Оригинальная статья / Original Paper

DOI 10.15826/urej.2020.4.2.002 **УДК** 528.13

Brief Analysis of GNSS and LNSS Vulnerabilities with the Focus on Spoofing for the Marine Autonomous Surface and Undersea Vehicles

E. Ochin
Maritime University of Szczecin, Faculty of Navigation,
1-2 Wały Chrobrego Str., Szczecin, 70-500, Poland
✉ E.Ochin@AM.Szczecin.pl

Abstract

Positioning and navigation problems have proven to be well-developed in all areas of the Earth (on the surface of the lithosphere and hydrosphere, in the atmosphere, troposphere and stratosphere), except the hydrosphere. This article is devoted to the problem of a analysis of the state of the underwater positioning and navigation and practically the undeveloped problem of the underwater navigation safety. Here we restrict ourselves to analyzing the possibility of transferring the well-established GNSS technology to the underwater world. Unfortunately, GNSS signals attenuate very quickly in water, thus all GNSS-like technologies are of the local nature, based on the transformation of the electromagnetic wave of GNSS signals into an acoustic wave. Therefore, we use the term LNSS (Local Navigation Satellite Systems) to refer to this underwater technology.

Keywords

GNSS, LNSS, Local Navigation Satellite Systems, Undersea LNSS, Jamming, Meaconing, Spoofing, Self-Spoofing, Spoofing Detection

For citation

Ochin E. Brief Analysis of GNSS and LNSS Vulnerabilities with the Focus on Spoofing for the Marine Autonomous Surface and Undersea Vehicles. *Ural Radio Engineering Journal*. 2020;4(2):167–187. DOI: 10.15826/urej.2020.4.2.002.

Краткий анализ уязвимостей GNSS и LNSS с акцентом на спуфинг морских надводных и подводных автономных аппаратов

Е. Ф. Очин
Щецинский морской университет,
Республика Польша, 70-500, г. Щецин, ул. Валы Хробрего, 1-2
✉ E.Ochin@AM.Szczecin.pl

Аннотация

Проблемы позиционирования и навигации хорошо зарекомендовали себя во всех областях Земли (на поверхности литосферы и гидросферы, в атмосфере, тропосфере и стратосфере), за исключением гидросферы. Данная статья посвящена проблеме анализа состояния подводного позиционирования и навигации и практически неразвитой проблемы безопасности подводного плавания. Здесь мы ограничиваемся анализом возможности передачи устоявшейся технологии GNSS в подводный мир. К сожалению, сигналы GNSS очень быстро затухают в воде, поэтому все технологии, подобные GNSS, носят локальный характер и основаны на преобразовании электромагнитной волны сигналов GNSS в акустическую волну. Поэтому мы используем термин LNSS (Локальные навигационные спутниковые системы) для обозначения этой подводной технологии.

Ключевые слова

ГНСС, ЛНСС, локальные навигационные спутниковые системы, подводная ЛНСС, джамминг, меконинг, спуфинг, самоспуфинг, обнаружение спуфинга

Для цитирования

Очин Е. Ф. Краткий анализ уязвимостей GNSS и LNSS с акцентом на спуфинг морских надводных и подводных автономных аппаратов. *Ural Radio Engineering Journal*. 2020;4(2):167–187. (На англ. яз.) DOI: 10.15826/urej.2020.4.2.002.

1. Introduction

GNSS [1–7] is the common name for the four Global Navigation Satellite Systems GPS (USA), GLONASS (USSR, RF), BeyDou-2 (PRC), GALILEO (EU), the main purpose of which is the ground and air positioning, navigation and timing on land, in the sea and underwater of mobile vehicles at anytime, anywhere in the world.

RNSS is the common name for two Regional Navigation Satellite Systems

- **NavIC** (**NAV**igation with **I**ndian **C**onstellation), Government of India,
- **QZSS** (**Q**uasi-**Z**enith **S**atellite **S**ystem), Government of Japan, whose main purpose is the same as the GNSS goal.

Until 2016, NavIC was called **IRNSS** – **I**ndian **R**egional **N**avigation **S**atellite **S**ystem. NavIC is an autonomous system designed to cover the Indian region and 1500 km around the Indian mainland. The system consists of 7 satellites.

QZSS operated by QZS System Service Inc. QZSS complements GPS to improve coverage in the East Asia and Oceania. The system consists of 4 satellites and will be expanded up to 7 ones for autonomous capability by 2023.

GNSS pinpoint latitude, longitude and altitude to about a meter of accuracy and provide nanosecond precise time anywhere on the Earth.

GNSS is a dual-use system: a standard civil location service (SPS) and a military precise positioning service (PPS). The access to PPS is controlled using cryptography and other information security methods. Since the material in this article is designated for the civil community, we will only consider SPS and when considering GNSS goals, we will mainly focus on GNSS positioning as the main goal of GNSS, without which it's pointless to discuss the GNSS navigation and timing.

GNSSs are composed of three different complementary segments, as shown in Fig. 1:

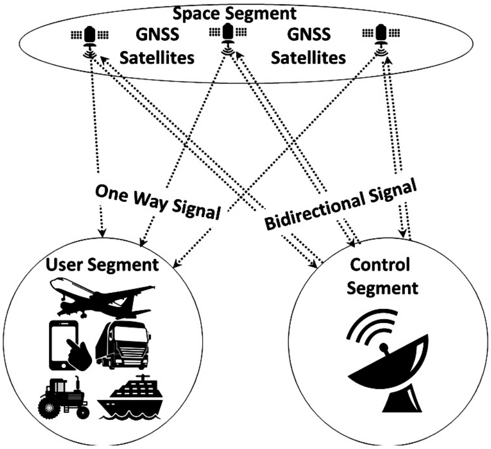


Fig. 1. GNSS consists of three segments: the Space Segment, the Control (or Ground) Segment, and the User Segment

Рис. 1. GNSS состоит из трех сегментов: космический сегмент, управляющий сегмент и пользовательский сегмент

The Space Segment, consisting of navigation satellites, is a combination of sources of radio navigation signals that simultaneously transmit a significant amount of overhead information. The main functions of each satellite are the generation and emission of radio signals necessary for navigational determinations of consumers and the control of onboard satellite systems.

