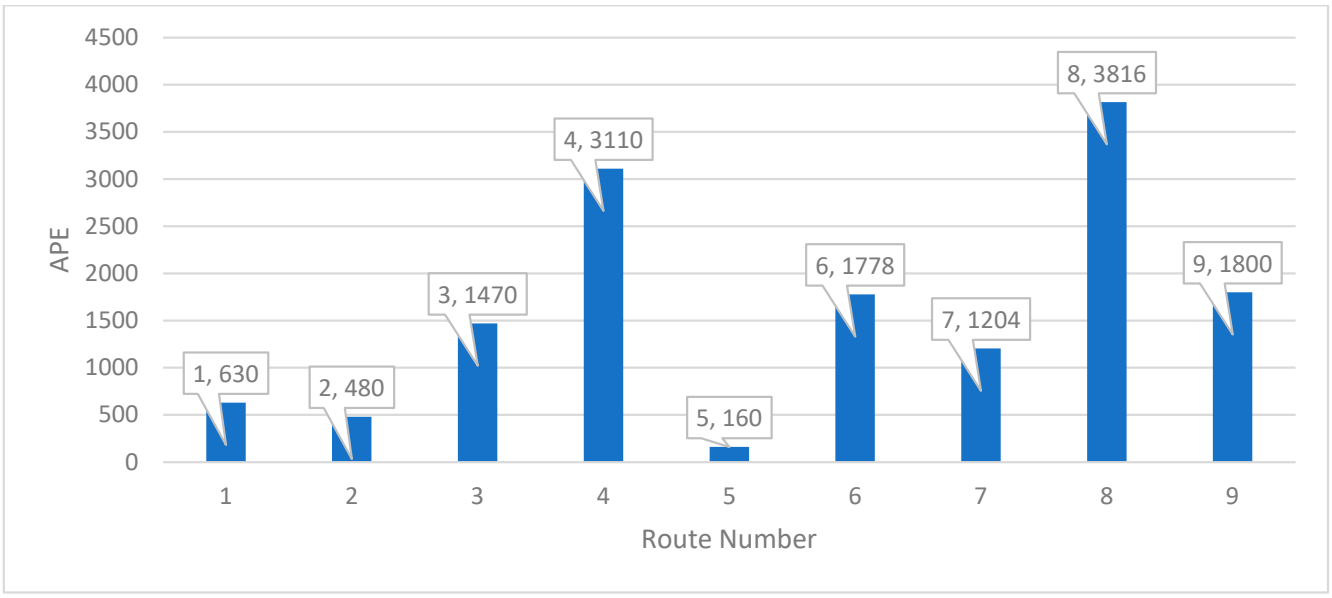


Figure 7. Performance comparison of proposed approach based on APE values.

Further, to check the positional accuracy, mapping the location of the ship on a digital map was analyzed using the mean error, RMSE, and NMSE. Figure 8 provides the RMSE per traversal per route. The same route was traversed more than once, so RMSE was calculated every time to check the accuracy of the location mapping procedure. The maximum RMSE was identified with a value of 0.7, and the minimum value of RMSE was 0.009. The average score of RMSE per route is shown in Figure 9. The peak value of positional error was identified during a high volume of environmental disturbances. During the simulation, environmental variables were controlled using the Markov process. The random value of the environmental variable highly affects the positional accuracy.

