INSTITUTE of INFORMATION SECURITY
Graduate School of Information Security
Master's Thesis

Attack and Countermeasure for GPS-based Ship Navigation Systems

Student ID 5505504
Saneyuki Senda

Supervisor Kuniyasu Suzaki

February 2024

Abstract

Navigation systems such as AIS and ECDIS are indispensable for ship operations, and many of them rely heavily on satellite systems such as GPS to obtain the location information.

On the other hand, several maritime cases have reported attacks on GPS, and the vulnerability of GPS has been revealed. However, cybersecurity measures for ships, including navigation systems, have been very slow and many maritime organizations are exploring various countermeasures, but most of them are focused on conventional cyber-attack countermeasures and few are specific to ships.

This paper first investigates the relationship between GPS and GPS-based navigation systems in order to present the importance of GPS signals to ships. Next, the probability of radio frequency attacks such as jamming and spoofing against GPS-based navigation systems and security measures are investigated. We also examine the impact of GPS attacks on navigation systems and vessels, and the ship-specific countermeasures for open-sea and near-sea vessels, and propose a response chart showing the procedures for applying GPS and existing navigation systems as a GPS-independent method. Then, the similarity between the navigator's response to a GPS spoofing attack and the proposed method is verified using a ship-handling simulator device to identify new problems and to derive countermeasures necessary for future ship operations.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Research Background

In the maritime industry, with the development of maritime broadband communications such as satellite lines and ICT (Information and Communication Technology), there are concerns about various risks such as cyber attacks that violate ship navigation safety and economic damage. Ships are experiencing technological developments such as the widespread use of navigational instruments such as Automatic Ship Identification Systems (AIS) and Electronic Chart Information Display Systems (ECDIS), and rapid advances in sensors, IoT, AI, and big data processing. Large ships are being operated with fewer crew members than ever before, and the supply and demand for crew members is becoming tighter. In order to reduce the workload and improve efficiency, countries are developing and implementing autonomous ship technology. In Japan, the Ministry of Land, Infrastructure, Transport and Tourism has indicated that it plans to aim for the realization of autonomous ships in stages. Traditionally, each piece of equipment and system on a ship was independent, but as satellite links have become faster, some systems have been combined, making it possible to communicate data with land.

The maritime industry is a relatively small-scale industry; for example, there are approximately 98,000 commercial ships with propulsion of over 100 gross tonnage operating internationally[1]. This limits the industry's ability to conduct systematic analysis and learn from others, making it difficult to improving cybersecurity measures. A ship is a complex "sailing village" equipped with a variety of ICT. The range is wide-ranging, from office systems to life support systems, engine automation, and navigation systems. Ships typically have a lifespan of 25 to 35 years, and software upgrades occur at different time intervals for each piece of equipment. In other words, most ships have a mix of general IT (Information Technology) and OT (Operation Technology) equipment, which is complex and extremely difficult to maintain. Ships are subject to international regulation, but that regulation tends to focus on minimum technical requirements to ensure economic fairness,

making it a highly competitive and highly cost-sensitive market. Many stakeholders in the maritime industry do not give cybersecurity the priority it needs. Compared to general cybersecurity incidents, very little information has been made public about cybersecurity incidents in the maritime industry. This is said to be because there is no incentive to disclose information in the maritime industry. It is also said that this is due to reporting bias by the industry itself. Even so, the number of cases that are too big to hide is increasing as they tend to pose a threat to cybersecurity these days. Also, the number of incidents related to year and attack location does not have statistical significance to reveal a clear trend. Therefore, it is necessary to make a qualitative interpretation of the results. [2].

Over the past 14 years (2010-2024), the two main types of cyber incidents that affected ships were "Radio Wave Jamming" and "Malware infections" (particularly ransomware) (**Table 1.1**).

There have been several incidents in which shipboard IT systems have been attacked by malware, but the attack vectors are often accidental rather than targeted. Typical attack vectors are email attachments and links, which often render the ship's servers and clients unusable. Since all data is erased, the forensic evidence left behind is limited, making investigation difficult. OT systems are usually isolated from other systems, so they are rarely exposed. Nevertheless, instances of incidents against OT systems have occurred, and the consequences have been severe. Examples of attacks are system intrusions via infected USB memory sticks or computers that are unintentionally connected to the wrong network.Examples of systems targeted by attacks include ECDIS and propulsion control systems, and appear to occur during chart updates and system updates.

There are several examples of attacks on the communications systems of onshore and offshore facilities. While the impact on shipboard communications is less severe, there are many different and necessary communication systems on board that remain potential victims. These incidents show that hacking and ransomware tend to result in loss of availability

Vessels' position information is mainly obtained using GPS (Global Positioning System) signals. Since the GPS signal is used by ships for navigation purposes, attacks on the GPS signal are often related to "jamming" or "spoofing". This type of threat usually tends to manifest itself in geopolitically disputed areas such as the Black Sea.

Systems used for ship operations are increasingly integrating IT and OT. OT in ships are devices related to mechanical or electrical subsystems that automate shipboard operations, reducing costs and crew members' hazardous work. IT on ships, on the other hand, provides support for ship navigation planning, navigation control, and monitoring.Commercial vessels that sail internationally, such as large passenger ships and tankers, are subject to multilateral conventions that require them to be equipped with a variety of electronic devices [7]. The International Maritime Organization (IMO) has been pro-

Table. 1.1: Cyber Incidents Affecting Ships (2010 ～ 2024 年)[2]

Year	Attack	Summary
2016	Radio Wave Jamming	In South Korea, 280 ships had problems with their navigation systems and had to return to port. North Korea is believed to be the cause, but evidence is scarce [3].
2017	Radio Wave Jamming	In the Black Sea near Novorossiysk, the position data of at least 20 vessels indicated positions about 32 km away from their actual positions. These observations appear to be due to GPS spoofing [3][4].
2018～2019	Radio Wave Jamming	Several GPS disturbances were observed in northern Norway over a period of about two years. Some impact, but fortunately serious damage was avoided [1].
2019	Radio Wave Jamming	Ships exposed to GPS spoofing in the Black Sea. Although the ships were at sea, location information from the ships' navigation systems indicated that many ships were on land. This phenomenon reportedly occurred four times in three days, with the maximum occurrence time being approximately 30 minutes[2].
2019	Malware	On a large ship bound for New York, the ship's control system and network were infected with malware, limiting functionality [5].
2019	Malware	The management server of a tanker near the port of Naantali in Finland was infected with ransomware, and its backup data was also erased. Remote Desktop Protocol (RDP), USB devices, and email attachments have been identified as attack vectors. [2].
2019	Malware	Two vessels owned by the same owner were infected with the ransomware "Hermes 2.1" via a Word file attached to an email. Multiple workstations on the management network were affected[2].
2020	Malware	The ship's server and multiple client PCs on a ship docked near Tynemouth, UK, were infected with the ransomware "Ryuk". All data was encrypted and the system became unusable. Restored the system by complete reinstallation[2].
2020	Malware	Ransomware "Sodinokibi" infected the management systems of three American-flagged ships[2].
2023～2024	Radio Wave Jamming	At least six cases of GPS jamming and spoofing, believed to be by Russia, have occurred targeting Northern Europe and the Baltic Sea countries. [6].

moting e-Navigation [8] and other regulations and initiatives that have led to a significant digitization of shipboard systems, in which multiple systems are intricately integrated. The Integrated Navigation System (INS) is at the core of this digitization. By collecting information from various navigation systems and integrating their functions, the INS assists navigators and contributes to an improved overall situational awareness of the vessel [9].

On the other hand, the art of navigation is one of the basic skills for navigators, along with the art of shiphandling. Astronomical navigation used to be the cornerstone of ship and aircraft navigation, but it has been largely replaced by radio navigation. Radio navigation technology has evolved to include ground-based systems such as Loran, satellite-based systems such as GPS, and mixed systems such as Differential Global Positioning Systems (DGPS), which compensate for GPS positioning.. DGPS in Japan will be discontinued in 2019 due to the expected improvement of GPS accuracy and the start of operation of correction systems such as QZSS (MICHIBIKI) [10].

On top of that, ships stipulated by SOLAS (The International Convention for the Safety of Life at Sea) are equipped with ship-specific systems such as ECDIS and other navigation systems that are mandatory to be installed to support crews.

And after 2021, IMO mandates that the Safety Management System (SMS) of shipowners and operators of all ships, based on the International Safety Management Code (ISM Code) in SOLAS, must include cyber risk analysis and methods to protect ships and ship systems from cyber-attacks [11]. The IACS (International Association of Classification Societies) has issued a set of minimum requirements for ship cyber resilience. E26 (Cyber Resilience of Ships) [12] applying the NIST cybersecurity Framework as the minimum requirements for cyber resilience of ships and E27 (Cyber Resilience of Systems and Equipment on Ships) [13] applying IEC62443 as the uniform rules for cyber resilience of onboard systems and equipment. The two URs (Unified Requirements) will be applied to ships contracted for construction after July 2024. However, not many security measures against radio interference are described.

And since it is becoming more and more difficult to secure a crew these days, plans are underway to realize an automated vessel with independent decision-making and operating functions to further reduce the workload of vessel operation.

1.2 Research Objectives

The research objectives of this paper are to investigate the vulnerabilities of GPS and navigation systems, attacks on GPS and their impact, and current security measures for protection, and to propose a GPS-independent method and verify its similarity in order to identify issues for security measures for new navigation systems.

1.3 Research Results

The contributions of this study include the following.

- The impact of GPS attacks on navigation systems and vessels, and the organization of ship-specific countermeasures for open seas and near-shore waters
- Proposed response chart showing procedures for applying GPS and existing navigation systems
- Verification of similarity between GPS spoofing attacks and response charts using ship-handling simulator equipment at "National Institute of Technology, Hiroshima College", and verification of new problem extraction

This paper was presented at the "Computer Security Symposium 2023" [14] of the Information Processing Society of Japan and the "Symposium on Cryptography and Information Security 2024" [15] of the Institute of Electronics, Information and Communication Engineers.

1.4 Structure of this paper

This paper is organized as follows.

Chapter 2 describes existing navigational systems and support systems that are essential for navigating a ship, as well as existing navigational system maneuvering techniques that are tools for the operator (navigator) to obtain ship's position information. Chapter 3 describes the basic technical features of GPS. In Chapter 4, we describe the characteristics of attacks on GPS, mainly in the form of radio jamming, and discuss related research on countermeasures. In Chapter 5, we propose a response chart showing the procedures to be applied to existing navigation systems in case of GPS attacks. In Chapter 6, the response to GPS spoofing attacks is verified using a ship-handling simulation system to confirm the similarity of the proposed response chart. Finally, Chapter 7 summarizes this research and discusses issues to be solved in the future.

Chapter 2

Technical Background

This chapter describes the technical background of ship operation and navigation. Ships are equipped with navigation systems to assist in ship operation. The navigation system consists of several pieces of equipment.

2.1 Technical background in Shiphandling

Shiphandling techniques include the following.

- AIS (Automatic Identification System)
- Marine Radar
- ECDIS (Electronic Chart Display and Information System)

2.1.1 AIS

AIS (Automatic Identification System) is a system that transmits and receives information between ships or between ships and land using VHF radios to support safe and efficient ship navigation and to improve ship traffic operations. All passenger ships, ships of 300 gross tons or more engaged in international voyages, and ships of 500 gross tons or more not engaged in international voyages are required to be equipped with this system. The system exchanges static information such as the ship's name, identification code, and type of ship; dynamic information such as the ship's position, course, speed, and navigation status; and navigation information such as destination and estimated time of arrival. The dynamic information is displayed on the plotter screen of the ship radar or ECDIS by displaying the target symbol and vector representing the vessel, so that the speed and course of the vessel and the speed and course of other vessels can be easily grasped [16] .

AIS also has the same vulnerabilities as GPS[17][18] .

2.1.2 Marine Radar

RADAR (RAdio Detection And Ranging) is a system that uses radio waves to detect surrounding objects. The entire RADAR system depends on a variety of devices, but if we consider only the two main ones, the antenna unit and the display configuration, or PPI (Plan Position Indicator), the antenna rotates 360 degrees around a vertical axis, radiates radio waves, and receives the reflected waves from the target The antenna rotates 360 degrees around the vertical axis, radiates radio waves, and receives reflected waves from the target.

Marine radar onboard ships detects images of other vessels, route markers, and landfalls, and forms a crew's situational awareness based on the azimuth and distance of the images, as well as their time-varying information, and plays an important role in determining ship encounter situations and avoidance maneuvers (avoiding collisions and boarding), and in measuring positions [19]. Until the advent of ECDIS and AIS, radar has been used as a vessel's second set of eyes. ARPA (Automatic Radar Plotting Aid) enables Marine radar to automatically detect the tracks of other vessels [20].

Integration between shipboard radar systems and INS components is supported by navigation networks, two standard network protocols "NMEA 0183" and "ASTERIX CAT-240" [21]. The former allows interconnection between all devices and the latter allows video data transmission between shipboard radar antennas and displays. Two types of frequencies are used for shipboard radar: X-band (9 GHz band) and S-band (3 GHz band). On the other hand, S-band radar requires a larger antenna than X-band radar, but it can maintain its object detection capability even under the influence of fog, rain, and sea surface reflection. When two radars are installed, such as on a large ship, one X-band and one S-band radar are generally installed.

Different manufacturers have different specifications for shipboard radar antennas, including rotational speed and resolution related to bearing and range. Rotational speed specifies the speed at which the motor rotates the antenna. Azimuth resolution (angular resolution) determines the ability to separate nearby targets from targets at the same distance. Range resolution determines the ability to separate two targets in the same direction but at slightly different distances.

The antenna geometry is a slotted antenna with a narrow horizontal beamwidth and a large vertical beamwidth to allow for object detection even when the ship is moving. The horizontal beamwidth is generally 1 to 2 degrees and the vertical beamwidth is generally 20 to 30 degrees, depending on the antenna size and frequency. Horizontal polarization is used to reduce the effect of sea surface reflections.

2.1.3 ECDIS

ECDIS (Electronic Chart Display and Information System) [22] aggregates data from various sensor devices, including shipboard radar and GPS, with ENC (Electronic Navigational Chart) as the lowest layer. The ENC (Electronic Navigational Chart) is the bottom layer of the ECDIS, which aggregates data from various sensor devices, including Marine radar and GPS.

It is mandatory for SOLAS vessels to have it on board, and if two units are installed on a vessel, the vessel is exempted from carrying paper charts.

ECDIS has been shown to be critically vulnerable to weaknesses due to backup configuration (deployment), underlying operating system updates and secure setup, and in addition, has been determined to have a high risk level of cyber threat[23][24].

Fig. 2.1 and **Fig. 2.2** show the configuration of AIS, shipboard radar, and ECDIS, which are the navigation systems used in this study. The NMEA 0183 standard was established by the National Marine Electronics Association as a communication standard for GPS receivers and navigation systems. The NMEA 0183 standard was specified and managed by the National Marine Electronics Association as a communication standard for GPS receivers and navigation systems, and was internationally standardized as IEC61162-1 and IEC61162-2. 7-bit ASCII asynchronous serial communication is used, and devices on the data transmission and reception sides are respectively a talker and a listener. Data is sent from a single talker to a single or multiple listeners.

ENCs, which are charts displayed in ECDIS, are displayed by SENC (System ENC), which is a standard for each ENC dataset by S-57, in order to have an efficient data structure that allows quick display of data. SENC is converted to the ECDIS internal machine language format. The SENC format is different for each ECDIS manufacturer.

The functional requirements for ECDIS are as follows.

- All SENC information can be displayed.
- Select and highlight safety isobaths and safety depths.
- Can update ENCs and have a way to verify that they are loaded correctly into the SENC.
- When displaying radar and radar plotter (RP) information in ECDIS, charts, radar images, and RP information must match in scale, orientation, and projection method.
- ECDIS is equipped with a true azimuth display.

In addition, updating ENC data, which is essential for ECDIS, is done manually via USB memory or external storage media such as DVDs when data is downloaded via the

Internet or by e-mail, etc. Therefore, there is an inherent risk of infection by malware, etc. between air gaps.