The Control Segment tracks and maintains the satellites in space. The control segment monitors the satellite health and it maintains the satellite orbits as desired. Furthermore, the control segment updates the satellite clock corrections and ephemerides, among other parameters, encapsulated in the navigation message. The control segment includes a cosmodrome, a command and measurement complex and a control center. The spaceport provides the launch of satellites into the required orbits during the initial deployment of the navigation system, as well as the periodic replenishment of satellites as they fail or resource exhaustion.

The User Segment combines all user installations and their supporting equipment. A custom installation typically consists of an antenna, a GNSS receiver, a processor, a computer, and I/O devices. the field of view, measures the propagation time of these signals and Doppler frequency shifts, converts them to **pseudorange** and pseudo range variation rates and determines the spatial position and speed while setting the GNSS time.

To solve navigation problems, a specialized built-in computer is provided in the consumer equipment. The variety of existing consumer equipment meets the needs of land, sea, aviation, space etc. consumers (Table 1).

Table 1. The GNSS application on land, above water, in the air and (most importantly and almost not developed) underwater (sorted alphabetically)

Таблица 1. Применение GNSS на суше, над водой, в воздухе и (что наиболее важно и почти не разработано) под водой (отсортировано по алфавиту)

	Agriculture		Power grids (hydro, heat, wind, solar)
	Armament		Search and Rescue
	Building		Space navigation
	Banking systems (Online trading, Stock and Mobile markets, ATMs)		Transport (Aviation, Cars, Trains Sea vessels)
	Communication systems		Search and Rescue
	Geodesy and cartography		Underwater LNSS (GNSS-like) navigation
	Personal navigation		

Positioning and navigation problems have proven to be well-developed in all areas of the Earth (on the surface of the lithosphere and hydrosphere, in the atmosphere, troposphere and stratosphere), except the hydrosphere. This article is devoted to the problem of a brief analysis of the state of underwater positioning and underwater navigation and practically the undeveloped problem of the underwater navigation safety. Here we restrict ourselves to analyzing the possibility of transferring the well-established GNSS technology to the underwater world. Unfortunately, GNSS signals attenuate very quickly in water, therefore all GNSS-like [8] technologies are of the local nature, based on the retransmission of the electromagnetic wave of GNSS signals into the acoustic wave

Hence, hereinafter we will use the term LNSS (Local Navigation Satellite Systems) to refer to this technology.

2. GNSS Vulnerabilities

When using GNSS, vehicle information protection is required. GNSS is vulnerable to Interference, Jamming, spoofing and self-spoofing attacks (Fig. 2).

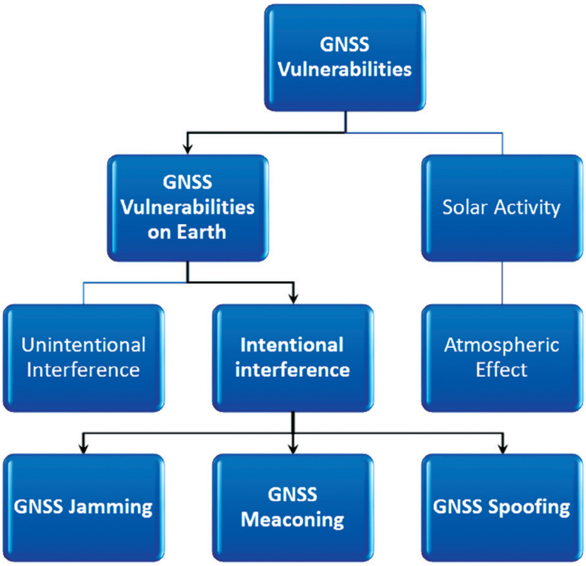


Fig. 2. The main GNSS Vulnerabilities

Рис. 2. Основные уязвимости GNSS

Here we do not consider the influence of Solar Activity and the related Atmospheric Effect on the GNSS accuracy, and do not consider the Unintentional Interference (Industrial Electromagnetic Interference, Multipath and Jamming). We focus on the Intentional Interference, including

1. GNSS Jamming Attacks.
2. GNSS Meaconing Attacks[1].

[1] Meaconing can be considered as a special case of spoofing, however, in the literature it is usually allocated in a separate class due to the historical features of the use of this technology in electronic warfare.

3. GNSS Spoofing Attacks.
4. GNSS Self-Spoofing Attacks [9].

The problem of dealing with jamming is well-developed. The most difficult type of attacks is spoofing. The spoofer can transmit false signals from a distance of several tens or hundreds of meters from the victim. The spoofing can be divided into simple, intermediate, or complex attacks in terms of their effectiveness. In this article, we briefly look at Interference and Jamming, as well as the algorithms for detecting meaconing and Spoofing based on one or two receivers. We also overview briefly the issues of anti-meaconing and anti-spoofing.