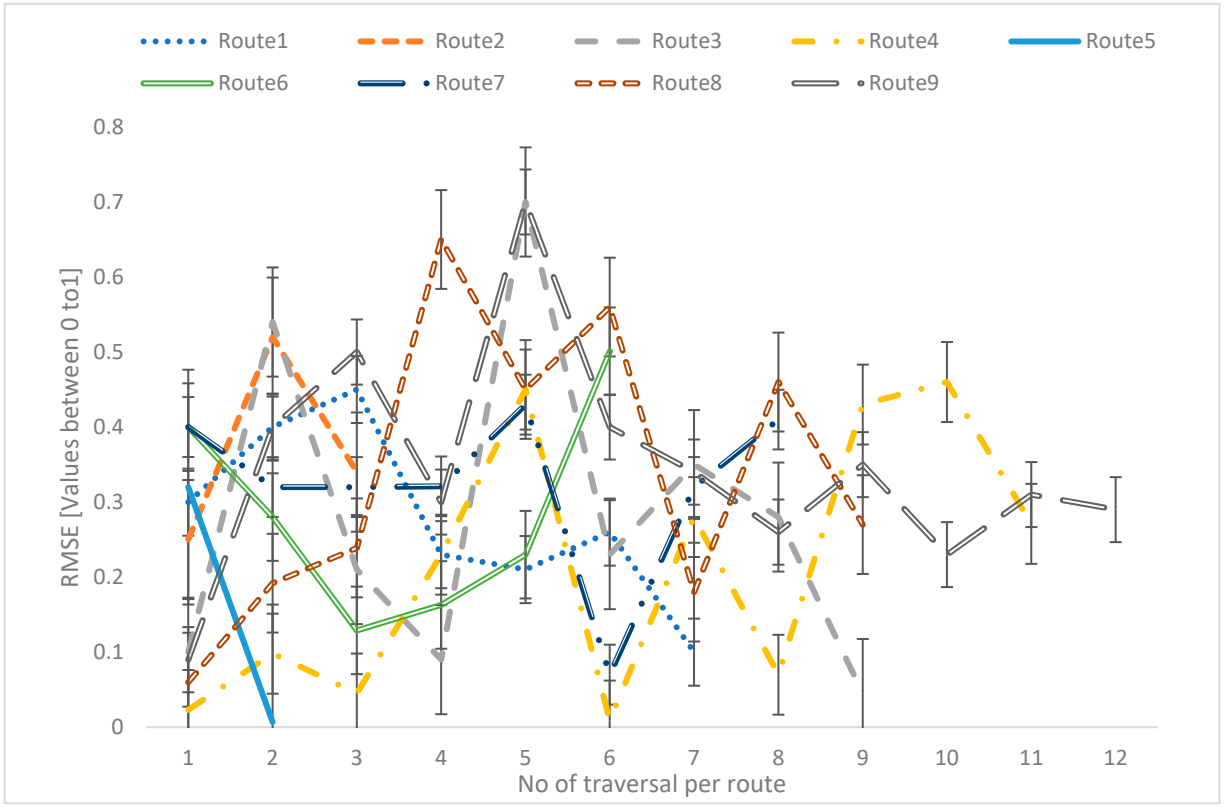


Figure 8. RMSE values corresponding to each traversal of the selected route.

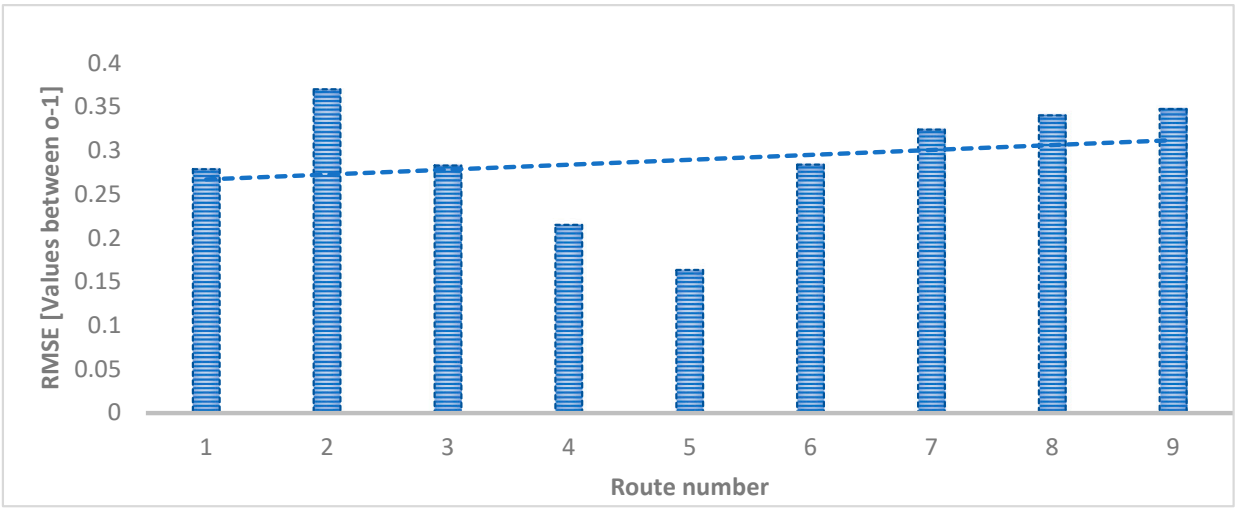


Figure 9. Average value of RMSE for each route.