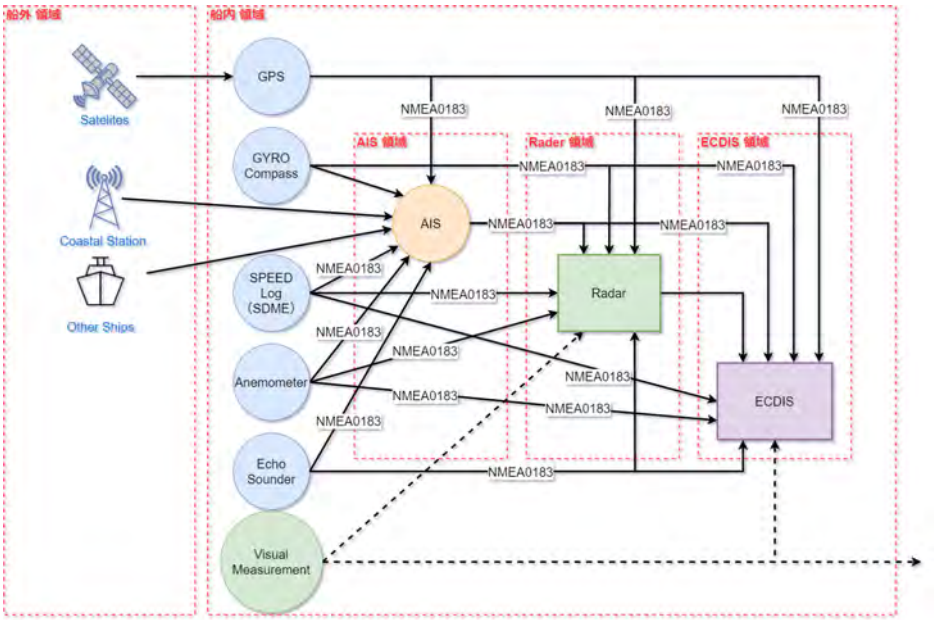


Fig. 2.1: Configuration of the navigation system

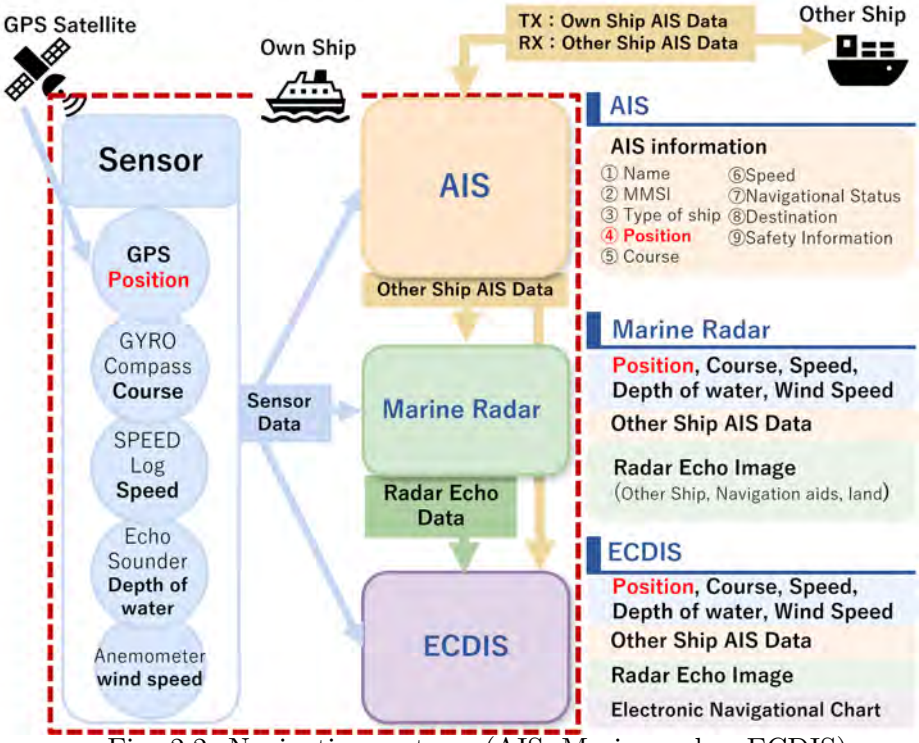


Fig. 2.2: Navigation systems (AIS, Marine radar, ECDIS)

2.2 Background of Navigation technical

The line segments drawn on the Earth's surface during vessel movement include the following line segments.

- A line of sight: A line segment drawn when a ship is sailing on a constant course with constant angles of intersection with meridians at various locations.
- Great Circle: A line segment connecting two points on the surface of a sphere with the shortest distance between them, used when crossing an ocean.

When the true calf line (true north-south line) is used as a reference, the intersection between it and the ship's wake is called the "True Course," and the intersection between the bow and stern lines (bow-stern line) is called the "Apparent Course. The intersection of the true bearing with the great circle passing through the surveyor and the object marker is called "True Bearing", and the intersection of the north-south line of the compass with the great circle passing through the surveyor and the object marker is called the compass bearing.

Ship navigation is a method of guiding a vessel from one point to another. The route a ship travels does not have a clear path like a road traveled by a car.In addition, ships cannot follow the route accurately due to external forces such as wind and waves, and will deviate from the route. Therefore, in order to guide a vessel to the desired point, it must periodically determine its exact position and correct its course and speed.

There are four main types of ship navigation: inertial navigation, geographic navigation, astronomical navigation, and radio navigation. The first navigation method developed was geographic navigation, which uses landmarks such as well-known landmarks as landmarks. Astronomical navigation, which uses celestial objects to navigate the open seas, was developed later.Inertial navigation is used to obtain a ship's course.

2.2.1 Inertial Navigation

Navigation systems have evolved over a long period of time based on a multitude of technological developments. INS (Inertial Navigation Systems) is the most important system of inertial navigation that indicates a ship's course.

The mechanism of the inertial navigation system uses an accelerometer and a gyroscope IMU (Inertial Measurement Unit) to measure acceleration and direction to obtain the heading that the bow of the ship is facing. Then, by integrating them, it is possible to obtain the speed and distance. By entering the starting position, the current position can be calculated relative to the distance and direction traveled. Therefore, in

order to calculate the relative position of one's vessel, the starting point and heading are indispensable.

Inertial navigation systems do not rely on external radio signals, so they are less susceptible to weather and interference. However, because they calculate the relative position of the ship by integrating the measurements from the sensors, the accuracy of the system deteriorates over long periods of time and long distances as gyro-compass errors and integration errors accumulate.

2.2.2 Terrestrial Navigation

Terrestrial navigation is a method of guiding a vessel to a target point while confirming its position (ship's position) by using prominent landmarks (mountain peaks, headlands, lighthouses, and other landmarks) marked on nautical charts. Since the ship is located in two-dimensional space on the earth's surface, it is necessary to determine two or more elements of the relationship between the location of the marker and the ship, such as azimuth, distance, and emphasis (two markers appear to overlap in the same direction), in order to determine the position of the ship[25].

Terrestrial navigation involves a wide variety of individual navigation methods for deriving ship positions. Among these, the most commonly used method to obtain accurate ship's position while navigating along the coast is called cross bearing. In cross bearing, multiple beacons (two or more) are selected, their azimuths are measured, and the ship's position is determined by the intersection of the line of position (LOP) that is the line segment of each beacon (図 **Fig. 2.3**). However, in the case of measuring the bearings of three object beacons, if the measurement errors overlap, the lines of position from the three object beacons do not intersect at a single point and an error triangle (Cocked Hat) is generated (図 **Fig. 2.4**). In order to minimize the error triangle as much as possible, it is necessary to pay attention to the intersection angle of the lines of position, select a prominent object whose position is accurate and whose distance is close, and measure the azimuth as soon as possible starting from the object whose azimuth changes quickly.

2.2.3 Celestial Navigation

Celestial navigation is a method of guiding a ship to a target point while checking its position using celestial objects[26]. In celestial navigation, two spheres are used for convenience: the real "Earth" and a virtual sphere called the "Celestial Sphere. The celestial sphere is assumed to be the surface of the celestial sphere with the earth at its center and infinite radius, and the positions of celestial objects on the celestial sphere are considered fixed. Since the earth rotates the center of the celestial sphere, the position

Fig. 2.3: Position acquisition by cross bearing[25]

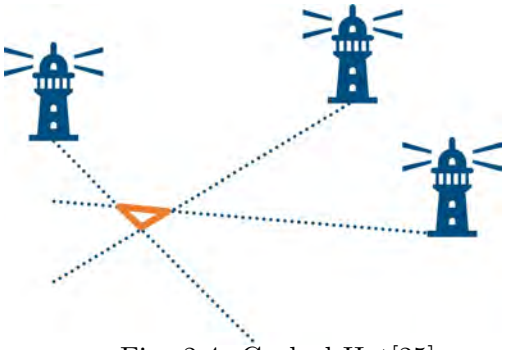


Fig. 2.4: Cocked Hat[25]

of the sun on the celestial sphere is apparently shifted, and the shifted path is called the ecliptic. The two points where the ecliptic and the celestial equator intersect are called "Vernal Equinox" and "Autumnal Equinox", respectively. The position of a celestial body on the celestial sphere is expressed in terms of its declination (angle from the equator) and right ascension (angle from the vernal equinox). The location of the celestial body to be observed from a ship at the time of observation can be expressed in terms of the local hour angle, which is the difference between the latitude on the earth and the celestial equatorial latitude. The time that has elapsed since the vernal equinox passed the local meridian (longitude time) is Sidereal Time, and the time we usually use is Mean Solar Time (equatorial time), which is based on the hypothetical sun (mean sun) that moves at a constant speed along the equator.

The relationship between the Right Ascension of Mean Sun and the equatorial longitude of each celestial body can be obtained from "The Nautical Almanac Japanese and UK edition (The Nautical Almanac Japanese edition is no longer available[27])". If the normal time at the time of observation is known, the position of the celestial body on the earth at that time (equatorial latitude and local time angle) can be determined. Since the only thing that can be observed in relation to a celestial body and a ship is the azimuth and

altitude of the celestial body, it is necessary to obtain the true altitude by correcting the observed altitude. On the other hand, the altitude of a celestial body can be calculated (Calculated Altitude) based on the estimated position (Dead Reckoning Position), and since the observed position is different from the estimated position, the difference in latitude and longitude between the observed position and the estimated position can be obtained from two or more celestial bodies by observation, drawing and The difference in latitude and longitude between the observed and estimated positions can be obtained from two or more celestial objects by drawing and calculating from observations.

The flow of the celestial survey on a vessel is as shown below, and consists of three phases: "Preparation," "Altitude measurement," and "Position determination[26](**Fig. 2.5**).

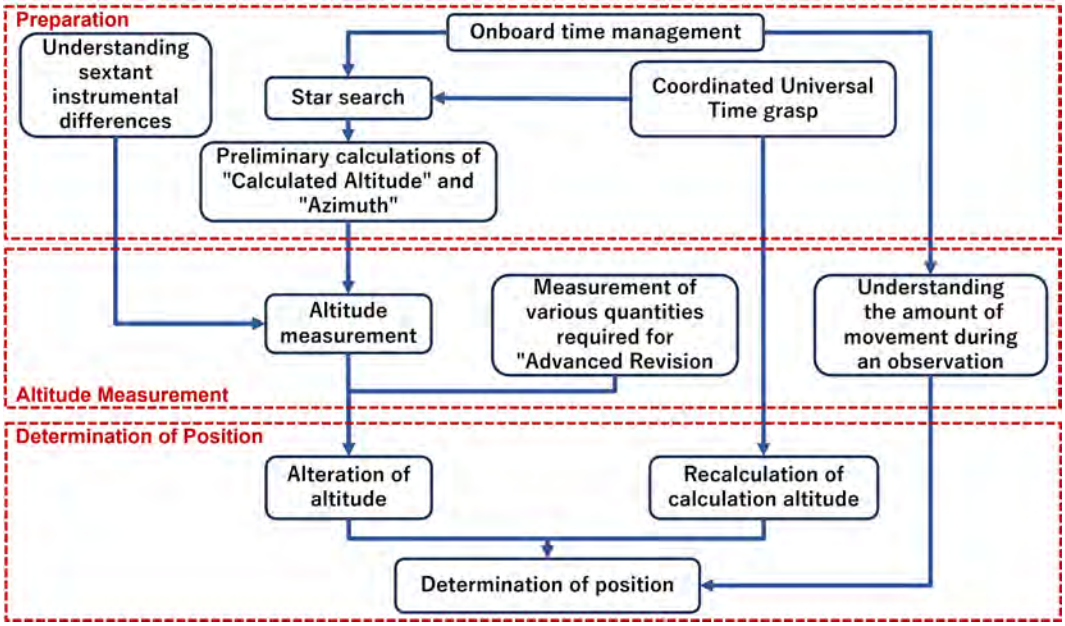


Fig. 2.5: The entire process of sky surveying in celestial navigation[26]

(1) **Preparation**

1. **Coordinated Universal Time grasp**

   In order to determine the calculated altitude of a celestial object, the position of the object is required. The positions of celestial objects are listed in The Nautical Almanac. In order to retrieve the position of a celestial object from The Nautical Almanac based on Coordinated Universal Time (UTC), the world time at the time of the celestial survey must be known. In order to keep track of world time, ships need high-precision shipboard reference clocks such as chronometers. However, it is necessary to keep track of any errors (e.g.,

chronometer errors) that may occur in the clocks.

2. **Understanding sextant instrumental differences**
   Sextant instrumental error (Index Error) affects the altitude calculation and must be understood.
3. **Onboard time management**
   The horizon must be visible to determine the altitude of a celestial body using a sextant. The time of day, sunset or twilight, when the horizon is visible, should be taken into account when selecting the observation period.
4. **Star Search**
   It is necessary to identify the objects to be observed. As mentioned above, the Sun, stars, planets, and the Moon are candidates. However, the objects to be observed are those that are within the range of 90° from the zenith to the true horizontal at the time of the observation. In addition, the magnitude of the object and the degree of refraction of the light rays must be comprehensively taken into consideration while taking into account the crossing angle between the lines of position.
5. **Preliminary calculations of "Calculated Altitude" and "Azimuth**
   Once the "time of observation" and the "estimated position" are determined from 1 to 4 above, the "azimuth" and "calculated altitude" of each object can be determined in advance. When observing, it is important to confirm on which side of the ship the object you have searched for is visible, taking into account the "azimuth" and the "ship's course".

(2) **Altitude measurement**

1. **Measurement of various quantities required for "Advanced Revision**
   Atmospheric conditions (atmospheric pressure, air and sea temperatures) must be observed in order to better revise the measured altitude (altitude revision). Since eye level is also a necessary factor for altitude revision, it is essential to confirm the eye height on the deck to be observed.
2. **Altitude measurement**
   Record the sextant altitude and Coordinated Universal Time (UTC) when the sextant telescope is aligned with the celestial body and the horizon.
3. **Understanding the amount of movement during an observation**
   At twilight, the sextant altitudes and UTCs are obtained for each of the multiple sources. Since the vessel is moving slightly, fine adjustment is required for each position line. The course and speed of the vessel at the time of observation should also be confirmed.

(3) **Determination of position**

1. **Recalculation of calculation altitude**
   The estimated position and the position of the celestial object are determined again from the onboard time and UTC when the altitude was measured, and the calculated altitude and azimuth are recalculated based on these. The calculated altitude calculated in advance deviates from the actual time of the measurement. The larger the time deviation, the larger the estimated position deviation, and thus the larger the correction difference. As the correction difference increases, an intersection of position lines appears at a distance from the estimated position. The greater the distance between the intersection and the guessed position, the greater the effect of the error in linear approximation. Recalculation is performed to avoid this.
2. **Alteration of altitude**
   The sextant altitude is the sextant reading when the altitude is measured. The instrumental error (I.E.) is added or subtracted to obtain the observed altitude. Various altitude corrections are added to this value to obtain the true altitude.
3. **Determination of position**
   Subtract the calculated altitude from the true altitude to obtain the corrected difference. From the corrected difference and azimuth, the line of position is identified, and latitude and longitude are determined as the true position by drawing or calculation.

The unique measurement methods used in astronomical navigation make it extremely difficult to automate. In order to replace human vision (visual observation), automated vessels can use images captured by cameras to identify objects through machine learning.

The feasibility of automating astronomical navigation has already been verified by simulations using a hybrid system of deep learning and convolutional neural networks to train a composite image of celestial objects combined with the time the image was taken [28].

2.2.4 Radio Navigation

Radio navigation, also called hyperbolic navigation, determines a line of position as one of a group of hyperbolas whose focal point is a fixed point if the distance difference from the fixed point is known, and the ship's position is determined as the intersection of such a line of position with other lines.

The following two methods are used to measure the difference in distance.

(1) Using pulsed waves, the difference in arrival time of radio waves from two transmitting stations is measured by utilizing the constant speed of radio waves (Loran navigation system [29]) .

(2) Continuous waves are used to measure the phase difference between the radio waves from two transmitting stations (Decca navigation system [30], Omega navigation system [31]).

These transmitting stations are located on the ground, but can be considered satellite navigation if they are located in space. The performance of each system is shown in **Table. 2.1**.

However, these transmitting stations have already been decommissioned and are no longer available [32].

Table. 2.1: Comparison of each radio navigation system

System Name	Radio Wave	Positioning Accuracy (Approx.)
Loran navigation system [29]	A:MF(1,750 ∼ 1,950kHz) C:(100kHz)	Several hundred m
Decca navigator system [30]	LF(70 ∼ 130kHz)	100 m
Omega navigation system [31]	HLF(10.2 ∼ 13.6kHz)	1,000 ∼ 2,000 m

The newest system in radio navigation is the LOLAN navigation system (LOng RAnge Navigation system). The LOLAN system is a navigation system that operates at 100 kHz. It was developed during World War II and played an important role in the navigation of ships at sea [29].

Initially, the system was operated as Loran A, and Loran C was developed and operated

as a later model. Later, a system called eLoran (Enhanced Long-Range Navigation) was studied, but has not been adopted due to the current GPS operational status. The Loran system uses the difference in arrival time of frequency signals from each radio station to obtain a position. Loran stations transmit (broadcast) pulse signals in groups called chains, each chain covering a specific area. Each chain consists of a main station (M) and several secondary stations (W, X, Y, Z). The secondary stations have eight pulses, the main station has nine, and the last pulse is used to identify the main station. The pulses in each chain are broadcast repeatedly at fixed time intervals called Group Repetition Intervals (GRI). The repetition interval of each GRI is designed to be different to eliminate cross rate interference. The station pulse interval is 1,000 µsec, with the last pulse of the main station 2,000 µsec away from the eighth pulse. For example, the West Coast chain is GRI 9940, whose pulses are transmitted every 0.0994 sec. The Loran stations are synchronized, and the timing of station transmissions is controlled by the system area monitor [33]. **Fig. 2.7** shows a diagram of the Loran chain signal and an ideal pulse [33]. Loran C enabled the Loran system to acquire positions by forming a chain of coordinated radio stations through international cooperation among the countries operating the system (**Fig. 2.8**, **Table. 2.2**) [34] .