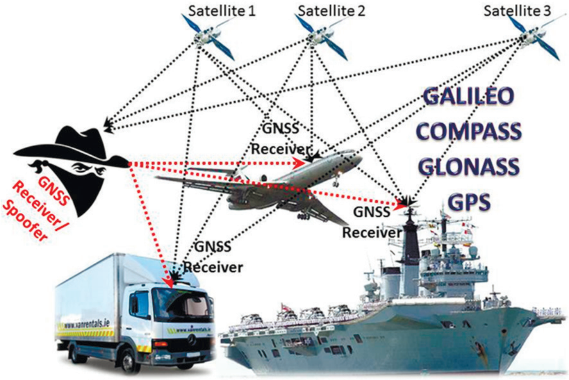


Fig. 3. GNSS Spoofing. Spoofing interferes with the structure of GNSS transmission and deliberate modification of the receiver's route. This is a terrorist, information attack involving the use of original data from a reliable source of information to fraudulent customer security by sending distorted or false data in its place

Рис. 3. Спуфинг GNSS. Спуфинг изменяет структуру передачи данных GNSS и преднамеренно модифицирует маршрут пользователя. Это террористическая информационная атака, включающая использование оригинальных данных из надежного источника информации для преодоления безопасности клиентов путем отправки на их место искаженных или ложных данных

GNSS signals have low power, which means that a weak source of interference can cause the receiver to fail or create dangerously misleading information. So far, the biggest concern for GNSS has been its possible jamming by masking the satellite signal with noise. The complete loss of GNSS is fairly easy to detect, but barely noticeable movements due to jamming can seem like spoofing, which can be very difficult to detect.

Spoofing is more insidious: a false signal from a ground station that simply knocks down the satellite receiver. For simplicity, jamming leads to the death of the receiver, and forgery – to the fact that the receiver is lying. However, as explained below, this statement is not technically correct, but it provides a broad overview of what the main difference between interference and spoofing is.

2.1. Why GNSS is relatively easily affected by vulnerabilities

The qualitative analysis shows that the radiation energy of the satellite's transmitting antenna significantly decreases when approaching the Navigator's receiving antenna (Fig. 4).

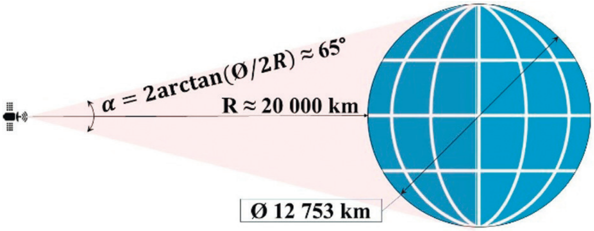


Fig. 4. The radiation flux density decreases with the distance from the satellite

Рис. 4. Плотность потока излучения уменьшается с удалением от спутника

The energy that electromagnetic waves carry over time is distributed over a larger and larger surface (Fig. 5). The quantitative analysis shows that the energy transmitted through the surface of a single site (shown in blue in Fig. 5) per unit time, i.e., the radiation flux density, decreases with distance from the source as

$$I = \frac{\Delta W}{S\Delta t} = \frac{\Delta W}{4\pi\Delta t}\frac{1}{R^2} \tag{1}$$

consequently, the study flux density decreases inversely with the square of the distance to the satellite's antenna.

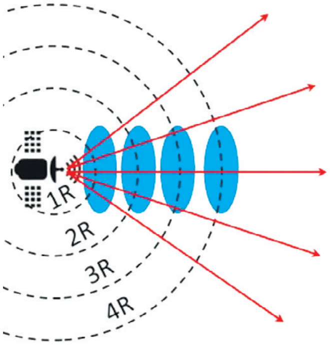


Fig. 5. The radiation flux density decreases with distance from the satellite in inverse proportion to the square of the distance to the satellite's antenna

Рис. 5. Плотность потока излучения уменьшается с расстоянием от спутника обратно пропорционально квадрату расстояния до антенны спутника

If we take into account that the GNSS orbits are at altitudes of about 20,000 km, then equation (1) can be written as

$$I = \frac{\Delta W}{S\Delta t} = \frac{\Delta W}{4\pi\Delta t}\frac{1}{400{,}000{,}000{,}000{,}000} \qquad (2)$$

This means that the radiation flux density upon reaching the navigator’s antenna decreased 400 trillion times! From here we make an exceptional first important conclusion.

With the help of a primitive jammer at the cost of tens of dollars, any uneducated terrorist can suppress the GNSS operation within a radius of several tens of meters. If you need to increase the range of the jammer to several tens of kilometers, you will have to pay several thousand dollars, unless, of course, military jammers are sold to you.

2.2. Why {GNSS + INS} partially block vulnerabilities

The exceptional second important conclusion is as follows. To ensure the safe piloting of autonomous vehicles, GNSS should be viewed as an aid to positioning and navigation. Wherever possible, we should equip our unmanned vehicles with INS, etc.

An inertial navigation system is a navigation device that uses motion sensors to continuously track the position, orientation, and speed of a vehicle without the need of external links.

The application of microelectromechanical systems (MEMS) in INS is of particular significance for commercial unmanned vehicles.

Several types of INS have been developed for maritime, air and land applications. A number of ground moving objects have odometrical coordinate systems based on counting the number of revolutions of a standard wheel. The information on the covered distance is obtained by the odometer, and information on the direction is obtained by the gyroscope. If the tool starts from a known position, then the information about the distance and direction can be used to determine the position at any time. Being an environment-independent system, INS provides the same high accuracy as GNSS, but for a short time after initialization. Moreover, INS provides high-speed data updates comparable to GNSS. The main disadvantage of INS is that they accumulate an invalid positioning error over long time intervals.

The combination of GNSS and INS overcomes the limitations of both systems.

Concluding the introduction, we would like to pay attention to Fig. 6, which shows the main focus of this article.

GNSS Position, Navigation, and Timing in the Air, on Land, in the Sea and Under Water
GNSS Jamming, Meaconing, and Spoofing

Fig. 6. Two closely related classes of GNSS problems

Рис. 6. Два тесно связанных класса проблем GNSS

The devil is not so terrible as he is painted – it's about jamming and spoofing. If the "Spoofing Detection" subsystem has detected an attack, the processor will switch the navigation to the INS subsystem and if the GNSS "signal loss time" and the corresponding accumulated error are valid for these INS, then it will return to GNSS navigation.