NMSE was used to measure the accuracy and efficiency of mapping the positions onto the map. To evaluate the effectiveness of mapping, nine routes were traversed with different values. For each traversal, NMSE errors were calculated. From NMSE, it can be observed that reparative traversal does not provide a huge impact to improve the error rate (shown in Figure 10). Error rates are independent of traversal time and totally depend on the positional parameters. Figure 8 provides the detailed analysis of RMSE per route per traversal. Figure 8 provides visualization of the average value of RMSE obtained per route. Similarly, Figure 10 provides the comparison of error obtained using RMSE and NMSE per route.

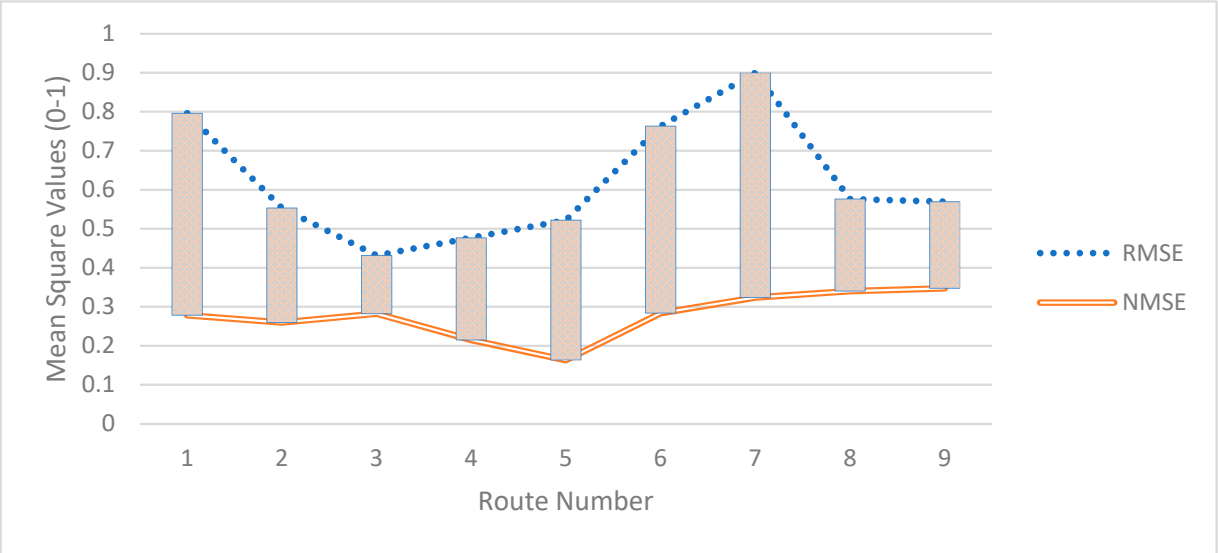


Figure 10. Accuracy comparison based on RMSE and NMSE.

Monte Carlo simulation in the probability model was used to launch the spoofing attack. During the navigation, deviation from the actual route can be either due to spoofing or environmental and device errors. The covariance matrix was used to identify deviation from the actual route due to the presence of a spoofing attack. Figures 11 and 12 show the use of the Error covariance matrix to identify the true positional errors under normal conditions, and errors in position due to spoofing attacks. Equation (21) provides the Error Bound of the covariance matrix (*CEB*).

$$CEB = \left| \sqrt{Reading\ at\ spoofed\ Condition} - \sqrt{Reading\ at\ spoofed\ Condition} \right| \quad (21)$$