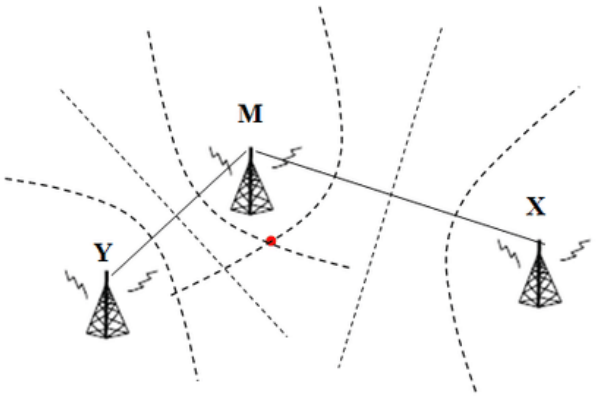


Fig. 2.6: Acquisition of position by hyperbolic curve [33]

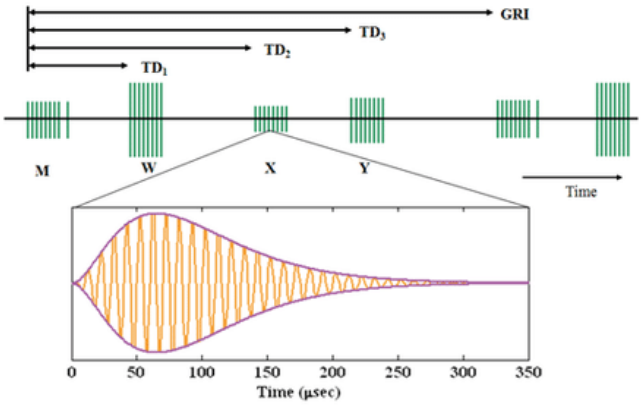
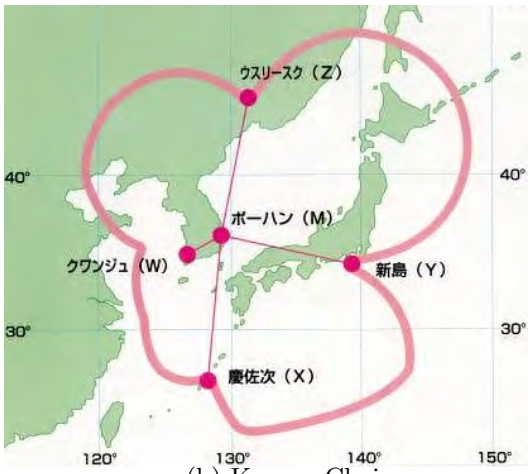
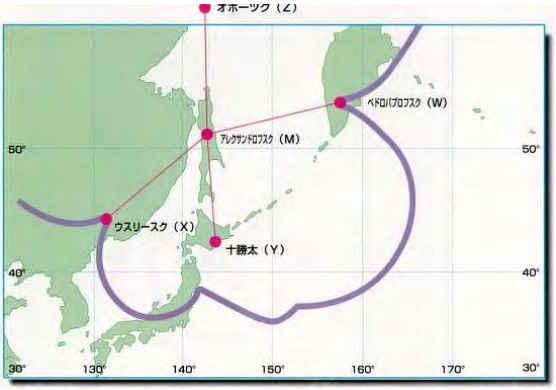


Fig. 2.7: Loran Chain Signal and Ideal Pulse [33]

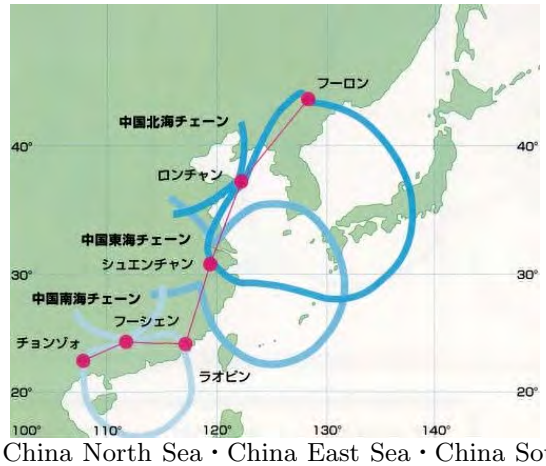
(a) Northwest Pacific Ocean Chain



(b) Korean Chain



(c) Russia Chain



(d) China North Sea・China East Sea・China South Sea Chain

Fig. 2.8: Example of Loran C International Cooperation Chain[34]

Table. 2.2: Example of Loran C International Cooperation Chain [34]

Chain Name	Station Name	Master & Slave	Transmission Power
Northwest Pacific	Niijima(Japan)	Master(M)	1000kW
Ocean Chain	Tokatibuto(Japan)	Slave(Y)	1000kW
GRI:8930	Gesashi(Japan)	slave(W)	1000kW
	Pohang(Republic of Korea)	Slave(Z)	150kW
Russia Chain	Alexandrovsk(Russia)	Master(M)	700kW
GRI:7950	Petropavlovsk(Russia)	Slave(W)	700kW
	Okhotsk(Russia)	Slave(Z)	10kW
	Ussuriisk(Russia)	Slave(X)	700kW
	Tokatibuto(Japan)	Slave(Y)	600kW
Korean Chain	Pohang(Republic of Korea)	Master(M)	150kW
GRI:9930	Niijima(Japan)	Slave(Y)	1000kW
	Gesashi(Japan)	Slave(Z)	600kW
	Kwangju(Republic of Korea)	Slave(W)	50kW
China North Sea	Rongcheng(China)	Master(M)	1200kW
Chain	Helong(China)	Slave(W)	1200kW
GRI:7430	Xuancheng(China)	Slave(W)	1200kW
China East Sea	Xuancheng(China)	Master(M)	1200kW
Chain	Rongcheng(China)	Slave(Y)	1200kW
GRI:8390	Raoping(China)	Slave(X)	1200kW
China South Sea	Hexina(China)	Master(M)	1200kW
Chain	Chongzuo(China)	Slave(Y)	1200kW
GRI:6780	Raoping(China)	Slave(X)	1200kW

2.2.5 GNSS

Each country has developed a GNSS (Global Navigation Satellite System) system as an alternative to GPS for radio navigation. The types of systems are listed in **Table. 2.3**. Each system operates in a different frequency band to avoid signal collisions with other systems. However, in order to use GNSS, it is necessary to have a receiver that is compatible with the frequency of each positioning satellite's signal or that can convert the signal and receive it.

GNSS is a group of satellites that transmit time and position from orbit, and several satellite networks exist. There are several satellite networks:

1. GPS (originally known as Navstar GPS)
2. Galileo (European Union)
3. GLONASS (Russia)
4. BeiDou (China)
5. NavIC (India)
6. QZSS (Japan)

The performance of GNSS makes it a potential target for many attackers. In addition, the low power of many GNSS signals makes them a serious technical weakness, as they are often subject to interference from natural solar flares, the Earth's ionosphere, other radio frequencies, and spectral congestion.

2.2.6 Galileo

Galileo[35] was developed in 1998 by the European Union (EU) to ensure full compatibility with the GPS system by providing an independent satellite positioning system for civilian use around the world. The SOL (Safety Of Life) service includes an authentication service to ensure that the received satellite signal is truly transmitted by Galileo. In addition, the SOL service includes integrity monitoring and notification, which alerts the user if the safe use of SOL signals cannot be guaranteed according to the specifications. 28 satellite constellations and a global ground control segment are used to ensure interoperability between the two systems. Measures are in place to ensure interoperability between the two systems.

2.2.7 GLONASS

GLONASS [36] is a Russian satellite positioning system that corresponds to GPS. It consists of a constellation of satellites in mid-Earth orbit, ground control segments, and user equipment. The constellation consists of 24 satellites in orbit. The signals are G1 (1602.00 MHz), L2 (1246.00 MHz), and L3 (1204.704 MHz). The feature of this system is that the frequencies are assigned in such a way that they do not interfere with other GNSS frequency bands.

2.2.8 Beidou

Beidou (BeiDou Navigation Satellite System) is China's own satellite positioning system [37]. The constellation has 52 satellites in orbit, the most of any satellite positioning system. There are five satellite signal frequencies: B1I (1561.098 MHz), B1C (1575.42 MHz), B2a (1176.45 MHz), B2b (1207.14 MHz), and B3I (1268.52 MHz), with B1C and

B2a complementing GPS L1 and L2.

2.2.9 NavIC

NavIC (Navigation Indian Constellation) is a GPS-compatible satellite positioning system that covers a limited area in and around India (including the Indian Ocean) [38]. The constellation of eight satellites is operated in two frequency bands: L5 (1176.45 MHz), which is the same as GPS, and S (2492.08 MHz), which is a stand-alone frequency band. It is a satellite system that can be operated only in the vicinity of India, which is a very difficult environment for normal use as an alternative to GPS.

2.2.10 QZSS

QZSS (Quasi-Zenith Satellite System), also called MICHIBIKI (Quasi-Zenith Satellite System), is a Japanese satellite positioning system [39]. QZSS can be called the Japanese version of GPS because it is designed to complement GPS first and foremost and covers all GPS frequencies. The satellites are in quasi-zenith and geostationary orbits of about 200 to 1,000 km and 36,000 km, respectively, and as of 2024, four satellites are in operation. Three of the four satellites cover the Asia-Oceania region. Currently, MICHIBIKI is complementing GPS and Galileo, but it is expected that a system of seven satellites will eventually be established, and that MICHIBIKI alone will be able to provide continuous positioning because more than four satellites will always be in the sky over Japan.

In addition, as a countermeasure against spoofing in satellite positioning services, a "Signal Authentication Function" that adds authentication information (digital signature) to navigation messages has been added and is scheduled to be operational from FY2024 [40].

Table. 2.3: Types of GNSS

System Name	Galileo[35]	GLONASS[36]	Beidou[37]	NavIC[38]	QZSS[39]
Developing Countries	EU	Russia	China	India	Japan
Number of Satellites	28	24	52	8	4
Approx. Altitude (km)	23,000	19,100	21,800	24,000 (3) 250 (5)	200 - 1,000 36,000
Frequency (MHz)	E1(1575.42) E5(1176.45) E6(1278.75)	G1(1602.00) L2(1246.00) L3(1204.704)	B1I(1561.098) B1C(1575.42) B2a(1176.45) B2b(1207.14) B3I(1268.52)	L5(1176.45) S(2492.08)	L1(1575.42) L2(1227.60) L5(1176.45) L6(1278.75)

Chapter 3

What is GPS?

3.1 GPS

GPS is the first familiar satellite positioning system using satellites (positioning satellites) owned by the U.S. government and operated by the U.S. Air Force [9].

3.1.1 GPS Overview

To use GPS for positioning, we use four positioning satellites to obtain position information (x, y, z). Calculate the distance between yourself and each of the four satellites to obtain four distances. The point where the four distances intersect is mathematically determined to be your position.

Assume a number of GPS satellite transmitters S_i orbiting at a known position $L^S \in \mathbb{R}^3$, each equipped with a synchronous clock with no clock. The exact time is offset to t^S and the navigation signal $s_i(t)$ is transmitted (broadcast). The signal in that case propagates at speed c.

GPS receiver V using an omni-directional antenna at coordinates $L \in \mathbb{R}^3$ receives the transmitted signal. It receives all signals that are within range:

$$g(L,t) = \sum_i A_i s_i \left(t - \frac{|L_i^S - L|}{c} \right) + n(L, t^s) \tag{3.1}$$

where A_i is the attenuation the signal undergoes between L_S and L, $|L_i^S - L|$ is the Euclidean distance between L_i^S and L, and $n(L,t)$ is the noise.

Due to the characteristics of the GPS signal $s_i(t)$, the receiver can separate each term of this sum and extract the relative spread-sign phase, satellite ID, data content, etc. by using a spread-sign replica. Then, given the data and relative phase offset, the receiver can estimate the distance by identifying the time delay $|L_i^S - L|/c$ for each satellite.

Then, given three known distances d_i and a known GPS transmitter position L_i^S, the three equations 3.2 can be uniquely formulated for L. except when all three S_i are located on the line.

$$d_i = |L_i^S - L| \tag{3.2}$$

Since the GPS receiver V is not bi-directionally clock-synchronized, having a clock offset $(t = t^S + \delta)$ yields the equation 3.3 from the equation 3.1.

$$g(L, t^S) = \sum_i A_i s_i \left(t - \frac{d_i}{c} - \delta \right) + n(L, t^S) \tag{3.3}$$

On the other hand, given a pseudorange R_i, the GPS receiver can infer the equation 3.3 from the delay $d_i/c - \delta$.

$$R_i = d_i + c \cdot \delta \tag{3.4}$$

The clock offset δ can be solved for both L and δ by adding a fourth unknown scalar value, so that the resulting equation 3.4 can be solved for both L and δ if pseudo-distance measurements for at least four GPS transmitters S_i are available. The resulting equation can be solved for both L and 3.4 to obtain both the exact position and time, without the need for an exact clock.

Then, if $L_i^S = (x_i^S, y_i^S, z_i^S)$, $L = (x, y, z)$, $\Delta = c \cdot \delta$ then we can transform the expression 3.4 into the expression 3.5 [41][42].

$$(x - x_i^S)^2 + (y - y_i^S)^2 + (z - z_i^S)^2 = (R_i - \Delta)^2 \forall S_i \tag{3.5}$$

Radio waves transmitted from a positioning satellite contain information on the time of transmission, so the difference between the time of transmission and the time of arrival of the radio wave at one's location determines the time of propagation. Calculations show that three pieces of distance information are enough to determine one's position, but the receiver's clock contains only a small amount of "error. However, because there is a slight error in the receiver's clock, there is a discrepancy in the position information among the

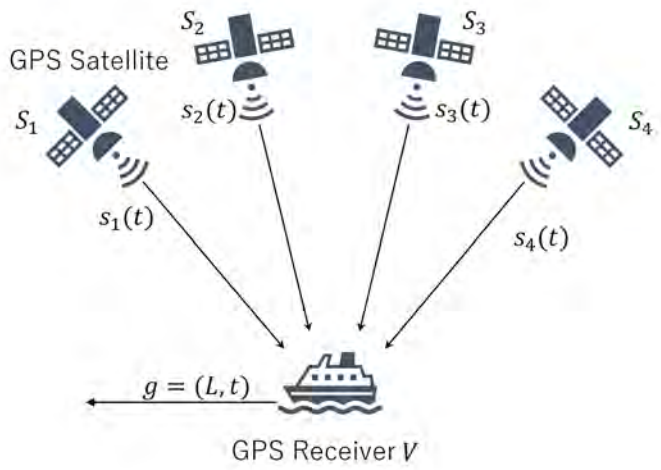


Fig. 3.1: GPS operation (Ship assumption)[42]

three satellites. To compensate for this slight error, information from at least one more satellite is required.

GPS positioning methods include "Independent Positioning," "DGPS (Differential GPS Positioning)," "Relative Positioning," "RTK-GPS Positioning," and "Network RTK-GPS Positioning.

There are two main types of positioning methods: single positioning and relative positioning. The single positioning method covers the entire world with an accuracy of about 10 m. The relative positioning method covers only the vicinity of a reference station, but provides highly accurate positioning.

GPS can determine the latitude and longitude of the current position by receiving radio waves from GPS satellites. For this purpose, there are about 31 GPS satellites orbiting around six orbits at an altitude of about 20,000 km (about 24 satellites in operation), as shown in **Fig. 3.2**. GPS satellites are constantly transmitting GPS signals to the earth's surface.

Because GPS uses radio waves, the receiver needs an antenna. The larger the antenna, the better the positioning accuracy. As mentioned earlier, GPS cannot be used indoors in tunnels and underground malls, where there are obstructions from satellites. Even indoors, it is often difficult to get a GPS signal, but high-sensitivity GPS receivers are designed to provide some position information.

To measure the distance between the satellite and the user and determine the position, the GPS signal must have at least the following three characteristics.

1. Must be able to measure the distance from the propagation time of radio waves.
2. Must be able to measure the distance to more than 3-4 satellites simultaneously.

item The user must be able to calculate the position of a satellite from time to time.

To satisfy the above requirements, each of the following conditions must be met.

1. The user must be able to determine when the currently received GPS signal was transmitted from a satellite.
2. The user must be able to receive GPS signals from each satellite without interference.
3. The information about the position of the satellite must be sent with the GPS signal.

GPS constellation coverage extends far beyond the land-based Loran system described above [43].

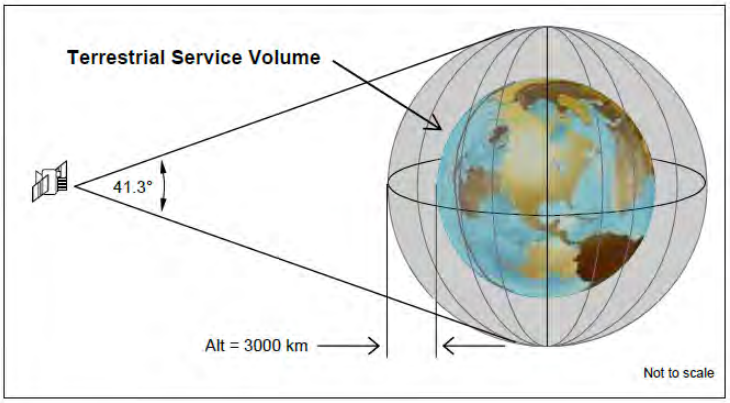


Fig. 3.2: GPS satellite constellation coverage [43]

3.1.2 GPS Signal

GPS [44] signals are produced by modulating the carrier wave with two codes called PRN codes (Pseudo Random Noise Codes) and navigation messages. The PRN code is an irregular code that randomly generates "0s" and "1s" and repeats the same pattern over a fixed length. In the early days of operation, GPS satellites transmitted data in two frequency bands, L1 (1575.2 MHz) and L2 (1227.6 MHz), with L1 being a "C/A The C/A code is used to identify GPS satellites and is used for coarse distance measurements, while the P(Y) code is used to identify GPS satellites and is used for coarse distance measurements. L2 carries only the P(Y) code, which is classified as classified, but it is possible to obtain a system that can receive the P(Y) code.