3. Classification of Marine Unmanned Vehicle

Unmanned Vehicles appeared in the late 80s. DARPA[1] pioneered this technology. To broaden its horizons, DARPA created the biennial AUV conference. However, even at present, the terminology associated with the design and use of marine unmanned vehicles (MUV) still requires significant systematization, therefore in this article we use the following basic abbreviations, designations, terms and their definitions (Fig. 7 and Table 2), which the author has collected and systematized from various sources (111, etc.).

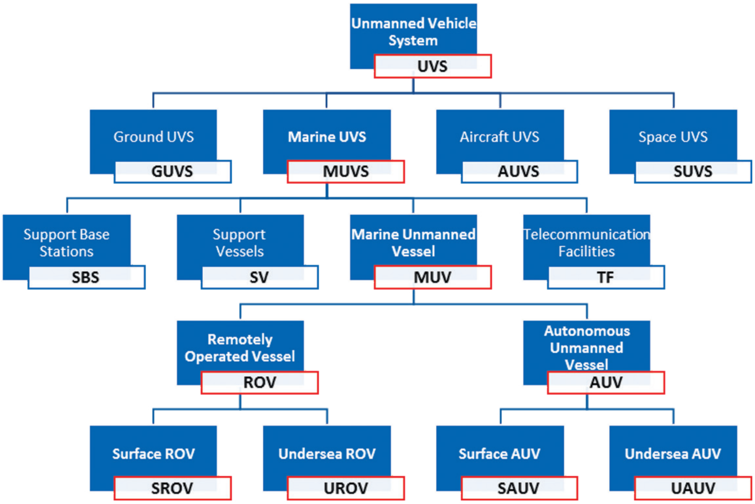


Fig. 7. Classification of Marine Unmanned Vehicles

Рис. 7. Классификация морских беспилотных аппаратов

[1] https://www.darpa.mil/ (Accessed: 17 July 2020)

Table 2. Main abbreviations, designations, terms and their definitions

Таблица 2. Основные сокращения, обозначения, термины и их определения

Object	Description
Marine Unmanned Vessel System (MUVS)	The infrastructure for providing the mission for marine unmanned vehicles, representing the combination of marine unmanned vessels, manned support vehicles, support base stations, telecommunications facilities, etc.
Support Base Station (SBS)	The Support Base Station (SBS) is the ground and /or surface part of MUVS, ensuring the execution of the mission for marine unmanned vessels.
Marine Unmanned Vessels (MUV)	Marine Unmanned Vessels (MUV) is a surface or submarine vessel that does not have a command on board and is capable of performing MisUV autonomously using an on-board computer and/or via remote control of a dispatcher or dispatch computer.
The Given Route (GR) of a UV	The Given Route (GR) of a MUV is the route of a MUV on the water surface and/or underwater from one 3D point of the sea to another 3D point of the sea through open areas of the sea and/or narrowness (straits, channels, rivers and lakes). The GR forms the SBS.
The Mission of a UV (MisUV)	The Mission of a UV (MisUV) is the precise preprogrammed trajectories of a MUV on the water surface and/or underwater from one 3D point of the sea to another 3D point of the sea through open areas of the sea and/or narrowness (Straits, channels, rivers and lakes). The MUV forms the SBS as preplanning of all MUV courses based on the study of the navigation situation along the mission using lots, large-scale sea maps, bathymetric data, meteorological bulletins, etc.
The navigation padding of the MUV	The navigation padding is a continuous control of the MUV movement using an onboard computer with maximum proximity to the MisUV during the entire mission.
Remotely Operated Vessel (ROV)	Remotely Operated Vessel (ROV) is a MUV that is capable of performing MisUV via remote control of a dispatcher or dispatch.
Surface ROV (SROV)	Surface Remotely Operated Vessel (SROV) is a surface ROV that is capable of performing MisUV via remote control of a dispatcher or dispatch computer and maneuvers in two dimensions.
Undersea ROV (UROV)	Surface Remotely Operated Vessel (SROV) is an undersea ROV that is capable of performing MisUV by remote control of a dispatcher or dispatch computer and maneuvers in three dimensions.
Autonomous Undersea Vessel (AUV)	Autonomous Undersea Vessel (AUV) is a MUV that is capable of performing MisUV autonomously using an onboard computer and maneuvers in three dimensions.
Surface AUV (SAUV)	Surface Autonomous Undersea Vessel (SAUV) is a surface AUV that is capable of performing MisUV autonomously using an on-board computer and maneuvers in two dimensions.
Undersea AUV (UAUV)	Undersea Autonomous Undersea Vessel (SAUV) is an undersea AUV that is capable of performing MisUV autonomously using an on-board computer and maneuvers in three dimensions.

Among the many UVSs (Fig. 7) in this article, we limit ourselves to considering only the Marine Unmanned Vehicle System (MUVS). Table 2 helps to understand the abbreviations, designations and terms.

The main problem of the classification is that, on the one hand, it is important to preserve the well-established abbreviations, designations, terms and their definitions, and on the other hand, it is important to adhere to the general principles of object classification. Hopefully, we managed to find a middle ground in this difficult search.

4. Underwater navigation

Omitting many important historical and engineering details, we consider the basic technologies of underwater LNSS positioning and LNSS navigation.

The simplest satellite positioning technology is the LNSS based on the popup tethered GNSS antenna (Fig. 8*a*). This technology is used to refine the $\{x, y\}$ coordinates (the $\{z\}$ coordinate is calculated based on a water pressure sensor and knowledge of the sea level altitude). The navigation problem is solved with the antenna towing or the Inertial Navigation System (INS).