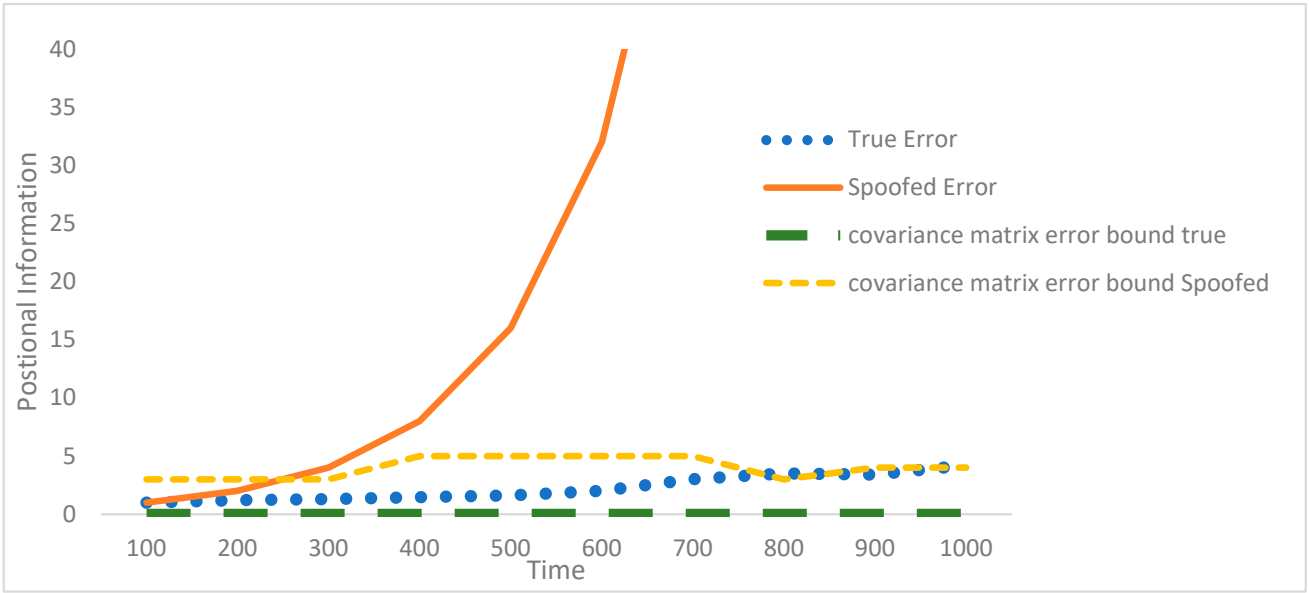


Figure 11. Error covariance matrix to check the effect of Monte Carlo simulation spoofing attack of different densities for high-intensity attack.