The PRN code has two characteristics. The first is that the code consists of a fixed pattern, so the user can know where in the overall pattern the currently received signal

falls. As a result, if the transmitter defines the timing of code transmission, the user can determine when the currently received signal was transmitted from the satellite. The shorter the length per bit of the code, the more accurate it is, so the P(Y) code is more accurate than the C/A code. Another feature is that the signal power of the modulated carrier is spread over a wide frequency band because the PRN code is a pseudo-random number; in the case of the P(Y) code, the signal power is spread over a band of about 20 MHz, and in both cases the signal is buried in the noise. This is why many GPS satellites do not interfere with each other even if they use the same frequency, and the signal power from the other satellites is less than the noise. This type of communication method is called spread spectrum communication, and is said to be excellent for multiplex communication and concealment. In order for a receiver to receive a GPS signal from a particular satellite, it is necessary to multiply the same PRN code again with the GPS signal transmitted by that satellite and remove the effect. As a result, the signal power that was spread over a wide bandwidth is returned to a very narrow bandwidth, allowing the signal to be captured. This process is called inverse diffusion. Because back-diffusion of GPS signals from unobjected satellites also causes interference, PRN codes are chosen to have the lowest possible cross-correlation (the correlation value between codes with different patterns).

Later, in the process of updating GPS, L1C (L1 Civil) signals were added to L1, L2C (L2 Civil) signals to L2, L5 signals [45] to a frequency band called L5 (1,176.45 MHz), and military signals called M codes to L1 and L2 (**Fig. 3.4, Table. 3.1**)[46].

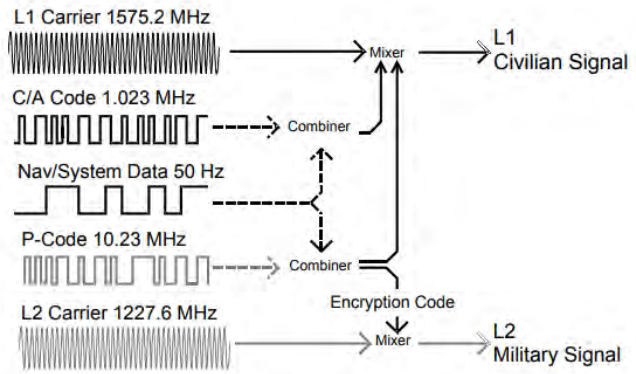


Fig. 3.3: Example of GPS signal generation [44]

The DOP (Dilution of Precision) is a value that indicates the degree of degradation of GPS positioning accuracy. The DOP value depends on the position of the GPS satellites, and the more evenly distributed they are in the sky, the higher the accuracy.

The field strength of the transmitted GPS signal is very small. It is transmitted at about 30 to 50 W, and by the time it arrives at earth, it is 10^{-16} W. This is why it is so

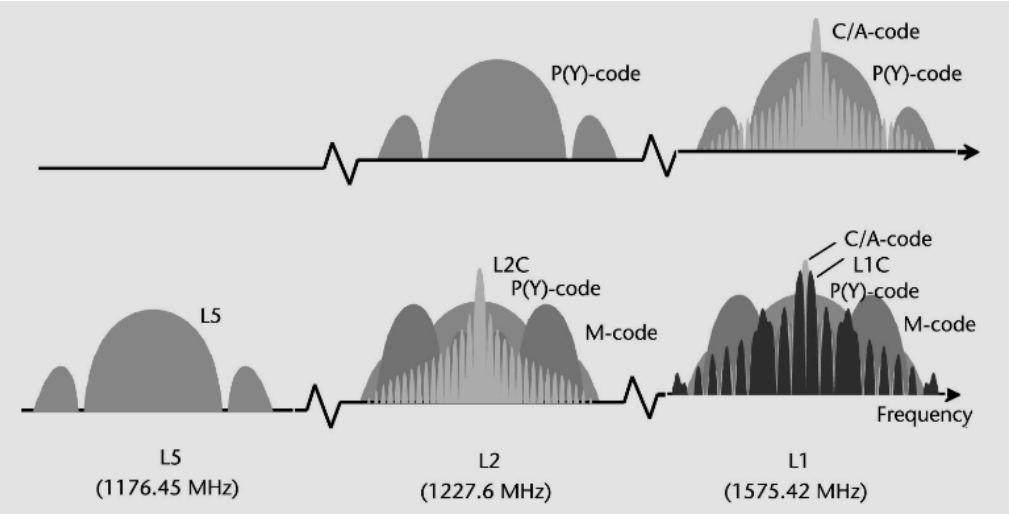


Fig. 3.4: Signals from GPS satellites (Old signal (upper row) & current signal (lower row)) [47]

easy to achieve GPS jamming [47]. The field strength of the transmitted GPS signal is very low. This is why achieving GPS jamming is so easy. All that is needed is a signal of the right frequency.

Table. 3.1: GPS signal (frequency band & PRN code)

L1 (1575.42 MHz)			L2 (1227.60 MHz)			L5 (1176.45 MHz)		
C/A	:	Civil code	L2C	:	Civil code	L5	:	Civil code
L1C	:	Civil code	P(Y)	:	Military code			
P(Y)	:	Military code	M	:	Military code			
M	:	Military code						

3.1.3 GPS receiver configuration

A GPS receiver receives all GPS signals transmitted by GPS satellites orbiting in the sky and measures the distance between the GPS satellites. The GPS receiver can calculate its own position if it can receive signals from at least three to four GPS satellites, depending on the type of GPS receiver. If conditions are good, the receiver can determine the current position with an accuracy of several meters, although this depends greatly on the performance of the GPS receiver and the surrounding environment. The processing circuitry of a GPS receiver is now on a chip and can be integrated into a cellular phone.

In addition to reverse diffusion of the PRN code and decoding of the navigation message, the receiver also performs carrier wave phase tracking. The carrier phase represents the integral of the Doppler shift between the satellite and the user, and is used to output the delta range and the observed quantity called the carrier phase. The configuration of the receiver varies depending on how the hardware is assembled, but as a result of recent advances in semiconductor technology, most receivers use digital processing circuits and control processors to perform the main processing, while the analog portion consists only of an antenna and a circuit that down-converts the carrier wave to an intermediate frequency. The digital processing consists of a delay-lock loop that performs inverse PRN code diffusion, a costus loop that tracks the carrier phase, and a message decoding loop that decodes the navigation message. In general, the order of processing is as follows: the delay lock loop performs inverse diffusion, followed by the costus loop, which establishes carrier phase synchronization and extracts the navigation message [47].

Chapter 4

Related Research

In this study, we present related research mainly in the navigation systems that may be attacked by GPS and in the satellite line equipment that supports the communication lines.

4.1 GPS Vulnerability

4.1.1 GPS jamming

GPS jamming, also known as masking, is an attack in which a signal is transmitted at the same frequency as the target signal and with equal or greater power, making the receiver unable to distinguish between the legitimate signal and the jamming signal. Jamming is an attack that makes the receiver unable to distinguish between a legitimate signal and a jamming signal, or makes the receiver unable to recognize a legitimate signal. Jamming does not require advanced techniques, although it requires the collection of information such as frequencies and output magnitudes in advance. As described in **Section. 3.1.2**, attacks on GPS receivers need to be limited to the downlink, which is the communication from GPS satellites to ground radio stations including ships, and since the output power of GPS signals transmitted from satellites is very small, it is very easy to achieve attacks on GPS. Depending on the distance, a signal of a few W is enough to achieve this. The PPD (Personal Privacy Device) jammer, which is an attack tool, is inexpensive, costing only a few tens of thousands of yen, and is readily available on the Internet [48].

The attack only affects the receiver while it continues to transmit, so once the attack is stopped, the legitimate signal can be received again, and it does not necessarily cause permanent damage to the receiver.

However, in the event of an attack, it is possible to detect the direction of the attack, but it is difficult to measure the distance. In the event of an anomaly in the navigation system, it is very difficult to determine whether the attack was intentional or an accidental

failure.

As a related study of GPS jamming for ships, GPS jamming experiments were conducted in actual sea areas [49]. The test was conducted by transmitting a known PRN code (C/A code) over the entire 2 MHz bandwidth of L1 from a GPS jammer unit at 25 m above the ground with a total power of about 2 dBW ($\sim$ 1.5 W) at low power (maximum power 1.58 W). Dynamic and static tests were conducted over a period of three days by navigating the attacked vessel in the surrounding waters, and the possible effects of GPS jamming on various factors of safe navigation were confirmed (**Fig. 4.1**, **Fig. 4.2**).

Vessels subjected to GPS jamming attacks lost their GPS positioning capabilities and ECDIS was particularly affected, affecting the safe navigation of ships at sea and in particular the ability of the crew to navigate safely. The safety and security of the crew may be seriously affected by the inability of the ship's crew to recognize that they are being GPS jammed and by the loss of the opportunity to switch to an alternative navigation method. Alan's [49] have identified a number of countermeasures to GPS jamming, including the use of Roland Roland's Roland Rockett (RRT), which is a GPS jamming technique that can be used to detect and prevent GPS jamming. Alan's proposed supplementing the Loran system as a countermeasure to GPS jamming. However, while many vessels were equipped with Loran systems as a supplement to GPS at that time, they are no longer feasible because the Loran system service has been discontinued or reduced in many countries nowadays [32].

Fig. 4.1: GPS jammer unit installed in Flamborough Head, England [49]

Alan's [49] also studied the impact of attacks by PPD jammer devices using the conventional method of GPS L1, as well as the impact of GNSS attacks in cooperation with the German Aerospace Center (DLR: Deutsches Zentrum für Luftund Raumfahrt) and

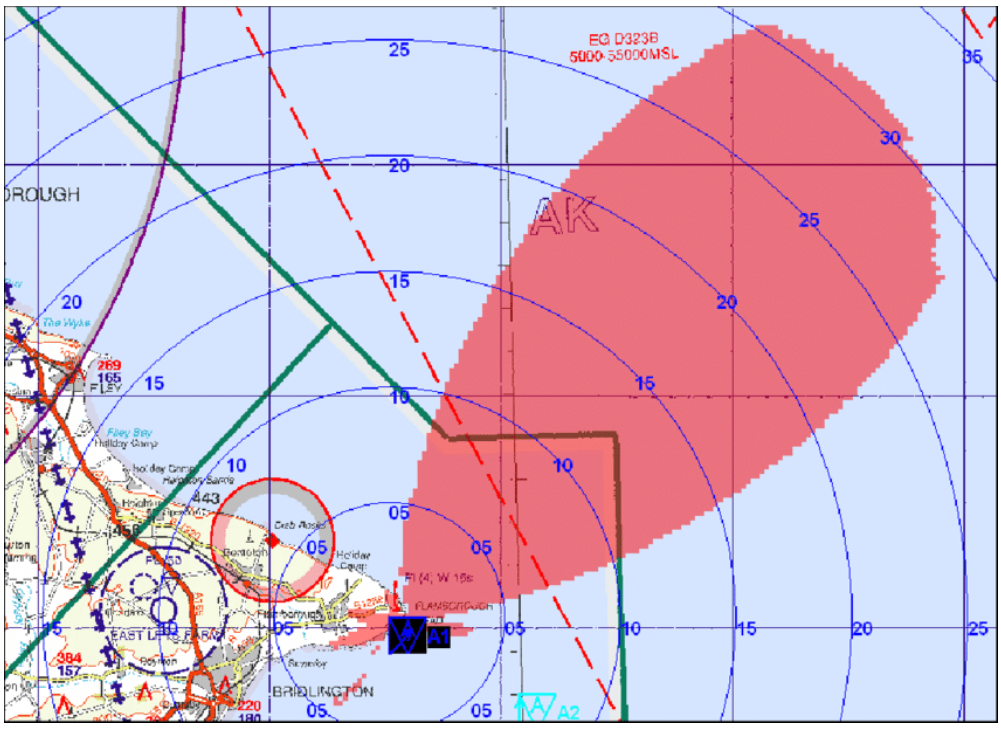


Fig. 4.2: GPS jammer unit coverage area [49]

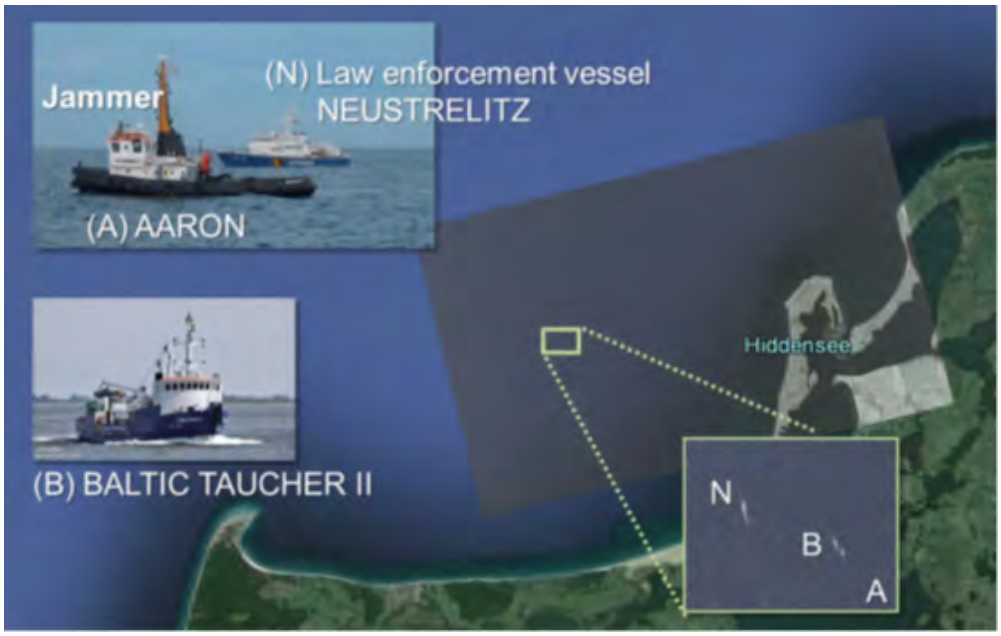


Fig. 4.3: GNSS jamming experiment in the north of Daru Peninsula [50]

the German Federal Network Agency for Electricity, Gas, Telecommunication, Post and Railway (BNetzA), as well as Alan's. The GNSS jamming testbed was prepared in coop-

eration with the Federal Network Agency for Electricity, Gas, Telecommunication, Post and Railway (BNetzA), as well as with Alan et al. (BNetzA), a GNSS jamming testbed has been prepared and GNSS jamming experiments have been conducted in actual maritime environments. Daniel's [50]. prepared three vessels (attack ship [A], damaged ship [B], and alert ship [N]) in a test area located about 10 km north of the Dals peninsula in the Baltic Sea, as shown in **Fig. 4.3**, for a period of 3 h (07:00 - 10:00 UTC on October 22, 2015), where the attack ship was The test was conducted with the attacking vessel anchored in the center of the experimental area, while the damaged vessel sailed at a distance of 40 m to 4,000 m, at a maximum speed of 8 kts. The results of the experiment show that even an attack with a PPD jammer device of relatively simple specifications had an impact over a very large area. On the other hand, the results show that the GNSS is not necessarily affected when close to the source of the attack.

4.1.2 GPS Spoofing

GPS spoofing is the transmission of generated false signals to a target's receiver to provide deceptive information and confuse location information. A cybersecurity incident involving GPS spoofing occurred in June 2017, when the navigation systems of approximately 20 vessels were guided to different locations while sailing in the Black Sea, even though they were operating properly. It is believed that this was most likely due to interference with GPS signals caused by GPS spoofing by the Russian authorities [4]. In addition, the GPS receiver of one of the vessels at that time is said to have confirmed multiple GPS satellites showing approximately the same values of field strength, suggesting an attack from the same transmission output or the same location (**Fig. 4.5**)[51].

The attacked vessel was able to determine the presence or absence of a GPS spoofing attack by using a VHF telephone to check for similar phenomena on other vessels sailing in the vicinity.

4.1.3 GPS Meaconing

GPS Meaconing is an attack that records a legitimate GPS signal, delays it for a certain period of time, and then transmits it to a target receiver to confuse it. As in a man-in-the-middle attack, an RF recorder, which can receive, record, and play back any wireless signal, can be easily used as a meaconing device if it can play back the recorded GPS signal by attaching an antenna to it for transmission. One possible countermeasure against meaconing is to compare the GPS signal with a clock built into the GPS receiver, but there is no unified standard for this function since it varies depending on the GPS receiver. In addition, it is said that this is not an effective countermeasure against meaconing by

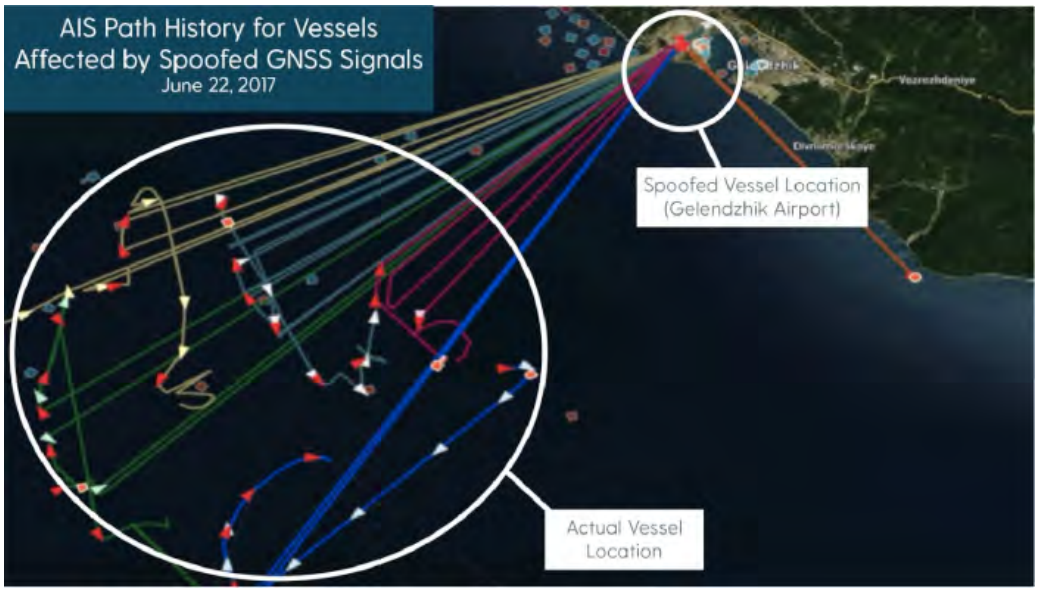


Fig. 4.4: GPS spoofing situation [4]

repeaters and those with only a very short delay even in playback [48].