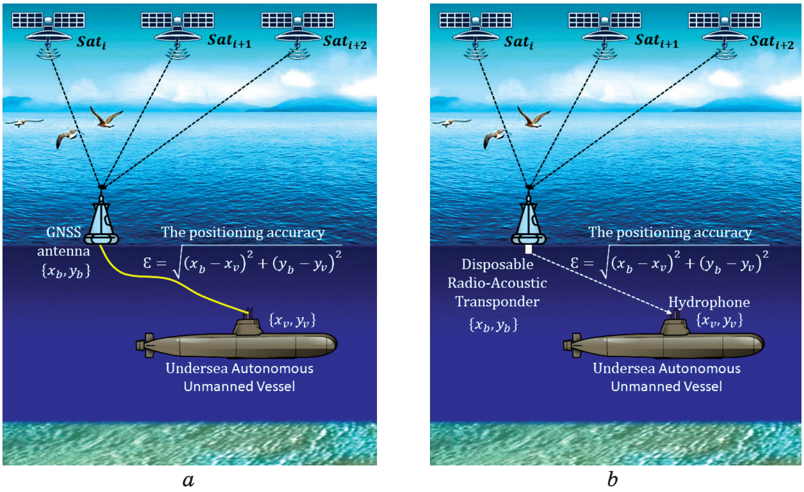

Sat_i
Sat_{i+1}
Sat_{i+2}
GNSS antenna $\{x_b, y_b\}$
The positioning accuracy
$\varepsilon = \sqrt{(x_b - x_v)^2 + (y_b - y_v)^2}$
$\{x_v, y_v\}$
Undersea Autonomous Unmanned Vessel
a
Sat_i
Sat_{i+1}
Sat_{i+2}
Disposable Radio-Acoustic Transponder $\{x_b, y_b\}$
The positioning accuracy
$\varepsilon = \sqrt{(x_b - x_v)^2 + (y_b - y_v)^2}$
Hydrophone $\{x_v, y_v\}$
Undersea Autonomous Unmanned Vessel
b

Fig. 8. LNSS Position: a – based on popup tethered GNSS antenna, b – based on tethered Disposable Radio-Acoustic Transponder

Рис. 8. LNSS-позиционирование: а – на основе всплывающей привязанной антенны GNSS, б – на основе привязного одноразового радиоакустического транспондера

At greater depths, the use of the cable becomes difficult and one has to use the LNSS technology based on Tethered Disposable Radio-Acoustic Transponder (Fig. 8*b*). The Transponder can be tethered from an UAUV or installed from a ship or aircraft. In this case, navigation is only possible with INS[1].

The underwater navigation [8; 10–12] has become widespread as a complex of technologies, which in the literature are usually described together – Short Baseline (SBL) (Fig. 9*a*), Ultra-Short Baseline (USBL) (Fig. 9*b*), and Long Baseline (LBL) (Fig. 9*c*). These three technologies have a lot in common, but, of course, they differ significantly.

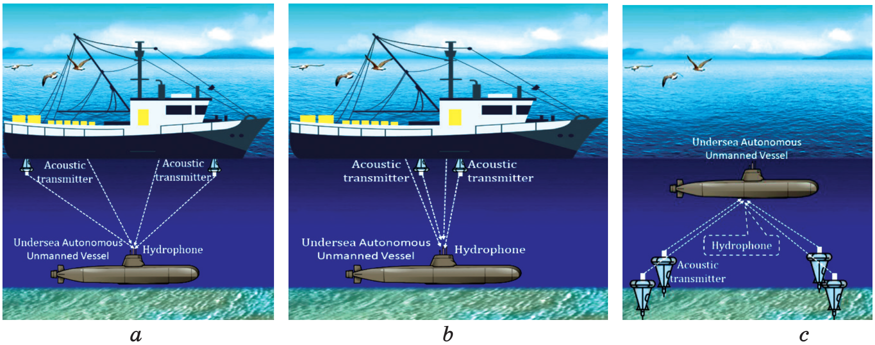


Fig. 9. a – Short Baseline (SBL), b – Ultra-Short Baseline (USBL), c – Long Baseline (LBL). The positions of each acoustic transmitter are specified in geographic coordinates using GNSS or (for SBL and USBL) in relative coordinates, for example, relative to the center of the support vessel as {0,0,0}

Рис. 9. а – Короткая базовая линия (SBL), б – Ультра-короткая базовая линия (USBL), с – Длинная базовая линия (LBL). Положение каждого акустического передатчика указывается в географических координатах с использованием GNSS или (для SBL и USBL) в относительных координатах, например, относительно центра судна поддержки как {0,0,0}

They are similar in the following parameters. Here, the trilateration method, well studied in geodesy, is used. Determining the location of the $\{x, y\}$ of undersea UAUV is based on measuring the distances (ranges) from the acoustic transmitters to the hydrophone of the Vessel in terms of the speed and propagation time of acoustic waves. If the range of up to three acoustic transmitters is measured and their coordinates are known the coordinates of the vessel's position may be determined.Due to the different accuracy of the "clocks" on the acoustic transmitters and in the hydrophone and some other reasons, the distances determined by the acoustic transmitters may be defined with an error. This erroneous distance is called "pseudo-range". If we omit the

[1] An inertial navigation system (INS) is a navigation device that uses a computer, motion sensors (accelerometers) and rotation sensors (gyroscopes) to continuously calculate by dead reckoning the position, the orientation, and the velocity (direction and speed of movement) of a moving object without the need for external references.

problem of error analysis, then we can write a system of equations connecting the coordinates of acoustic transmitters and UAUV

$$\begin{cases} (x_1 - x_v)^2 + (y_1 - y_v)^2 = D_1{}^2 \\ (x_2 - x_v)^2 + (y_2 - y_v)^2 = D_2{}^2, \\ (x_3 - x_v)^2 + (y_3 - y_v)^2 = D_3{}^2 \end{cases} \tag{3}$$

where D_i, $i = \overline{1{,}3}$ – the measured distances up to three (Fig. 8) acoustic transmitter, $\{x_i,\ y_i\}$ $i = \overline{1{,}3}$ – the known coordinates of three acoustic transmitters, $\{x_v,\ y_v\}$ – the unknown coordinates of UAUV.