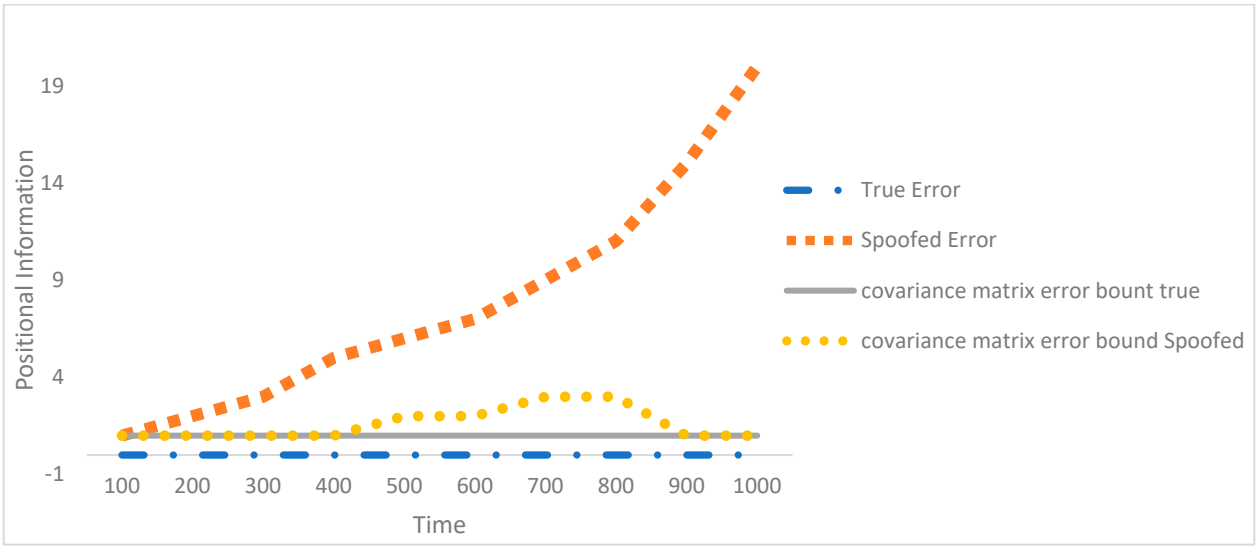


Figure 12. Error covariance matrix to check the effect of Monte Carlo simulation spoofing attack of different densities for low-intensity attack.

Figure 10 shows the high-intensity spoofing attack and Figure 11 shows the low-intensity spoofing attack. The covariance matrix can easily differentiate the spoofing error and true positional error using the error-bound parameter of the covariance matrix.

According to the performed experiment and analysis, the proposed approach identifies spoofing attacks with an average accuracy value of 90 percent. The positional mapping error is identified using the RMSE, and the cumulative value of RMSE is 0.28. In the best case, the proposed approach provides an RMSE of value 0.009 which is approximately equal to no error. The major limitation of this experiment is the lack of actual environmental variables and weather conditions. Though environmental variables are added using the Markov process it is still very different from the actual situation. Table 5 compares the proposed technique with state-of-the-art techniques.

Table 5. Comparison of proposed approach with state of art techniques.

Sno.	Technique	Description	Results and Findings
1	Resilient Multi-Frequency, Multi-Constellation (MFMC) receiver [11]	This approach identifies GNSS spoofing using the PVT calculations of the GNSS signal using MFMC receiver.	In best- and worst-case scenarios, recorded RMSE for positioning was 0.5 m and 13.27 m, respectively.
2	Orthogonal matching pursuit [40]	This approach uses array antenna-based direction of arrival (DoA), multiple pseudo-random number signals and orthogonal matching pursuit algorithm to detect the GNSS spoofing attack	The maximum value of RMSE for DoA estimation was 1 degree.
3	Modified MUltiple SIgnal Classification (MUSIC) [41]	Direction of Arrival with antenna patterns and phase difference of signals were used to identify the GNSS spoofing.	No qualitative matrices were provided for the spoofing detection accuracy.
4	Direction of arrival, elevation point and Azimuth angle based method [42]	A quality metric based on pitch, roll and yaw angle was designed to analyze the altitude. Altitude, DoA, elevation point, and azimuth angle were used to identify the spoofing.	Able to identify spoofing but detection time is high
5	Proposed technique based on genetic algorithm	Concept of a genetic algorithm and navigation devices like inertial sensors and pilot options for the ship. Simulation using MATLAB and NS3 tool is provided	The positional mapping error is identified using the RMSE, and the cumulative value of RMSE is 0.28. In the best-case scenario, the proposed approach provides an RMSE of value 0.009

6. Conclusions

We presented a GNSS spoofing detection and mitigation technique using the concept of genetic programming. The proposed technique uses an auxiliary navigation component with Receiver Autonomous Integrity Monitoring and a genetic algorithm to detect and mitigate the GNSS spoofing attack. GNSS spoofing is detected using RAIM and Inertial sensors. Along-track and out-of-track points were considered to check the diversion from the actual route. The proposed techniques also follow the PID concept to differentiate the spoofing situation and the normal diversion situation. This counter spoofing technique uses AIS data, current system state, and a genetic algorithm to provide the correct route. Genetic algorithms were used to solve the optimality problem and, in this technique, we used a genetic algorithm to optimally select the complete optimal path. To validate the proposed technique, MATLAB and Network Simulator (NS-3) tools were used to simulate the situation of GNSS spoofing. Sea Clutter and Simulink tools were used with MATLAB to model the ship's environment. For the experiment, a ship course was created using the AIS dataset. Nine different routes were considered to check the performance of the proposed algorithm. According to the performed experiment and result analysis, the proposed technique, in the average case, provides 90 percent accuracy to detect spoofing attacks. The error in route mapping was calculated using the RMSE and the average value of RMSE is 0.28. In the best-case scenario, the proposed approach provides an RMSE of value 0.009. The identified average value of positional error was 1605.3 m. The effect of intensity of spoofing attack was also analyzed using the covariance matrix and it has been observed that the proposed approach is capable to handle low- and high-intensity attacks. According to the performed experiment, it has been observed that a genetic algorithm with sensor data can be used to mitigate the GNSS spoofing attacks in the maritime environment. In the future, this technique can be implemented in real-time situations. Additionally, the detection technique can be improved by using only along with track points.