4.2 Security countermeasures for GPS

The vulnerability of civilian GPS signals to spoofing attacks is discussed as a security measure against attacks on GPS [44]. They also describe how GPS works and elaborate on the structure of the GPS signal. warner's [44] describe suggestions for detecting deception signals to counter spoofing attacks, including monitoring GPS signal strength, monitoring satellite identification codes, checking time intervals, comparing time timings and using an accelerometer to counter-checking using accelerometers, and so on. The proposals of Warner's are not demonstrated because no tests have been conducted to evaluate the performance of each method. In addition, most of the proposed methods only monitor signal characteristics.

In addition to the above, the following measures have been proposed.

1. **Protection by Signal Processing**
2. **Protection by Authentication**
3. **Protection by Sensor Fusion**
4. **Protection by Antenna**

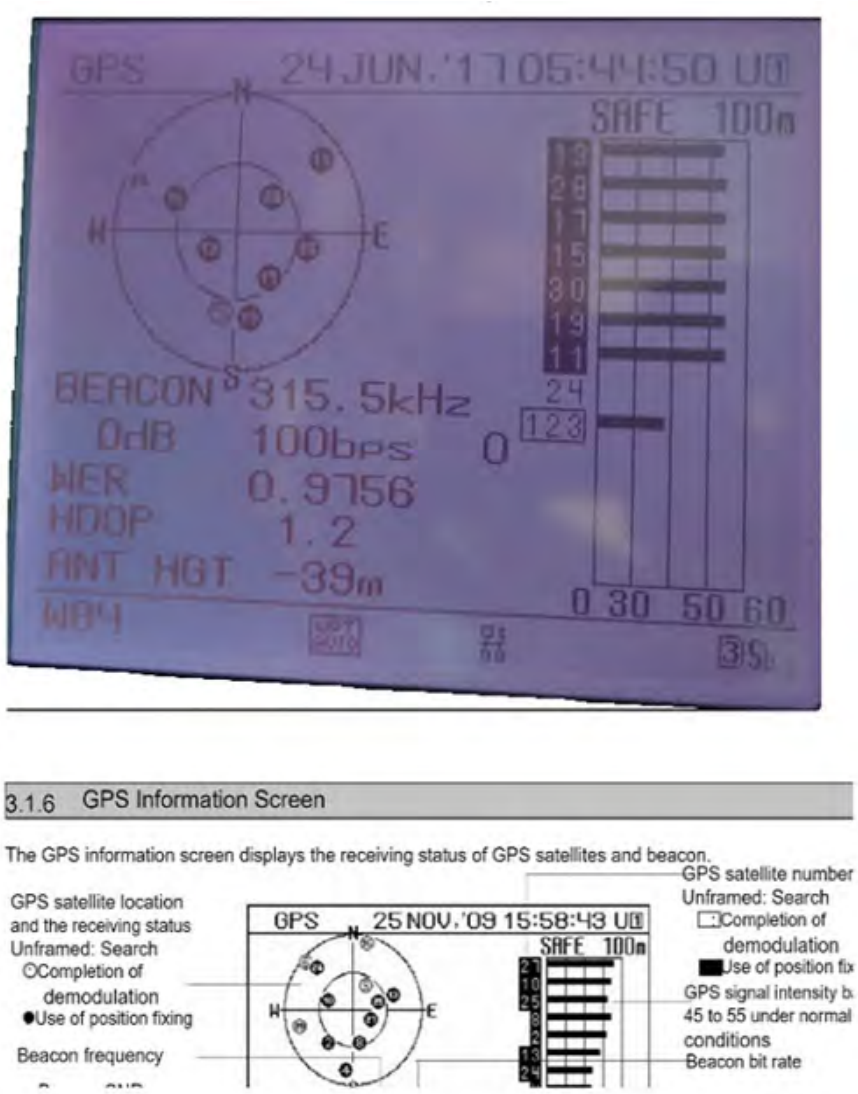


Fig. 4.5: GPS spoofed receiver status [4]

4.2.1 Protection by signal processing

There are spoofing detection techniques that can be implemented as signal processing algorithms in standard GPS/GNSS receivers.

(1) Signal distortion search
(2) Signal complex correlation function search
(3) Total acquisition search

The method in (1) searches for distortions or disruptions that occur during signal drag-off. The simplest technique is to search for unreasonable sudden jumps in the received

carrier amplitude A_i, beat carrier phase φ_i (t), or code phase τ_i (t). A sudden increase in A_i or an unusual displacement of φ_i (t), or τ_i (t), is said to occur at the beginning of an attack [52]. A search technique is to monitor the total received power of RPM (Received Power Monitoring) on an absolute scale. What this technique requires is to look at all received A_i values and the Automatic Gain Control (AGC) settings of the receiver RF front-end [53]. Then, the spoofer requires a significant power advantage, $A_s i \gg A_i$ (for all $i = 1, . , N$) is required, the total power may suddenly increase at the beginning of the attack. A sudden power spike may indicate an attack, especially if it increases by more than 1 to 2 dB. However, it is vulnerable to overpower attacks, including Noise Floor Spoofing [54].

The method in (2) is a detailed study of the complex correlation function when the receiver synthesizes the tracking loop discriminator. During the initial drag-off of a spoofing attack, the autocorrelation function is distorted due to the mismatch between the true code signal and the spoofed false code signal and carrier phase. To search for distortions in the correlation function, even a typical GPS/GNSS receiver is considered capable of correction [55]. The main requirement is to compute additional complex baseband correlations between the receiver's signal replica and the received signal, and these correlations are computed with a set of delay extensions along the code offset axis.

However, searching for complex correlation functions has two drawbacks [52]. First, natural multipath signals produce similar results. Therefore, the spoofing detector must verify that the observed distortion cannot be proven as mere multipath before issuing an alarm. Second, detection performance is poor when the spoofer device significantly overpowers the true signal. The output of the spoofer equipment necessary to avoid distortion is possible with the RPM detection scheme. Another issue is the transient nature of the detection [52]. If an attack is not detected at drag-off, both methods (1) and (2) may miss the opportunity to detect the attack.

The method in (3) is to constantly attempt to reacquire all the signals tracked. For each signal, a brute-force acquisition search is performed over the entire range of code phase and carrier Doppler shift. However, brute-force acquisition searches impose a large signal processing load on the receiver. Therefore, one reasonable approach is to search for additional instances of the tracked signal sequentially, one signal at a time. If a second version of the received signal is detected, the receiver is returned to the initial acquisition mode and all instances of all signals are searched again by brute force search. The receiver then attempts to sort out the true signals from the spoofed signals and restore the navigation function. However, this technique can be defeated by an overly powerful spoofer device that intercepts the true signal and renders it undetectable during the research. For strong spoofer devices, the RPM scheme is considered effective for detection [52].

4.2.2 Protection by Authentication

One of the countermeasures against spoofing is the authentication of positioning signals transmitted by GPS satellites. This is done by using a public-key cryptosystem that uses asymmetric key pairs for encryption and decryption to identify deception signals. Although this method cannot be used for GPS signals whose specifications have already been published, it is being used in other satellite navigation systems [40]. Specifically, the public key used for decryption is made known to the user in advance (and installed in the receiver), and if the signal can be decrypted correctly with this public key, it is guaranteed to have been generated by an operator who possesses the private key corresponding to the public key. However, it is difficult to maintain the strength of the authentication because the format of the information obtained as a result of decoding is known, the amount of information is not large, and the key pair cannot be changed arbitrarily because it is a one-way communication. On the other hand, encryption of positioning signals transmitted by GPS satellites has also been considered [48] , but it is not considered necessary because sensitive information is not included in the signals.

4.2.3 Protection by Sensor Fusion

If the physical movement status of the GPS receiver (antenna) is known, the presence or absence of deception can be determined. For this purpose, it is useful to compare with position sensors other than GPS [48]. Various sensors can be considered, but as mentioned above, ships are equipped with many sensors, especially the IMU (gyrocompass), so it is considered easier to compare signals than in other types of vehicles.

4.2.4 Protection by Antenna

As a characteristic of spoofing and meaconing in past cases, the attacker is expected to transmit from the vicinity of the ground. Therefore, although GPS receiving antennas are omni-directional in nature, a countermeasure is to make them directional so that they receive only signals coming from the direction in which GPS satellites actually exist (**Fig. 4.6**). However, since parabolic antennas are commonly used for directional antennas and are large in size, array antennas using multiple antennas are being considered as the main method of reception [48][56]. Since at least three types of antennas need to be arranged to achieve three-dimensional directivity, it is difficult to adopt this method in mobile devices.

It is also impossible for an attacker to place an antenna at the same position as a GPS satellite. Therefore, even if spoofing or meaconing is performed for a GPS receiver at a specific location, the same effect cannot be achieved for GPS receivers at distant locations.

In other words, it is not possible in principle to create a consistent deception signal for a wide geographic range of GPS receivers. It is proposed to use a network of many GPS receivers [48]. The measurements obtained by the GPS receivers participating in the network are compared and discrepancies are detected. Furthermore, it is also considered that GPS receivers exchange measurements and compare them with each other, which would function as an autonomous deception detection method. However, the location of the receivers for comparison may be difficult because of the need for separate transmission and reception.

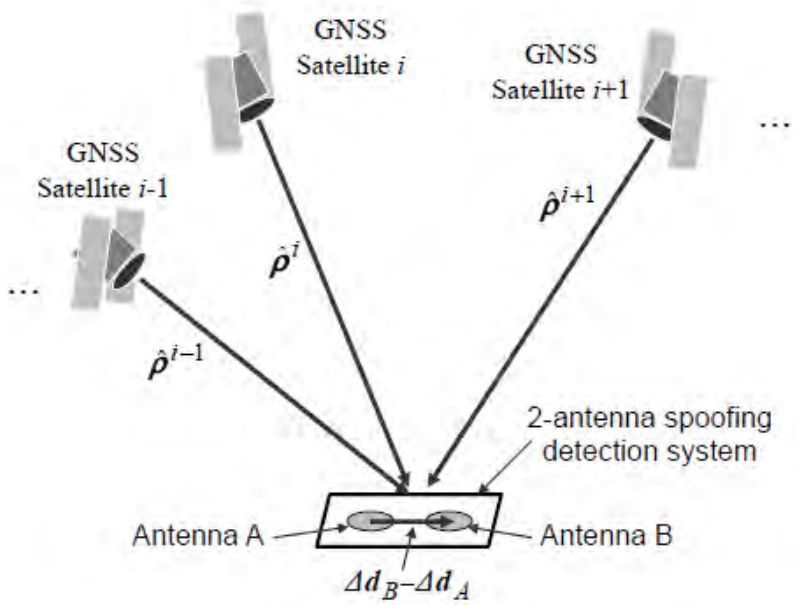


Fig. 4.6: 2-antenna based spoofing detection of typical signal arrival shapes [52]

4.3 Challenges with existing security countermeasures

As mentioned by **Section 4.2**, countermeasures against attacks on GPS have been studied in a wide range of areas, mainly detection, but have not been applied to existing navigational systems. However, the application to existing navigational systems has not progressed yet [57].

Because ship operations are subject to external environmental influences (e.g., wind, waves, ship traffic, etc.), the availability and continuity of ship operations are extremely important, and safe operations cannot be continued if they cannot be handled. Therefore, cybersecurity measures for OT equipment are highly necessary, but their application has not progressed much. Therefore, it is necessary to study the incident response of operators (navigators) to cyber-attacks, and to promote a common understanding of information

security incidents with related parties based on these studies, otherwise, availability and continuity may be lost. In addition, as mentioned in **Section 1.1**, it is important to study this knowledge as automation and autonomization are progressing.

Chapter 5

Proposed Method

When a ship's GPS is attacked by radio waves, it is very difficult for existing navigation systems to detect the presence or absence of the attack. In this chapter, we review shiphandling and navigation techniques, as well as navigation systems related to them, in order to examine detection and response methods to GPS attacks on ships by radio waves.

Based on the results, we derive the appropriate response flow, and propose the appropriate action flow to be taken by the crew (navigator or communicator) in case of an attack.

5.1 Organize navigation systems • Maneuvering • Navigation techniques

The positioning performance of the navigation methods used in navigation is compared, and the navigation systems that serve as tools for navigators are organized and their applications are discussed. GNSS, including GPS, is originally one of the radio navigation methods, but is treated as a separate method from radio navigation in order to separate the methods to be selected.

5.1.1 Comparison of positioning performance by navigation method

In the navigation technique described in **Section 2.2**, the method that can obtain position information as an absolute position by each navigation method is shown in **Table 5.1**. Radio navigation systems such as the Loran system are inferior to GNSS satellites, including GPS, which can communicate data from the sky, because the system has not been updated. In addition, the coverage area is dependent on the country where the service is provided, so it is also inferior in terms of application range. As mentioned in **Section 2.2.4**, many countries have discontinued the service.

Table. 5.1: Comparison of positioning performance by navigation method (Absolute Position)

Method	Accuracy (Approx.)	Scope of Coverage (Approx.)	Remarks
GNSS	1 m	Unobstructed	-
Radio navigation	100 m	1,000 km	Many abolished
Terrestrial Navigation	185 m	60 km (location dependent)	Nautical charts are required
Celestial Navigation	185 m	Visual range	Affected by Weather

Table. 5.2 shows the methods that can be used to obtain position information as a relative position for each navigation method in the navigation techniques described in **Section 2.2**. Visual observation is a visual measurement by the navigator, who is the crew of the vessel, and the navigational decisions are made by selecting and comparing the actual sea conditions, each system, and each navigation method.

Table. 5.2: Comparison of positioning performance by navigation method (Relative Position)

Method	Accuracy (Approx.)	Scope of Coverage	Remarks
Inertial navigation	300 m	Unlimited	Situation dependent
Visual	100 m	Only when visibility is good	-

5.1.2 Organize Categories

Each system, shiphandling and navigation system is divided into four layers as shown in **Fig. 5.1**. "Layer 4" is the full specification of each system, maneuvering and navigation for vessel position acquisition, and the number of available systems and navigation options decreases as one moves from "Layer 4" to "Layer 3" to "Layer 2" to "Layer 1".

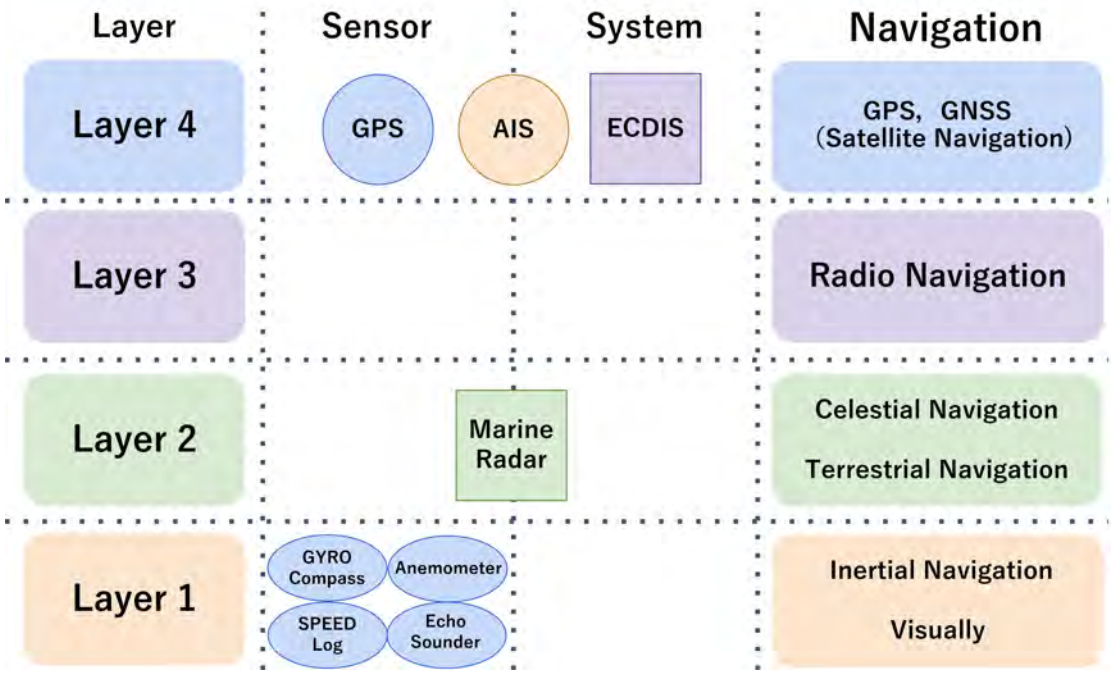


Fig. 5.1: Navigation Systems and Maneuvering (Navigation) Categories (Layered)

5.2 Response Chart to GPS Attack (Proposed Flow)

The navigator operating a vessel must navigate the vessel to a safe position by appropriately selecting the maneuvering and navigation techniques described in **Chapter 2**, depending on the sea area and conditions in which the vessel is navigating. The navigator must choose which maneuvering and navigation technique to apply based on the current ship's condition. However, the current state of the art is that which navigation technique and tool to use in the event of a GPS attack is still a matter of experience for each navigator, and has not yet been discussed. Therefore, this study proposes a flow of measures to be taken in the event of a GPS jamming/spoofing attack.

Assuming four ship situations from **(A) ∼ (D)**, we propose the application of the flows shown in **Fig. 5.2**, **Fig. 5.3**, **Fig. 5.4**, **Fig. 5.5**. Then, we propose the application of the flow shown in **Fig. 5.6** by synthesizing all of the flows.