The solution to the system of equations (1) is the calculated coordinates of UAUV (4):

$$\begin{cases} x_v = \dfrac{(y_2 - y_1)(D_2^2 - D_3^2 - x_2^2 + x_3^2 - y_2^2 + y_3^2) - (y_3 - y_2)(D_1^2 - D_2^2 - x_1^2 + x_2^2 - y_1^2 + y_2^2)}{2((y_3 - y_2)(x_1 - x_2) - (y_2 - y_1)(x_2 - x_3))} \\ y_v = \dfrac{(x_2 - x_1)(D_2^2 - D_3^2 - y_2^2 + y_3^2 - x_2^2 + x_3^2) - (x_3 - x_2)(D_1^2 - D_2^2 - y_1^2 + y_2^2 - x_1^2 + x_2^2)}{2((x_3 - x_2)(y_1 - y_2) - (x_2 - x_1)(y_2 - y_3))} \end{cases} \tag{4}$$

The coordinates $\{x_v,\ y_v,\ z_v\}$ of UAUV are estimated if the depth's calculation is added to the geographic coordinates using measured water pressure, i.e. $\{z_v\} = f(\textit{water pressure})$.

Without binding to GNSS, if the origin is as $\{x_v,\ y_v,\ z_v\} = \{0,\ 0,\ 0\}$, i.e. bind to some point of the supply vessel, then the natural depth of immersion is $\{z_v\} = 0$ at time $t = 0$.

Many hydroacoustic synchronous rangefinder navigation systems are also known. Examples include the Norwegian HiPAP from Kongsberg, the French GAPS from IXBLUE, as well as the huge contribution to these technologies by the American Teledyne, the German EvoLogics.de, the English Sonardyne, of course American DARPA (Fig. 10) and many others.

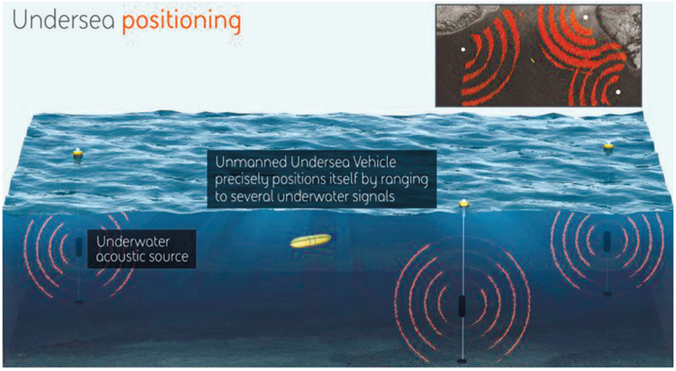

Undersea positioning
Unmanned Undersea Vehicle precisely positions itself by ranging to several underwater signals
Underwater acoustic source

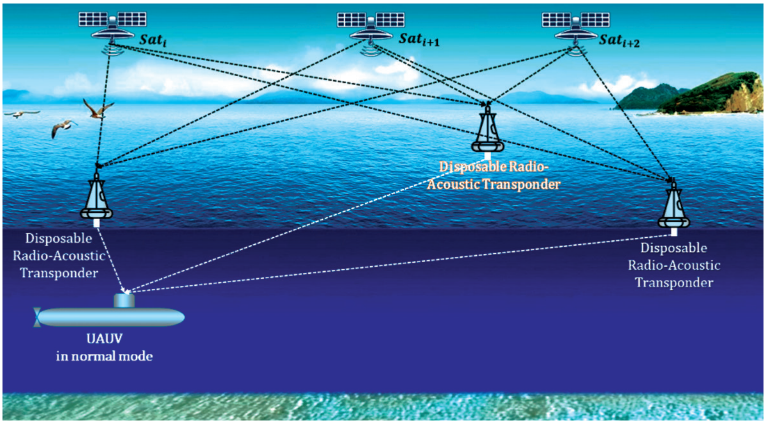
Fig. 10. DARPA program plunges into underwater positioning systems
From https://newatlas.com/darpa-underwater-navigation/43472/
(Accessed: 17 July 2020)

Рис. 10. Программа DARPA по системам подводного позиционирования
Источник https://newatlas.com/darpa-underwater-navigation/43472/
(Доступ: 17 июля 2020 г.)

5. GNSS-equipped Intelligent Buoys (GIB)

GIB provides real-time absolute coordinates, speed and trajectory of the movement of submarines, divers, remotely controlled underwater vehicles, autonomous manned and unmanned underwater vehicles. Based on the GIB, LNSSs are implemented, which can be classified as LBL acoustic positioners. GNSS-equipped Intelligent Buoys can be drifting or moored. The number of GIBs is determined by the size of the controlled area and the positioning accuracy.

We consider one of the many options for constructing an LNSS based on the GIB, indicated in Fig. 11 as the Disposable Radio-Acoustic Transponders.



Sat_i
Sat_{i+1}
Sat_{i+2}
Disposable Radio-Acoustic Transponder
Disposable Radio-Acoustic Transponder
Disposable Radio-Acoustic Transponder
UAUV in normal mode

Fig. 11. LNSS Navigation based on three Disposable Radio-Acoustic Transponders of type GIB (Disposable Radio-Acoustic Transponders)

Рис. 11. LNSS-навигация на основе трех одноразовых радиоакустических транспондеров типа GIB (одноразовые радиоакустические транспондеры)

The navigation satellite is a transmitting radio station with known $\{x, y, z\}$ coordinates, which emits directional radio signals. The radio receiver of a GIB measures Δt – the **Time of Arrival** (TOA or ToA, and also ToF – the time of flight) of the radio signal from the satellite to the radio receiver and determines the distance to it $\rho = c \cdot \Delta t$, where is the speed of electromagnetic waves propagation, approximately equal to the speed of light $c \approx 300{,}000$ km/s.