Author Contributions: S.S. (Saravjeet Singh) and J.S. were involved in conceptualization, data curation, formal analysis, project administration and preparing manuscript draft. S.S. (Sukhjit Singh) Sehra and S.B.G. helped in investigation and finalization of experiment methodology. M.S.R. and G.S. arranged resources and acquired funding. C.V. helped in reviewing and editing the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by Ministry of Research, Innovation, Digitization from Romania by the National Plan of R & D, Project PN 19 11, Subprogram 1.1. Institutional performance-Projects to finance excellence in RDI, Contract No. 19PFE/30.12.2021 and a grant of the National Center for Hydrogen and Fuel Cells (CNHPC)—Installations and Special Objectives of National Interest (IOSIN). Additionally, this research work has supported by UEFISCDI Romania and MCI through BEIA projects ADRIATIC, iPREMAS, PIMEO-AI, SOLID-B5G and by European Union's Horizon 2020 research and innovation program under grant agreement No. 101016567 (VITAL-5G). The work of Chaman Verma is supported under ÚNKP, MIT (Ministry of Innovation and Technology), and the National Research, Development, and Innovation (NRDI) Fund, Hungarian Government. Also, his work was supported by the Faculty of informatics, Eötvös Loránd University, Budapest, Hungary.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Voyer, M.; Schofield, C.; Azmi, K.; Warner, R.; McIlgorm, A.; Quirk, G. Maritime security and the Blue Economy: Intersections and interdependencies in the Indian Ocean. *J. Indian Ocean Reg.* **2018**, *14*, 28–48. [CrossRef]
2. Bosco, F.; Jordan, A.; Krieger, Z.; Lewis, R.; Ogée, A.; Philbeck, T.; Pipikaite, A.; Uzunova, A. The Global Risks Report 2020 | World Economic Forum. In *The Global Risks Report 2020*; Wharton Risk Management and Decision Processes Center, University of Pennsylvania: Philadelphia, PA, USA, 2020; pp. 70–110.