(A) **GPS unavailability**

This is exactly the situation where an attack is made on GPS, and either the location information from GPS can't be obtained, or the location information has been falsified and does not indicate the correct location.

(B) **Area of ocean you are navigating (Outer Sea or Coastal Waters)**

(1) **GPS attack in open sea** (open sea with no land in sight)

The attack from land is likely to be by radio waves with high output power. Attacks from the sea are likely to be made by ships and aircrafts sailing nearby. The attacked vessel will lose its position and only know its direction.

(2) **GPS attack in near-shore** (sea area near land, landmarks (lighthouses, etc.) visible)

Easy to execute attacks (low power is sufficient), regardless of whether they are at sea or on land. Tokyo Bay and other areas where vessels are crowded with ships. When an attack succeeds, the inside of the bridge is in chaos, and a delay in judgment can be fatal.

(C) **Weather Conditions**

Vessels using celestial navigation cannot see the sun or planets if the weather in the area they are navigating is anything other than "clear".

(D) **Visibility Conditions**

Due to dense fog, heavy rain, etc., it is impossible to see the situation at sea from the ship's bridge. Due to poor visibility, inertial navigation is applied to obtain

information on the vessel's position, which is calculated and deduced from the heading in which the vessel is traveling.

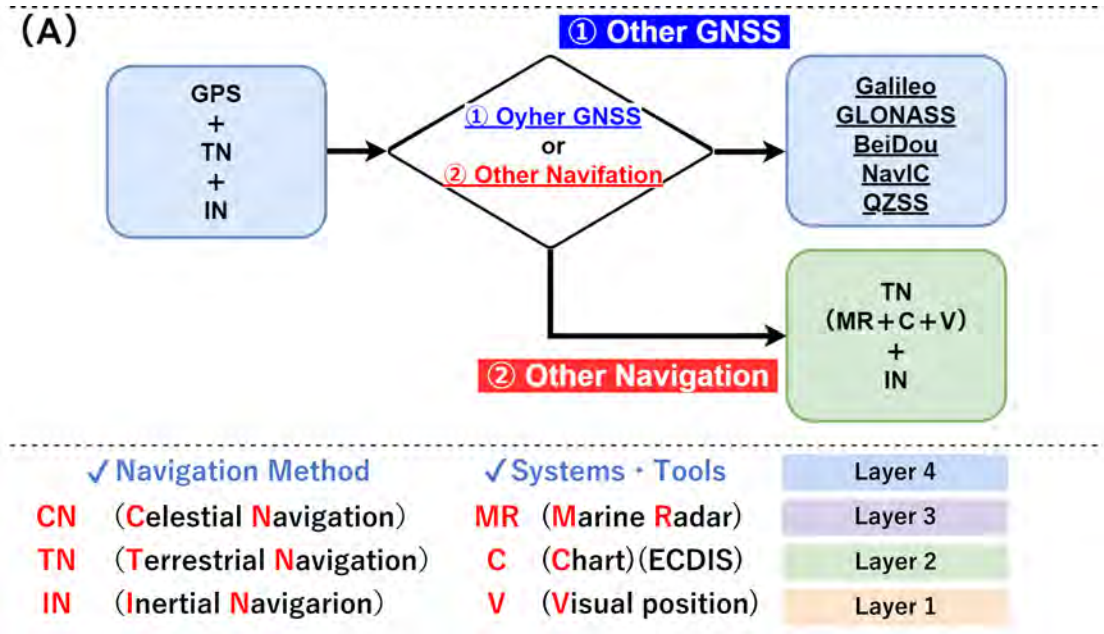


Fig. 5.2: (A) Flow of handling GPS jamming/spoofing (GPS unavailability)

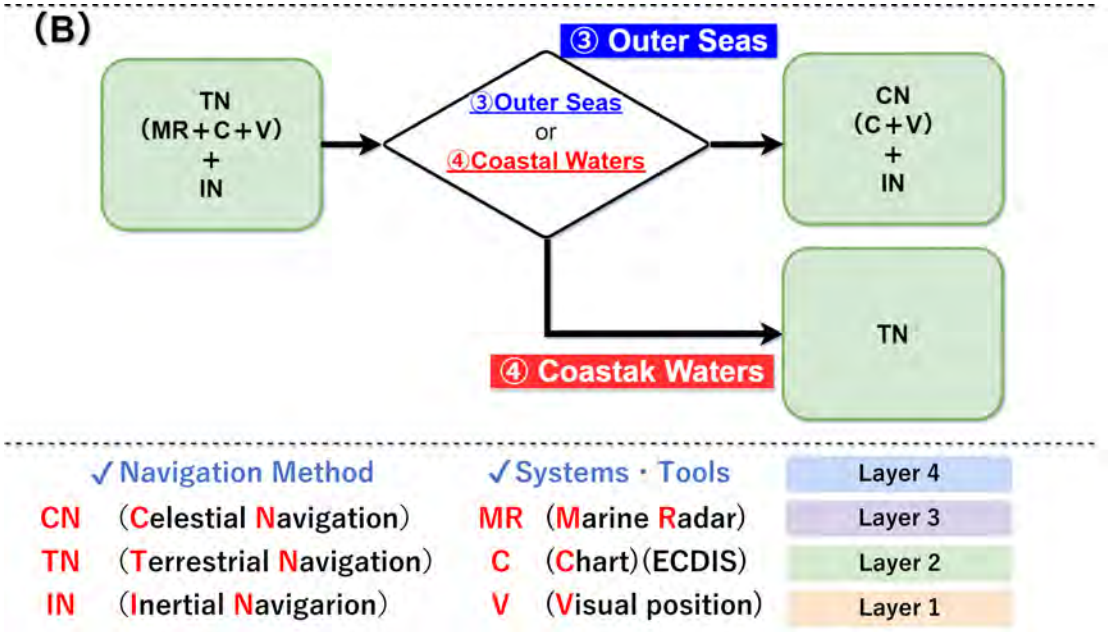


Fig. 5.3: (B) Flow of handling GPS jamming/spoofing (Area of ocean you are navigating)

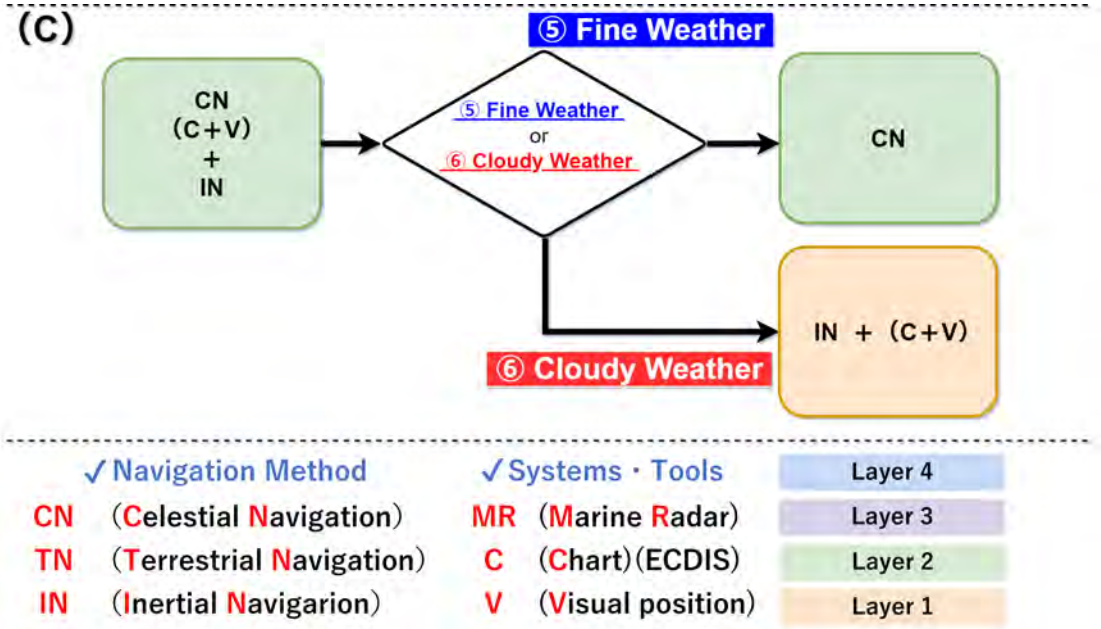


Fig. 5.4: (C) Flow of handling GPS jamming/spoofing (Weather Conditions)

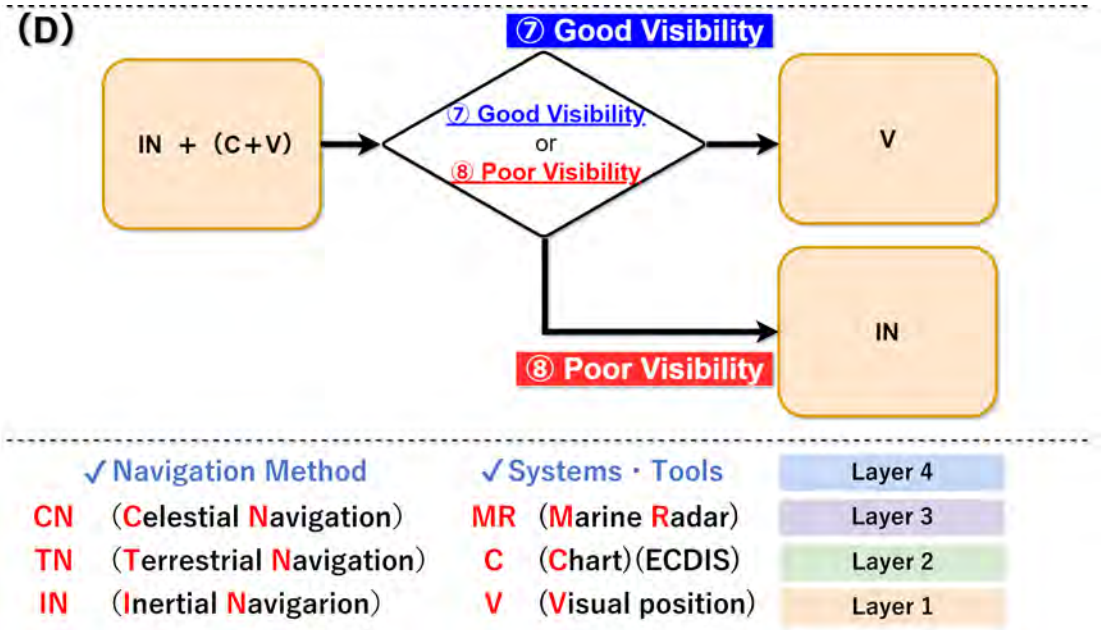


Fig. 5.5: (D) Flow of handling GPS jamming/spoofing (Visibility Conditions)

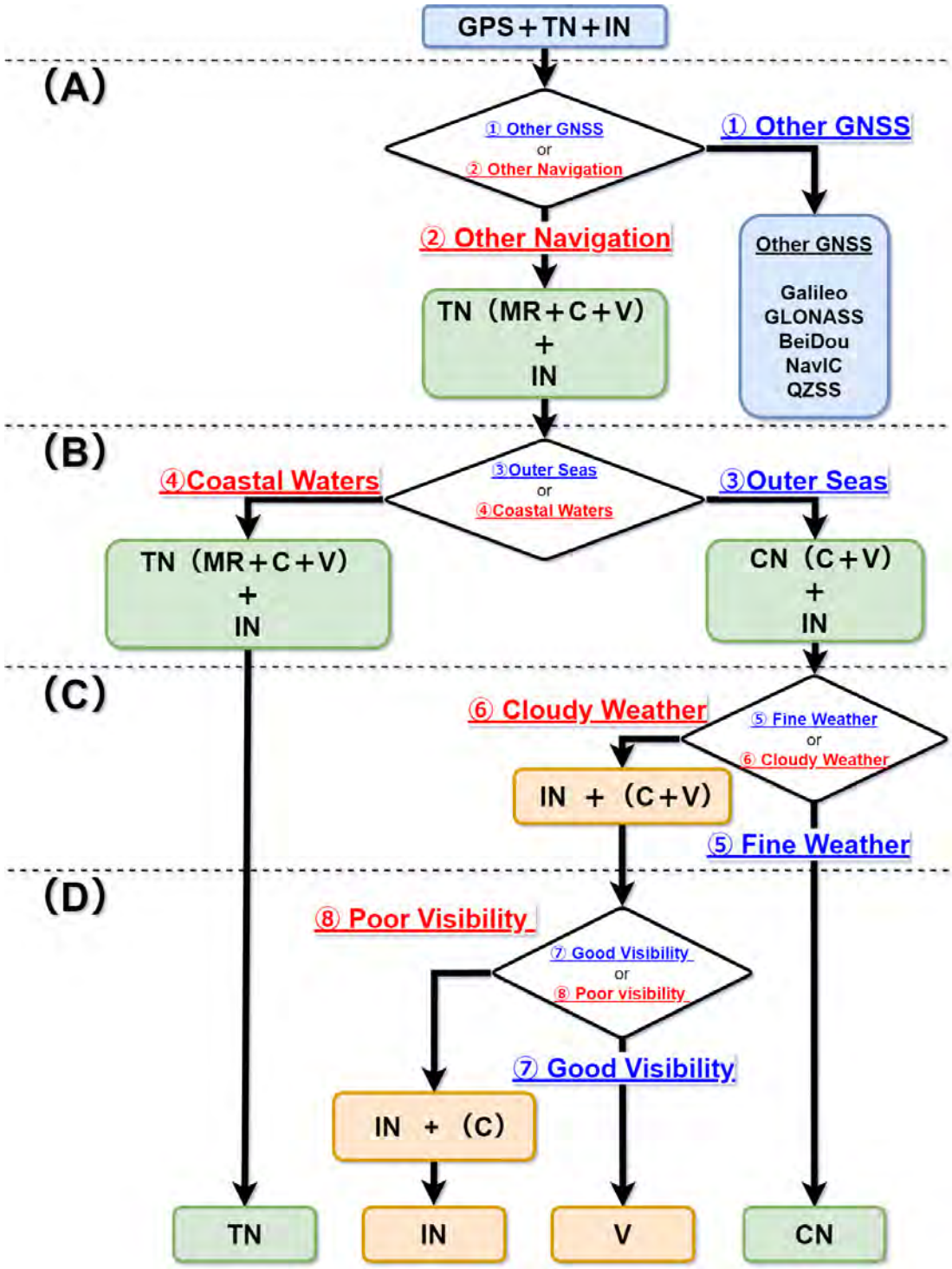


Fig. 5.6: Flow of actions to be taken by navigators in response to GPS jamming/spoofing

Chapter 6

Evaluation

We will conduct experiments and evaluate the similarity of the flowchart shown in **Fig. 5.6**, confirming the impact on ship operations and insecurity issues when assuming that a spoofing attack, which is considered to have the greatest impact on ships, occurs during navigation using GPS radio waves.

6.1 Attack Feasibility

There have not been many evaluations of the feasibility of realizing jamming, spoofing, and meaconing attacks in the field. Attacks on the most common types of receivers, such as cell phones and automobiles, are impractical due to the high degree of difficulty relative to the return of benefit to the attacker.

On the other hand, targets such as ships, airplanes, and power plants remain of higher value.

6.1.1 Execution cost and effort

The cost should be evaluated in terms of the practical costs associated with the simulation and the device according to the specifications of the GPS jammer and spoofer devices described in **Section 4.1**, which depend on the specifications of the GPS jammer and spoofer devices that will be used as attack tools and the type of attack targets to be constructed. Much of this is so far only theoretical. However, simple GPS jammer devices are available at low cost, in the order of tens of thousands of yen [48].

6.1.2 Required cost of simulator

Software to generate one or more GPS satellites is available from simulator manufacturers. There are two types: analog and digital [58]. Analog ones tend to be very expensive, up to $ 500,000, because they require a separate transmitter to represent each satellite

[58].

6.1.3 Required Cost of Meaconing

There are not too many references to building an instrument meaconner to realize meaconing. However, it is expected to be relatively easy to build a meaconar based on a software-defined radio (SDR), which sells for $ 2,300, and a wideband transceiver for an additional cost of $ 700. This could be combined with signals acquired from a GPS antenna and played back after a delay [52]. However, introducing variable delays for SCER (Security Code Estimation and Replay) and separating the various satellite signals would require software development, and the final cost would probably approach that of an inexpensive full simulator.

6.2 Experiment

6.2.1 Environmental for Experiment

Experiments were conducted to determine the impact of GPS spoofing on ship operations, to identify unsafe issues, and to clarify the similarity of the flowchart shown in **Fig. 5.6**. In this study, a simulation of GPS spoofing was conducted using a ship-handling simulator device with the cooperation of "National Institute of Technology, Hiroshima College" [*1], and a simulation was conducted by a navigator with experience in ship operation. As shown in **Fig. 6.1**, the simulation was conducted with two people on duty: the navigator on navigational duty and the helmsman who operates the steering system. This is a typical duty system under typical traffic conditions in a typical sea area.

In this study, we constructed a GPS-spoofed scenario and investigated the effects on the navigation system through the behavior of the navigators, the trajectory of the voyage, and a questionnaire survey. In conducting the experiment, the subjects and the questionnaire survey were conducted in accordance with the Ethics Code of the Japanese Psychological Association.

The composition of the experimental environment is shown in **Table. 6.1**, and the items of the questionnaire are shown in **Table. 6.2**.