In the general case for N satellites (the positioning accuracy increases with the increase in the number of the “visible” satellites)

$$\{\rho_i = \sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} - \Delta\rho\},\ i = \overline{1, N}, \tag{5}$$

where x_i, y_i, z_i – the known coordinates of the i-th satellite that the i-th satellite transmitted to the vehicle; x_v, y_v, z_v – the unknown coordinates of the vehicle V; ρ_i – measured pseudorange from the *i*-th satellite to the vehicle *V* with the unknown error Δρ, which is the same for all satellites; *N* – the number of “visible” navigation satellites.

To solve the system of equations (5), relatively complex iterative algorithms are used to calculate $\{x_v, y_v, \Delta\rho\}$, consideration of which is beyond the scope of this article.

Suppose LNSS Navigation is built on three UAUV of the GIB type. In this case it can be shown that the system of equations (6)

$$\begin{cases}(x_1-x_v)^2+(y_1-y_v)^2=D_1^2\\(x_2-x_v)^2+(y_2-y_v)^2=D_2^2,\\(x_3-x_v)^2+(y_3-y_v)^2=D_3^2\end{cases}\qquad(6)$$

where D_i, $i=\overline{1,3}$ – measured distances up to three (Fig. 8) GIB, $\{x_i, y_i\}$ $i=\overline{1,3}$ – known coordinates of three GIBs, $\{x_v, y_v\}$ – unknown coordinates of UAUV.

The solution to the system of equations (6) is the calculated coordinates UAUV (7):

$$\begin{cases}x_v=\dfrac{(y_2-y_1)(D_2^2-D_3^2-x_2^2+x_3^2-y_2^2+y_3^2)-(y_3-y_2)(D_1^2-D_2^2-x_1^2+x_2^2-y_1^2+y_2^2)}{2((y_3-y_2)(x_1-x_2)-(y_2-y_1)(x_2-x_3))}\\y_v=\dfrac{(x_2-x_1)(D_2^2-D_3^2-y_2^2+y_3^2-x_2^2+x_3^2)-(x_3-x_2)(D_1^2-D_2^2-y_1^2+y_2^2-x_1^2+x_2^2)}{2((x_3-x_2)(y_1-y_2)-(x_2-x_1)(y_2-y_3))}\end{cases}.\qquad(7)$$

The coordinates $\{x_v, y_v, z_v\}$ of UAUV are estimated by adding the depth calculation to geographic coordinates using measured water pressure, i.e. $\{z_v\} = f(\textit{water pressure})$.

6. Underwater spoofing

Omitting many extremely important engineering details, let’s move on to the main topic of this article – the safety issue of LNSS underwater navigation [13–24].

The spoofer (Fig. 12) enters the UAUV area of responsibility quietly, “listens” to GIBs, calculates its own coordinates $\{x_S, y_S, 0\}$. In underwater mode, the spoofer calculates its depth $\{z_S\} = f(\textit{water pressure})$ and gets its coordinates $\{x_S, y_S, z_S\}$. Listening to UAUV noises, the spoofer determines the bearing and distance to UAUV and estimates the target coordinates $\{\tilde{x}_v, \tilde{y}_v, \tilde{z}_v\}$.

Next, the spoofer processor solves the inverse problem (8)

$$\begin{cases}(x_1-\tilde{x}_v+\Delta_x)^2+(y_1-\tilde{y}_v+\Delta_y)^2=(D_1+d_1)^2\\(x_2-\tilde{x}_v+\Delta_x)^2+(y_2-\tilde{y}_v+\Delta_y)^2=(D_2+d_2)^2,\\(x_3-\tilde{x}_v+\Delta_x)^2+(y_3-\tilde{y}_v+\Delta_y)^2=(D_3+d_3)^2\end{cases}\qquad(8)$$

where $\{\Delta_x, \Delta_y\}$ – the desired UAUV offset that can be achieved by introducing appropriate delays Δt_i for the GIB signals (9)

$$\begin{cases} \Delta t_1 = d_1 / c \\ \Delta t_2 = d_2 / c, \\ \Delta t_3 = d_3 / c \end{cases} \tag{9}$$

where c is the speed of sound in water (for the given frequency).

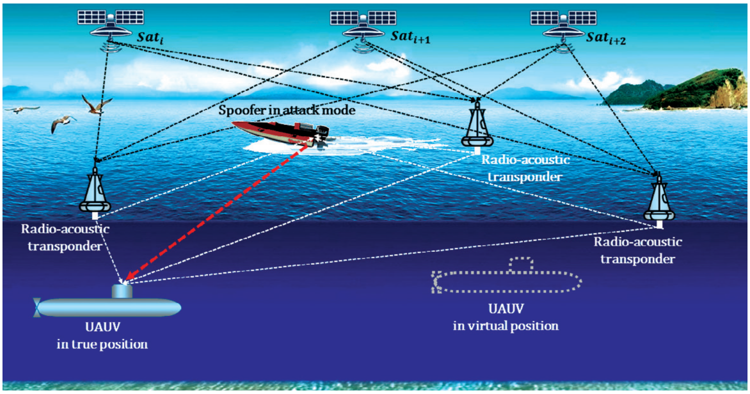


Fig. 12. The Spoofing of LNSS Navigation based on three Disposable Radio-Acoustic Transponders of type GIB

Рис. 12. Спуфинг LNSS-навигации на основе трех одноразовых радиоакустических транспондеров типа GIB

Further, the spoofer uses acoustic radiation directed at the UAUV of increased power compared to the power of acoustic signals from the GIBs. As a result, UAUV "switches" from real GIB signals to fake spoofer signals and solves the already "fake" system of equations (7)

$$\begin{cases} (x_1 - x_v)^2 + (y_1 - y_v)^2 = (D_1 + d_1)^2 \\ (x_2 - x_v)^2 + (y_2 - y_v)^2 = (D_2 + d_2)^2, \\ (x_3 - x_v)^2 + (y_3 - y_v)^2 = (D_3 + d_3)^2 \end{cases} \tag{10}$$

where $\{D_i + d_i\}$, $i = \overline{1,3}$ – measured distances up to three (Fig. 8) "false" GIBs, $\{x_i, y_i\}$ $i = \overline{1,3}$ – known (unmodified by the spoofer) coordinates of the three GIBs, $\{x_v, y_v\}$ – unknown coordinates of UAUV.