3. Mclennan, M. The Global Risks Report 2021 16th Edition Strategic Partners. Available online: http://wef.ch/risks2021 (accessed on 9 August 2021).
4. Rizika, R. Maritime Cyber Attacks Increase By 900% in Three Years. Available online: https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/# (accessed on 9 August 2021).
5. Akos, D.M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (agc). *Navig. J. Inst. Navig.* **2012**, *59*, 281–290. [CrossRef]
6. Goodchild, M.F. Citizens as sensors: The world of volunteered geography. *GeoJournal* **2007**, *69*, 211–221. [CrossRef]
7. Wiese, B.M. Seized UK Tanker Likely 'Spoofed' by Iran: Lloyd's List. Available online: https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran (accessed on 9 August 2021).
8. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing cyber challenges of maritime navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [CrossRef]
9. Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. *Network* **2022**, *2*, 123–138. [CrossRef]
10. Androjna, A.; Perkovič, M.; Pavić, I. Cyber Security Challenges for Safe Navigation at Sea. In *14th Baška GNSS Conference: Technologies, Techniques and Applications across PNT*; David, B., Marko, V., Serdjo, K., Eds.; University of Rijeka, Faculty of Maritime Studies: Rijeka, Croatia, 2022; pp. 48–60.
11. Islam, S.; Bhuiyan, M.Z.H.; Thombre, S. Combating Single-Frequency Jamming through aMulti-Frequency, Multi-Constellation Software Receiver: ACase Study for Maritime Navigation in the Gulf of Finland. *Sensor* **2022**, *22*, 2294. [CrossRef]
12. Zhou, X.; Li, H.; Wen, J.; Wei, Y.; Yang, C.; Lu, M. GNSS Spoofing Detection Using Visual Inertial Odometry. In Proceedings of the 2022 International Technical Meeting of The Institute of Navigation, Long Beach, CA, USA, 25–27 January 2022; pp. 1392–1404. [CrossRef]
13. Warner, J.S.; Roger, G.J. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *J. Secur. Adm.* **2002**, *25*, 19–27.
14. Psiaki, M.L.; O'Hanlon, B.W.; Bhatti, J.A.; Shepard, D.P.; Humphreys, T.E. Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals. In Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011), Portland, OR, USA, 20–23 September 2011; pp. 2619–2645. Available online: https://www.ion.org/publications/abstract.cfm?articleID=9815 (accessed on 11 January 2022).
15. Psiaki, M.L.; O'Hanlon, B.W.; Bhatti, J.A.; Shepard, D.P.; Humphreys, T.E. GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Trans. Aerosp. Electron. Syst.* **2013**, *49*, 2250–2267. Available online: https://ieeexplore.ieee.org/abstract/document/6621814/ (accessed on 26 August 2021). [CrossRef]
16. Wang, F.; Li, H.; Mingquam, L. GNSS spoofing detection and mitigation based on maximum likelihood estimation. *Sensors* **2017**, *17*, 1532. [CrossRef]
17. Falletti, E.; Motella, B.; Signal, M.G. Post-correlation signal analysis to detect spoofing attacks in GNSS receivers. In Proceedings of the 2016 24th European Signal Processing Conference (EUSIPCO), Budapest, Hungary, 29 August–2 September 2016; Available online: https://ieeexplore.ieee.org/abstract/document/7760408/ (accessed on 11 January 2022).
18. Abreu, F.H.O.; Soares, A.; Paulovich, F.V.; Matwin, S. A trajectory scoring tool for local anomaly detection in maritime traffic using visual analytics. *ISPRS Int. J. Geo-Inf.* **2021**, *10*, 412. [CrossRef]
19. Ziółkowski, C.; Kelner, J.M. Doppler-based navigation for mobile protection system of strategic maritime facilities in GNSS jamming and spoofing conditions. *IET Radar Sonar Navig.* **2020**, *14*, 643–651. [CrossRef]
20. Dobryakova, L.; Lemieszewski, L.; Ochin, E. Cloud-based GNSS navigation spoofing detection. *Zesz. Nauk. Akad. Mor. Szczec.* **2019**, *57*, 29–37. [CrossRef]
21. Abramowski, T.; Bilewski, M.; Dobryakova, L.; Ochin, E.; Uriasz, J.; Zalewski, P. Detection of Spoofing Used Against the GNSS-Like Underwater Navigation Systems. *Preprints* **2020**, 2020010187. [CrossRef]
22. Dobryakova, L.; Ochin, E.; Lemieszewski, Ł. Design and analysis of spoofing detection algorithms for GNSS signals. *Zesz. Nauk. Akad. Morska Szczecinie* **2014**, *40*, 47–52.
23. Ochin, E. GNSS and DGNSS Spoofing Detection. *Ural Radio Eng. J.* **2017**, *1*, 55–79. [CrossRef]
24. Zhao, L.; Shi, G. Maritime anomaly detection using density-based clustering and recurrent neural network. *J. Navig.* **2019**, *72*, 894–916. [CrossRef]
25. Zhang, K.; Tuhin, R.A.; Papadimitratos, P. Detection and Exclusion RAIM Algorithm against Spoofing/Replaying Attacks. In Proceedings of the International Symposium on GNSS, Kyoto, Japan, 16–19 November 2015; Available online: https://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A1172940 (accessed on 16 August 2022).
26. Kuusniemi, H.; Blanch, J.; Chen, Y.H.; Lo, S.; Innac, A.; Ferrara, G.; Honkala, S.; Bhuiyan, M.Z.H.; Thombre, S.; Soderholm, S.; et al. Feasibility of fault exclusion related to advanced RAIM for GNSS spoofing detection. In Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017), Portland, OR, USA, 25–29 September 2017; Volume 4, pp. 2359–2370. [CrossRef]
27. Zalewski, P. Real-time GNSS spoofing detection in maritime code receivers. *Sci. J.* **2014**, *38*, 118–124.
28. Fu, P.; Haozhou, W.; Kuien, L.; Xiaohui, H.; Hui, Z. Finding abnormal vessel trajectories using feature learning. *IEEE Access* **2017**, *5*, 7898–7909. [CrossRef]