[*1] National College of Technology in Osakikamijima-cho, Toyota-gun, Hiroshima, Japan. Department of Maritime Technology, Department of Electronic Control Engineering, Department of Distribution and Information Engineering, Department of Maritime Systems Engineering : https://www.hiroshima-cmt.ac.jp/

Fig. 6.1: Experiments (test subjects) in the shiphandling simulator (Experimenter (before) & helmsman (after))

Table. 6.1: Experiment Simulator Configuration

No.	Systems	Figure
1	Marine radar	**Fig. 6.2**
2	ECDIS	**Fig. 6.2**
3	Steering System	**Fig. 6.3**
4	VHF telephone system	**Fig. 6.4**

Table. 6.2: Questionnaire items for subjects

No.	Questions
Q1	Were you able to react to or identify a GPS spoofing attack?
Q2	When were you able to react or identify the GPS spoofing attack?
Q3	How did you feel when you were able to react to or identify a GPS spoofing attack?
Q4	Were you able to shift to GPS-independent navigation without hesitation?
Q5	What is the destination of the navigation system after GPS is disabled?
Q6	What is the destination of the navigation system after the GPS was disabled?
Q7	Other special notes (free text)

Fig. 6.2: Configuration of Shiphandling Simulator【Marine Radar (Left), ECDIS (Light)】

Fig. 6.3: Configuration of Shiphandling Simulator【Steering System】

Fig. 6.4: Configuration of Shiphandling Simulator【International VHF Radio Telephone System】

6.2.2 Experimental Scenario

The scenario is based on a comprehensive review of past incidents against ships [2], the cost, effort, and benefit of the attack, and the impact of the attack, and the likelihood of a direct attack on a ship is very low. Therefore, this experiment assumes a terrorist attack on a "military base" that exists to protect the lives and property of citizens, or an "airport" that may cause great damage to lives and the economy. Therefore, the area around "Port Island of Kobe" and "Kobe Airport" were chosen because the environment is very similar to past incidents against vessels. The Port of Kobe was selected as the experimental sea area.

- Physical security and "**Terrorist attacks**" on military installations, etc. (past case trends)
- Attacks on aircraft, drones, etc. (**high impact**)
- **Attacks on vessels are low**, but **secondary damage** is possible.

The time was set for a 12:00 start (daytime). The target vessel was a 1000 GT class general cargo ship. The experimental area is shown in **fig: 6.6**, where the antenna position that causes GPS spoofing is assumed to be located on the embankment of Port Island, and the spoofing range is defined as the yellow zone.

The target vessel is assumed to operate in the direction of 220 degrees from the starting point, then turn to 265 degrees, and continue straight for a while before terminating (**Fig. 6.6**). During this time, eight other vessels, including crossers, slow co-travellers, anti-travellers, and fishing boats, were assumed to be operating simultaneously in the traffic environment. **fig. 6.7** shows this situation. The simulator operator was assumed to be able to contact other vessels and the Vessel Traffic Advisory Service Center (VTASC)[*2] via "International VHF Telephone System", and to organize VHF contacts and traffic arrangements. The scenario was aborted in the case of failure to comply with the various laws and regulations.

GPS spoofing was designed to shift the GPS position by about 300 m in a 0 degrees (Northward) direction when the vessel entered the spoofing range, and to restore the GPS position when the vessel left the range (First spoofing). The ship's position was then shifted significantly by about 30,000 m in a 45 degree (Eastward) direction near the end point (Second spoofing). GPS spoofing affects the AIS data superimposed on the Marine

[*2] Established by the Japan Coast Guard at seven locations in Japan. It provides information necessary for the safe operation of vessels and performs centralized navigation control in the shipping lanes and congested waters designated by the Maritime Traffic Safety Law and the Port Regulations Law. https://www.kaiho.mlit.go.jp/soshiki/koutsuu/toudai/center.html

radar.

For this scenario, it is recommended to navigate above the line between "Kobe Oki No.1 Light Buoy" and "Kobe Oki No.2 Light Buoy" (this light buoy is designed to rectify vessel traffic flow), and the 300 m northward deviation would cause the vessel to navigate more to the south than expected if it were to navigate while observing this line, resulting in an unsafe position. This would result in an unsafe position, which could easily lead to a head-on collision. Therefore, as a criterion for evaluation in this simulation, we judged whether the ship's trajectory was above the line between "Kobe Oki No.1 Light Buoy" and "Kobe Oki No.2 Light Buoy".

The subjects of the experiment were mariners with a third-class maritime engineer's license (navigation) or higher and at least one year of experience on board a 1,000 GT-class ship. The classification was based on whether they had "experience in voyaging to the experimental area" or "experience on operational vessels," as shown in **Table. 6.3**. All ship operators are Japanese maritime engineers who were educated in Japan.

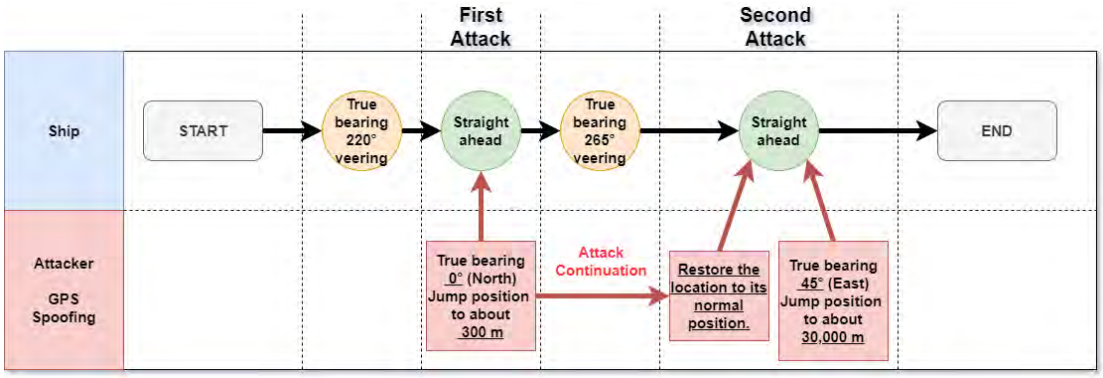


Fig. 6.5: Experiment Flow

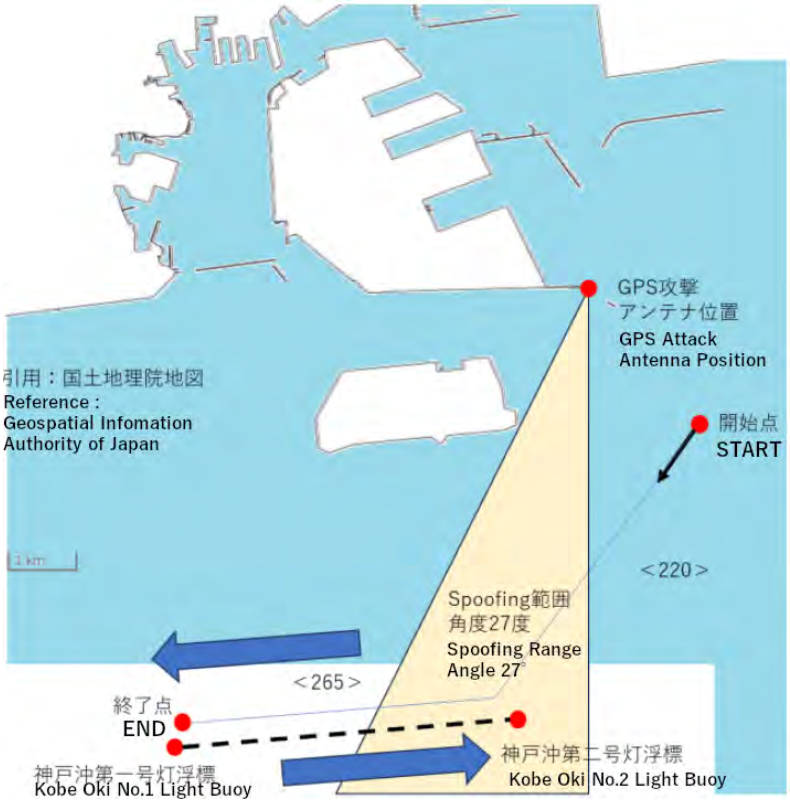


Fig. 6.6: Sea area of experiment

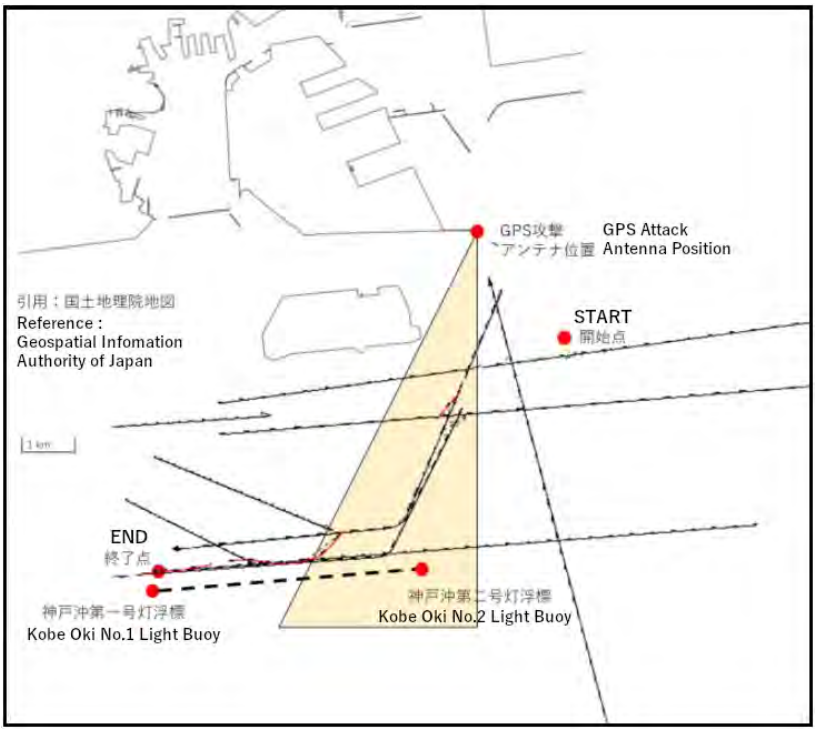


Fig. 6.7: Navigational status of other vessels

Table. 6.3: Subject's background and other information

Test subject	Experience in voyaging to the experimental area	Experience in operating vessels
A	Yes	More than 5 years
B	Yes	More than 5 years
B	Yes	More than 5 years
C	No	More than 5 years
D	Yes	More than 1 year Less than 5 years
E	No	More than 1 year Less than 5 years
F	No	Less than 1 year
G	No	Less than 1 year

By the way, if there is an error in the GPS data format entering the navigation system, the system itself such as AIS, ship radar, ECDIS, etc. will output an error alarm indicating the GPS data error because normal GPS data is not input to the system. If the alarm is for only one system, it is expected that only the system for which the alarm was issued will fail. In other words, in the case of a GPS jamming attack, all systems will simultaneously output error alerts because they cannot receive normal GPS data.

On the other hand, in the case of a GPS spoofing attack, no error alarm is output from the input navigational system because there is no abnormality in the GPS data format since it is a falsification of location information. Therefore, a GPS spoofing attack causes a discrepancy between the ship's own ship and radar image displayed in ECDIS and the electronic nautical chart (ENC), as shown in **Fig. 6.8**, without an error alarm being output. This is the first indication that the ship's navigator is aware of a possible GPS spoofing attack.

Fig. 6.8: GPS spoofing

6.3 Experimental Results and Discussion

6.3.1 Vessel Trajectory Results

Fig. 6.9 shows the results of the ship's trajectory using the ship-handling simulator. **Fig. 6.9** shows that all seven subjects were able to navigate above the line between "Kobe Oki No.1 Light Buoy" and "Kobe Oki No.2 Light Buoy". Therefore, it is clear that they were navigating safely, and the proposed response chart is presumed to be similar. However, in two cases, the ship terminated without any significant change in the situation before the end point, resulting in a northward-flowing wake.

6.3.2 Questionnaire Survey Results

Next, the questionnaire shown in **Table. 6.2** was administered to seven subjects after the test. The results of the questionnaire are shown in **Table. 6.4**. According to **Table. 6.2**, six subjects responded that they were able to react and grasp the GPS spoofing attack, and one subject responded that he was unaware of the GPS spoofing attack. However, this result indicates that none of the subjects noticed that they had been spoofed after the first GPS spoofing attack, which shifted the GPS spoofing 300 m to the north, and that they only became aware of the spoofing after the second attack. The subjects were able to notice the spoofing by checking the ECDIS and the ship's radar behavior after the vessel changed course.

The following two points can be inferred from the ship's wake results and the questionnaire results.

1. GPS spoofing attacks, which provide fine-grained changes, are less likely to affect experienced coastal navigators.
2. Navigators who tend to check ECDIS preferentially are more susceptible to GPS spoofing attacks.

First, it can be inferred that an attack by a slight position change of about 300 m in GPS spoofing may have little impact. This is because navigators who mainly have experience in coastal navigation mainly use geographic navigation (navigation using chart cross bearings) and radar navigation (navigation using shipboard radar) and do not pay attention to the GPS position on ECDIS (electronic charts). Therefore, this influence is considered to be small. However, depending on the opposite viewpoint, it is highly likely that they have already moved to **"Layer 1"** and **"Layer 2"** in the proposed response chart (**Fig. 5.6**), and the proposed response chart can be implemented without any discomfort as the behavior of navigators who usually navigate in Japan, especially those

who are engaged in coastal navigation. It is assumed that the proposed response chart can be implemented without any discomfort as the behavior of navigators who navigate in Japan, especially in coastal navigation. It is also assumed that in waters where there is a lot of traffic flow, it is necessary to visually assess the sighting relationship of vessels, and that the tendency to emphasize sighting was observed because safe navigation is not possible without cross bearings using surrounding scenery and nautical charts.

On the other hand, there was one case in which a subject who was navigating while keeping an eye on ECDIS made a mistake in recognizing his own position during GPS spoofing, resulting in a significant deviation from the planned navigation route and a panicked response later. This was presumably caused by the fact that the subjects tended to trust ECDI, which can grasp a large amount of information, and to check it preferentially, unlike navigators who mainly have experience in coastal navigation, who tend to emphasize the aforementioned visual observation in vessel operation.

In the second GPS spoofing attack, which caused a large GPS displacement of 30,000 m to the east, some mariners noticed the anomaly and responded to it by checking the instruction manuals and other documents. In addition, there were cases where navigators reported "navigation system anomalies" to the Maritime Traffic Center using an international VHF telephone system before entering waters covered by the Maritime Traffic Safety Act, i.e., waters that require the use of an appropriate navigation system. This action has precedents in past related studies, and it is assumed that it may be customary to do so [4][49]. In addition to the Maritime Traffic Center, the international VHF telephone system may be used as a means of confirmation with other vessels, and such communications for fact-finding and reporting are likely to increase in areas where many vessels are navigating. As a result, the radio frequencies for distress and emergency communications may be blocked, resulting in a temporary loss of communication between vessels and between vessels and land. Because of this potential secondary damage, it is assumed that maritime traffic centers need to be aware of this possibility.

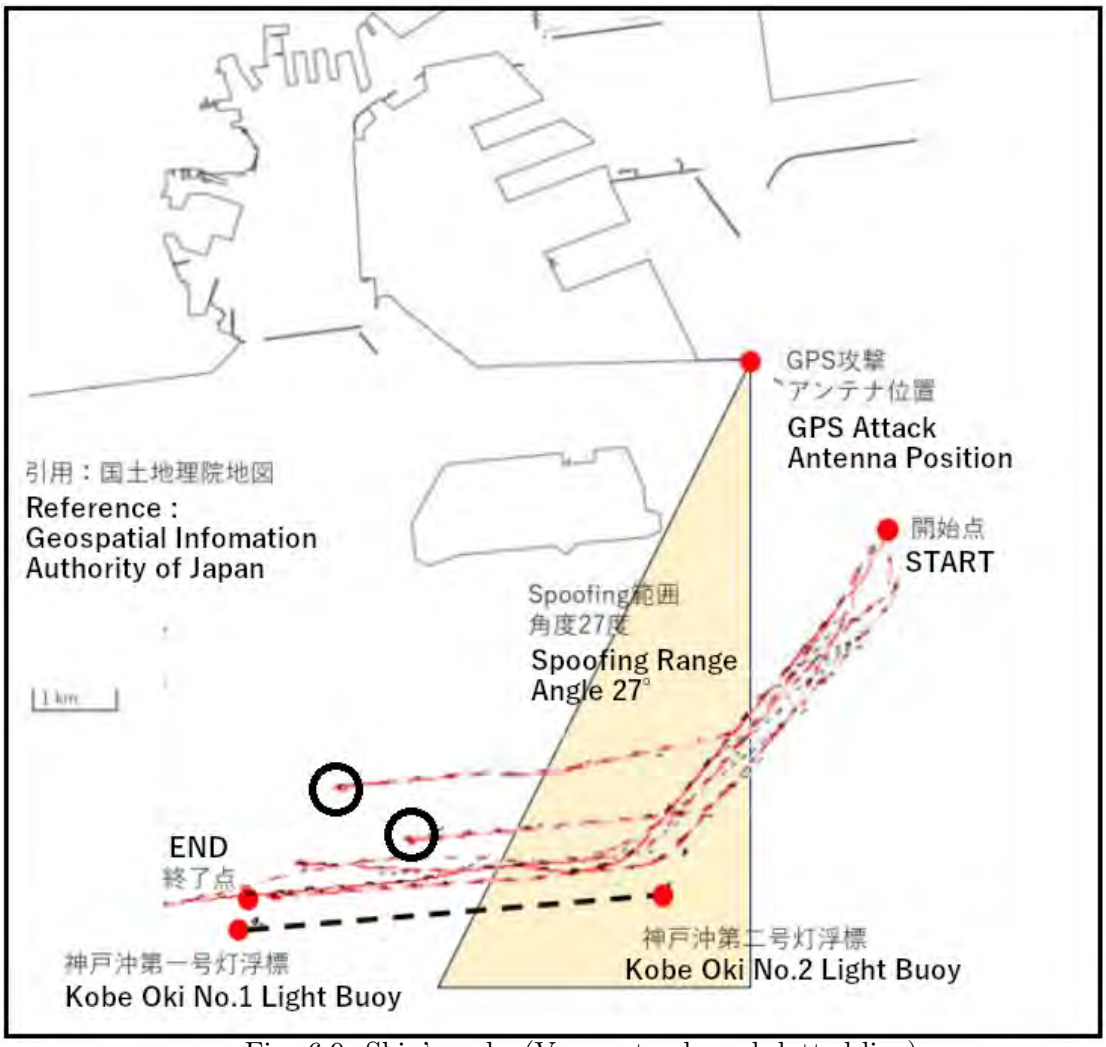


Fig. 6.9: Ship's wake (Voyage track: red dotted line)