29. Zhang, T.; Zhao, S.; Bo, C.; Chen, J. Detection of AIS Closing Behavior and MMSI Spoofing Behavior of Ships Based on Spatiotemporal Data. *Remote Sens.* **2020**, *12*, 702. [CrossRef]
30. Singh, S.; Singh, J.; Singh, S. Mitigating Spoofed GNSS Trajectories through Nature Inspired Algorithm. *Geoinformatica* **2021**, *25*, 581–600. [CrossRef]
31. Singh, J.; Singh, S.; Singh, S.; Singh, H. Evaluating the performance of map matching algorithms for navigation systems: An empirical study. *Spat. Inf. Res.* **2019**, *27*, 63–74. [CrossRef]
32. Singh, S.; Singh, J.; Sehra, S.S. Genetic-inspired map matching algorithm for real-time GPS trajectories. *Arab. J. Sci. Eng.* **2020**, *45*, 2587–2603. [CrossRef]
33. Singh, S.; Singh, J. Location Driven Edge Assisted Device and Solutions for Intelligent Transportation. In *Fog, Edge, and Pervasive Computing in Intelligent IoT Driven Applications*; Wiley-IEEE Press: Hoboken, NJ, USA, 2020; pp. 123–147.
34. Singh, S.; Singh, J. Map Matching Algorithm: Empirical Review Based on Indian OpenStreetMap Road Network Data. *Int. Arab J. Inf. Technol.* **2022**, *19*, 143–149.
35. Borre, K. GPS Easy suite II. *Insid. GNSS* **2009**, *2*, 48–51. Available online: http://kom.aau.dk/~{}borre/easy2/easy13 (accessed on 19 August 2022).
36. Moreira, L.; Fossen, T.I.; Soares, C.G. Modeling, guidance and control of "Esso Osaka" model. *IFAC Proc. Vol.* **2005**, *16*, 85–90. [CrossRef]
37. Shin, J.; Kwak, D.J.; Lee, Y. Il Adaptive path-following control for an unmanned surface vessel using an identified dynamic model. *IEEE/ASME Trans. Mechatron.* **2017**, *22*, 1143–1153. [CrossRef]
38. Bhatti, J.; Humphreys, T.E. Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *Navigation* **2017**, *64*, 51–66. [CrossRef]
39. U.S. Coast Guard. Automatic Identification System (AIS) Data. Available online: https://marinecadastre.gov/ais/ (accessed on 7 July 2022).
40. Lee, Y.-S.J.S.J.H.S.J.B.C. A Novel GNSS Spoofing Detection Technique with Array Antenna-Based Multi-PRN Diversity. *J. Position. Navig. Timing* **2021**, *10*, 169–177. [CrossRef]
41. Marcos, E.P.; Konovaltsev, A.; Caizzone, S.; Cuntz, M.; Yinusa, K.; Elmarissi, W.; Meurer, M. Interference and Spoofing Detection for GNSS Maritime Applications using Direction of Arrival and Conformal Antenna Array. In Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018), Miami, FL, USA, 24–28 September 2018; pp. 2907–2922. [CrossRef]
42. Appel, M.; Iliopoulos, A.; Fohlmeister, F.; Pérez Marcos, E.; Cuntz, M.; Konovaltsev, A.; Antreich, F.; Meurer, M. Experimental validation of GNSS repeater detection based on antenna arrays for maritime applications. *CEAS Space J.* **2019**, *11*, 7–19. [CrossRef]