Table. 6.4: Results of post-experiment questionnaire to subjects

No.	Questions	Summary	Results
Q1.	Were you able to react to or grasp the spoofing attack?	Reaction or understanding was possible.	6
		Response or could not be ascertained.	1
Q2.	When were you able to react or grasp the spoofing attack?	I knew when I was blown wide open (the second spoof), but I had no idea about the exquisite spoof (the first spoof). I understood that my ship had disappeared, but I did not think it was an attack. I felt that the ship radar was behaving strangely. I didn't see anything special about Marine Radar or ECDIS. After changing the needle position, the ship's position was determined when the ship checked the ECDIS screen to determine its position.	
Q3.	How you feel when you are able to react to or grasp a GPS spoofing attack.	I felt fear.	0
		I felt impatience.	3
		I didn't feel anything.	2
		Other	2
Q4.	Have you been able to transition to GPS-independent operations without hesitation?	Migrated.	5
		Could not migrate.	2
Q5.	What is the transition destination for the navigation system after GPS unavailability?	Other GNSS	0
		Radio Navigation	0
		Terrestrial Navigation	2
		Celestial Navigation	0
		Inertial Navigation	0
		Visual Navigation	4
		Other Method	1

Table. 6.4: Results of post-experiment questionnaire to subjects

No.	Questions	Summary	Results
Q6.	What is the transition destination for the navigation system after GPS unavailability? (Answer any other voyage systems used other than those in Q5.)	Other GNSS	0
		Radio Navigation	0
		Terrestrial Navigation	2
		Celestial Navigation	0
		Inertial Navigation	0
		Visual Navigation	4
		Other Method	1
Q7.	Other special remarks	I noticed a problem with the ECDIS and ship radar, but did not think to take any particular action because Kobe was a familiar place to me. The Akashi Kaikyo Channel is a difficult route, so our first priority was to keep the ship safe. If I had had the manpower, I would have solved the problems that occurred in ECDIS. Usually, I navigate by comparing what I see with my own eyes and the bearing to the charts. Before entering the Akashi Strait, ECDIS and ship's radar malfunctioned, so we were not sure whether we could continue to sail, so we contacted the Osaka Bay Marine Traffic Center via VHF for confirmation. The vessel radar and ECDIS were reactivated. In order to find the cause of the error, we searched for the operation manuals of the Marine Radar and ECDIS on the bridge. If the error was not resolved after reading the manual, you called the manufacturer to solve the problem.	

Table. 6.4: Results of post-experiment questionnaire to subjects

No.	Questions	Summary	Results
Q7.	Other special remarks	I did not feel much of a sense of urgency because I frequently changed course settings based on the movements of surrounding vessels rather than being aware of course lines. In this case, we did not pay much attention to the ship's position because we had checked the charts before the experiment to make sure that there were no obstacles or obstacles in the water.	

Chapter 7

Summary and Future Issues

This study proposes a response chart for the effect of GPS spoofing on the navigation system and the response after GPS spoofing, which are the most threatening factors in the operation using electronic chart display systems (ECDIS/ECS). The purpose of this study was to clarify the similarity of the response chart and the response after GPS spoofing through an experiment using a navigation simulation for Japanese mariners educated in Japan.

The following findings were obtained from the results of this study.

- Japanese mariners with insufficient knowledge of the threat of cyber-attacks were able to shift to GPS-independent operations without hesitation and to continue safe operations, even though they were unable to respond to or understand GPS spoofing.
- On the other hand, Japanese mariners who were not able to grasp the response chart and were dependent on ECDIS were found to be unable to grasp the situation and conducted unsafe operations.
- In the case of damage caused by GPS spoofing, the affected vessels may increase the communication between the vessel and the marine traffic center using "International VHF Telephone System", as well as between the vessel and the land.

These results confirm the similarity of the response chart shown in **Fig. 5.6**. The response chart is considered to be an important measure required of navigators for the operation of vessels that will be increasingly automated in the future.

On the other hand, future issues in this study are mainly as follows.

- Handling of operators with little experience in navigating in near-shore waters
- Time required to shift navigation timing
- Incident response in case of anomalies in other sensors
- Security measures for other GNSS

The subjects of the experiment in this study are Japanese maritime engineers with varying levels of experience navigating and operating vessels in the experimental area, so the rules of the route and the sea area to be trained are mainly the waters surrounding the Japanese archipelago. On the other hand, if foreign mariners with little experience navigating in Japan's neighboring waters were subjected to this experiment, it is highly likely that they would not be able to understand the situation as well as mariners who relied on ECDIS, and thus would be more likely to operate unsafely.

Since the experiment in this study was conducted to verify the similarity of mariners' behavior to the proposed response chart and GPS spoofing, the exact behavior of the mariners was not verified. Therefore, we believe that by verifying the timing (time) of the navigation transition, the time required, etc., it may be possible to derive detailed countermeasures when subjected to radio interference, including jamming.

If a cyber-attack occurs that disables shipboard radar, which is a tool for applying geo navigation, and gyro-compass, which is necessary for applying inertial navigation, as an indication that the subject has detected GPS spoofing, it is highly likely that the existing system alone will not be sufficient to ensure safety. Therefore, it is necessary to consider incident response in the event of an anomaly in sensors other than GPS.

As a future development of GNSS, the "QZSS Signal Authentication Service" [40]," which is scheduled to be provided from FY2024, will enable confirmation that signals received by GNSS receivers are true signals transmitted from positioning satellites, and thus it is expected that measures will be taken to prevent GPS spoofing in the Asia-Oceania region only. This research is expected to be able to take countermeasures against GPS spoofing in Asia and Oceania. Since this study mainly focused on GPS, it is necessary to consider further assumptions including GNSS including QZSS in the future.

In addition to the navigation methods discussed in this study, there is a new navigation system, quantum navigation, which uses a quantum compass. Quantum compass is said to be able to measure position without the use of GPS, combining the accuracy of quantum technology with measurement technology such as gyrocompass, which provides conventional "self-position estimation [59]. Quantum navigation has been successfully tested and implemented by the Royal Navy, which was the first in the world to install a quantum navigation system on a submarine [60]. This success is attracting worldwide attention as it represents an important step forward in naval technology and will have a positive impact on improving the navigability and operational efficiency of ships in a variety of maritime scenarios.

Acknowledgment

I would like to express my deepest gratitude to Professor Suzaki of the Graduate School of Information Security for his great guidance throughout this research as my supervisor. I am grateful to Professor Doi and Professor Fujimoto of the Graduate School of Information Security for their advice and support as sub-reviewers in the preparation of this paper. We also thank Associate Professor Kishi, and Mis. Sakamoto, Mis. Nomoto of National Institute of Technology, Hiroshima College, and Mr. Hasegawa of LAC Co., Ltd. for their great advice, experiments, and evaluations in conducting this research. Finally, we thank Prof. Matsui., a visiting professor of the Graduate School of Information Security, for his great advice and cooperation in the execution of this research. We would like to express our gratitude to him.

References

[1] NSM. 「risiko 2020」. https://nsm.no/getfile.php/131421-1587034764/NSM/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf, 2020. (visited on Jan. 16, 2024).

[2] Per Håkon Meland, Karin Bernsmed, Egil Wille, Ørnulf Jan Rødseth, and Dag Atle Nesheim. A retrospective analysis of maritime cyber security incidents. 2021.

[3] Anja Menzel and Lisa Otto. Connecting the dots: Implications of the intertwined global challenges to maritime security. *Global Challenges in Maritime Security: An Introduction*, pp. 229–243, 2020.

[4] Above Us Only Stars. Exposing GPS Spoofing in Russia and Syria. https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf, 2019. (visited on Jan. 16, 2024).

[5] Robert Lemos. Coast guard warns shipping firms of maritime cyberattacks, 2019. (visited on Jan. 16, 2024).

[6] Eric Tegle (Forbes JAPAN). 欧州で GPS 妨害が多発，航空機の運航に影響 発信源はロシアか. https://forbesjapan.com/articles/detail/68978, 2024.2.6. (visited on Jan. 16, 2024).

[7] IMO. SOLAS—Consolidated Edition 2020. *London, UK*, 2020.

[8] IMO MSC. 1/Circ. 1595 e-Navigation Strategy Implementation Plan—Update 1. *London, UK*, 2018.

[9] GPS: The Global Positioning System A global public service brought to you by the U.S. government. https://www.gps.gov/. (visited on Jan. 16, 2024).

[10] 海上保安庁, ディファレンシャル GPS の廃止について. https://www.kaiho.mlit.go.jp/10kanku/miyazaki/uminoanzen/kourohyoushiki/deta/dgpsnohaisi190301.pdf, 2019. (visited on Jan. 16, 2024).

[11] IMO MSC. Resolution MSC.428(98) Maritime cyber risk management in Safety Management Systems. *London, UK*, 2017.

[12] IACS. UR E26 "Cyber Resilience of Ships." IACS, 2022.

[13] IACS. UR E27 "Cyber Resilience of On-board Systems and Equipment." IACS, 2022.

[14] Saneyuki Senda and Kuniyasu Suzaki. Attack and Countermeasure for GPS-based

Ship Navigation Systems. *Computer Security Symposium 2023 Collected Papers*, pp. 1293–1300, 2023.

[15] Ayano Sakamoto, Rino Nomoto, Saneyuki Senda, TakumaTakuma Kishi, Kuniyasu Suzaki, and Choichi Hasegawa. Basic study on the effect s of ship GPS Spoofing on navigation systems. *Symposium on Cryptography and Information Security 2024 Collected Papers*, 2024.

[16] 近藤信竹. AIS (自動識別通報装置). Techno marine 日本造船学会誌, Vol. 851, pp. 297–301, 2000.

[17] Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit. A security evaluation of ais automated identification system. In *Proceedings of the 30th annual computer security applications conference*, pp. 436–445, 2014.

[18] Enricad' Afflisio, Paolo Braca, Peter Willett. Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection. *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 57, No. 4, pp. 2093–2108, 2021.

[19] Wu, Jianjun and Thorne-Large, James and Zhang, Pengfei. Safety first: The risk of over-reliance on technology in navigation. *Journal of Transportation Safety & Security*, Vol. 14, No. 7, pp. 1220–1246, 2022.

[20] Alan G Bole, Alan D Wall, and Andy Norris. *Radar and ARPA manual: radar, AI and target tracking for marine radar users*. Butterworth-Heinemann, 2013.

[21] International Electrotechnical Commission, et al. Maritime navigation and redio-communication equipment and systems, track control systems, operational and performance requirements, methods of testing and required test results. *IEC62065*, pp. 64–72, 2002.

[22] Adam Weintrit. *The electronic chart display and information system (ECDIS): an operational handbook*. CRC Press, 2009.

[23] Boris Svilicic, David Brčić, S Žuškin, and D Kalebić. Raising awareness on cyber security of ECDIS. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 13, No. 1, pp. 231–236, 2019.

[24] Mass Soldal Lund, Odd Sveinung Hareide, and Øyvind Jøsok. An attack on an integrated navigation system. 2018.

[25] 松本吉春. 精説地文航法. 成山堂書店, 1997.

[26] 廣野康平. 天文航法の ABC: 天測の基本から観測・計算・測位の実際まで. 成山堂書店, 2020.

[27] 海上保安庁. 「天測暦」等の廃刊について. `https://www1.kaiho.mlit.go.jp/KOHO/announce.html`. (visited on Jan. 16, 2024).

[28] Greg Tozzi. Toward Automated Celestial Navigation with Deep Learning. `https://github.com/gregtozzi/deep_learning_celnav`, 2020. (visited on Jan. 16, 2024).

[29] United States. Coast Guard. *Loran-C User Handbook*. Department of Transportation, Coast Guard, 1974.

[30] Walter Blanchard. The genesis of the Decca Navigator system. *The Journal of Navigation*, Vol. 68, No. 2, pp. 219–237, 2015.

[31] J Kasper and C Hutchinson. The Omega navigation system–An overview. *IEEE Communications Society Magazine*, Vol. 16, No. 3, pp. 23–35, 1978.

[32] 海上保安庁. 「慶佐次ロランC局の廃止について」. https://www.kaiho.mlit.go.jp/info/kouhou/h26/k20140801/k140801-1.pdf. (visited on Jan. 16, 2024).

[33] Di Qiu, Dan Boneh, Sherman Lo, and Per Enge. Reliable location-based services from radio navigation systems. *Sensors*, Vol. 10, No. 12, pp. 11369–11389, 2010.

[34] 海上保安庁. 「ロランC」. https://www.kaiho.mlit.go.jp/syoukai/soshiki/toudai/lolanc/index.htm, 2014. (visited on Jan. 16, 2024).

[35] European GNSS Service Centre. What is Galileo. https://www.gsc-europa.eu/galileo/what-is-galileo. (visited on Jan. 16, 2024).

[36] GLONASS. https://glonass-iac.ru/. (visited on Jan. 16, 2024).

[37] Beidou. http://www.beidou.gov.cn/. (visited on Jan. 16, 2024).

[38] NavIC. https://glonass-iac.ru/. (visited on Jan. 16, 2024).

[39] 内閣府宇宙開発戦略推進事務局. みちびきウェブサイト. https://qzss.go.jp/. (visited on Jan. 16, 2024).

[40] 内閣府宇宙開発戦略推進事務局.「信号認証サービス」(みちびきウェブサイト). https://qzss.go.jp/overview/services/sv14_sas.html, 2023. (visited on Jan. 16, 2024).

[41] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pp. 75–86, 2011.

[42] Alan Bensky. *Wireless positioning technologies and applications*. Artech House, 2016.

[43] GPS.gov. GPS Standard Positioning Service (SPS) Performance Standard. https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf, 2020. (visited on Jan. 16, 2024).

[44] Jon S Warner and Roger G Johnston. GPS spoofing countermeasures. *Homeland Security Journal*, Vol. 25, No. 2, pp. 19–27, 2003.

[45] Stefan Erker, Steffen Thölert, Johann Furthner, and Michael Meurer. L5–the new gps signal. *Proceedings of IAIN*, pp. 27–30, 2009.

[46] Brian C Barker, John W Betz, John E Clark, Jeffrey T Correia, James T Gillis, Steven Lazar, Kaysi A Rehborn, and John R Straton. Overview of the GPS M code signal. In *Proceedings of the 2000 National Technical Meeting of the Institute of Navigation*, pp. 542–549, 2000.

[47] Elliott D Kaplan and Christopher Hegarty. *Understanding GPS/GNSS: principles and applications*. Artech house, 2017.

[48] Takeyasu Sakai. Security of GPS: Vulnerability and Countermeasures. *IEICE Technical Report*, Vol. 118, No. 193, pp. 1–6, 2018.

[49] Alan Grant, Paul Williams, Nick Ward, and Sally Basker. GPS jamming and the impact on maritime navigation. *The Journal of Navigation*, Vol. 62, No. 2, pp. 173–187, 2009.

[50] Daniel Medina, Christoph Lass, Emilio Pérez Marcos, Ralf Ziebold, Pau Closas, and Jesús García. On GNSS jamming threat from the maritime navigation perspective. In *2019 22th International Conference on Information Fusion (FUSION)*, pp. 1–7. IEEE, 2019.

[51] Dana, Goward. Mass GPS Spoofing Attack in Black Sea. `https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea`, 2021. (visited on Jan. 16, 2024).

[52] Mark L Psiaki and Todd E Humphreys. Gnss spoofing and detection. *Proceedings of the IEEE*, Vol. 104, No. 6, pp. 1258–1270, 2016.

[53] Dennis M Akos. Who's afraid of the spoofer? gps/gnss spoofing detection via automatic gain control (agc). *NAVIGATION: Journal of the Institute of Navigation*, Vol. 59, No. 4, pp. 281–290, 2012.

[54] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. Predespreading authenticity verification for gps l1 c/a signals. *NAVIGATION: Journal of the Institute of Navigation*, Vol. 61, No. 1, pp. 1–11, 2014.

[55] Esteban Garbin Manfredini, Beatrice Motella, and Fabio Dovis. Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests. In *Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, pp. 3100–3106, 2015.

[56] Andriy Konovaltsev, Manuel Cuntz, Christian Haettich, and Michael Meurer. Autonomous spoofing detection and mitigation in a gnss receiver with an adaptive antenna array. In *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, pp. 2937–2948, 2013.

[57] 岸拓真, 濵崎淳, 清田耕司, 坂本彩乃. 船舶における OT 機器を伴うサイバーインシデントへのレスポンスに関する教育プログラムの開発. 第 149 回講演会日本航海学会講演予稿集 11 巻 2 号, pp. 43–46, 2023.10.

[58] IIvan Petrovski and Takuji Ebinuma. Everything you always wanted to know about GNSS simulators but were afraid to ask. *Inside GNSS September (2010)*, pp. 48–58, 2010.

[59] Imperial College London. Imperial News「Quantum 'compass' could allow navigation without relying on satellites」. `https://www.imperial.ac.uk/news/188973/`

quantum-compass-could-allow-navigation-without/, 2018. (visited on Jan. 16, 2024).

[60] Imperial College London. Imperial News「Quantum sensor for a future navigation system tested aboard Royal Navy ship」. https://www.imperial.ac.uk/news/245114/quantum-sensor-future-navigation-system-tested/, 2023. (visited on Jan. 16, 2024).