The solution to the system of equations (10) is the calculated "false" coordinates UAUV (11).

$$\begin{cases} x_v = \dfrac{\begin{gathered}(y_2 - y_1)((D_2 + d_2)^2 - (D_3 + d_3)^2 - x_2^2 + x_3^2 - y_2^2 + y_3^2) - \\ -(y_3 - y_2)((D_1 + d_1)^2 - (D_2 + d_2)^2 - x_1^2 + x_2^2 - y_1^2 + y_2^2)\end{gathered}}{2((y_3 - y_2)(x_1 - x_2) - (y_2 - y_1)(x_2 - x_3))}, \\ y_v = \dfrac{\begin{gathered}(x_2 - x_1)((D_2 + d_2)^2 - (D_3 + d_3)^2 - y_2^2 + y_3^2 - x_2^2 + x_3^2) - \\ -(x_3 - x_2)((D_1 + d_1)^2 - (D_2 + d_2)^2 - y_1^2 + y_2^2 - x_1^2 + x_2^2)\end{gathered}}{2((x_3 - x_2)(y_1 - y_2) - (x_2 - x_1)(y_2 - y_3))} \end{cases} \tag{11}$$

The further development of the spoofing strategy depends on many factors. Here we stop in believe that the main idea of the underwater LNSS vulnerability in the form of an underwater spoofing attack is clear to the reader.

7. Spoofing detection

If the spoofer is stationary and UAUV is moving in a certain direction at the speed V, then the spoofing detector, located on board the UAUV, at the time t' determines its coordinates $\{x'_v, y'_v\}$ in accordance with (3) and (4), adds the calculated depth using the measured water pressure, i.e. $\{z'_v\} = f(water\, pressure)$ and gets the coordinates $\{x'_v, y'_v, z'_v\}$ of UAUV. After some time the spoofing detector repeats the determination of its coordinates $\{x''_v, y''_v, z''_v\}$.

7.1. The spacing between two positions of UAUV in navigation mode

The measured distance Δd between the hydrophone at the times t' and is t'' (12)

$$\Delta d = \sqrt{(x'_v - x''_v)^2 + (y'_v - y''_v)^2 + (z'_v - z''_v)^2}. \qquad (12)$$

This Δd must be commensurate with the distance Δd covered by the vehicle over time Δt, i.e.:

$$\Delta d \approx V(t'' - t'). \qquad (13)$$

7.2. The spacing between two positions of UAUV in spoofing mode

The measured distance Δd between the hydrophone at the times t' and is t'' (14)

$$\Delta d = \sqrt{(x'_v - x''_v)^2 + (y'_v - y''_v)^2 + (z'_v - z''_v)^2} \approx 0, \qquad (41)$$

since all the hydrophones in the spoofing zone calculate the same false coordinates and should be commensurable with the distance Δd travelled by the vehicle over time $(t'' - t')$ over time $(t'' - t')$, i.e.:

$$\Delta d << V(t'' - t'). \qquad (15)$$

7.3. The decisive rule

Comparing equations (9) and (12), the decisive rule for detecting spoofing can be written as (16):

$$if\, \Delta d << V(t'' - t') \text{ then go to Spoofing.} \qquad (16)$$

The main disadvantage of this spoofing detection method is the spoofing dead zone $\{V < V_{\min}\}$, i.e. if UAUV stands still or moves at a low speed less than some experimentally determined speed $V_{\min}$, then spoofing cannot be detected. To overcome this disadvantage, it is necessary to have two hydrophones on the UAUV hull, spaced as far as possible D_{1-2} (for example, at the stern and at the stem).

In this case, UAUV can stand still or move at any speed. The spoofing detector determines its coordinates using the first hydrophone $\{x_v', y_v'\}$ in accordance with (3) and (4), adds the calculated depth using the measured water pressure, i.e. $\{z_v'\} = f(water\ pressure)$ and gets the coordinates of $\{x_v', y_v', z_v'\}$ UAUV. At the same time, the spoofing detector determines its coordinates using the second hydrophone $\{x_v'', y_v''\}$ in accordance with (3) and (4), adds the calculated depth using the measured water pressure, i.e. $\{z_v''\} = f(water\ pressure)$ and gets the coordinates $\{x_v'', y_v'', z_v''\}$ of UAUV.

The measured distance between hydrophones should be commensurate with the actual distance between hydrophones in normal UAUV operation (17)

$$\Delta d = \sqrt{(x_v' - x_v'')^2 + (y_v' - y_v'')^2 + (z_v' - z_v'')^2} \approx D_{1-2} \qquad (17)$$

and approximately equal to zero in spoofing attack mode (15)

$$\Delta d = \sqrt{(x_v' - x_v'')^2 + (y_v' - y_v'')^2 + (z_v' - z_v'')^2} \approx 0. \qquad (18)$$

Comparing equations (17) and (18), the decisive rule for detecting spoofing can be written as (16):

$$if\,\Delta d \approx 0 \text{ then go to Spoofing.} \qquad (19)$$

where "≈" refers to the definition of some area of uncertainty $\Delta d_{\min}$, determined on the basis of statistical studies at the design stage of a real detection system.

8. Simulation of the underwater LNSS

Initially, when the UAUV is launched from a support vessel, it travels down a spiral path before reaching operating depth (Fig. 13). At this point it is necessary to localize the UAUV to help calibrate the INS (if the UAUV has such equipment). Then UAUV performs the assigned mission and returns to the base.

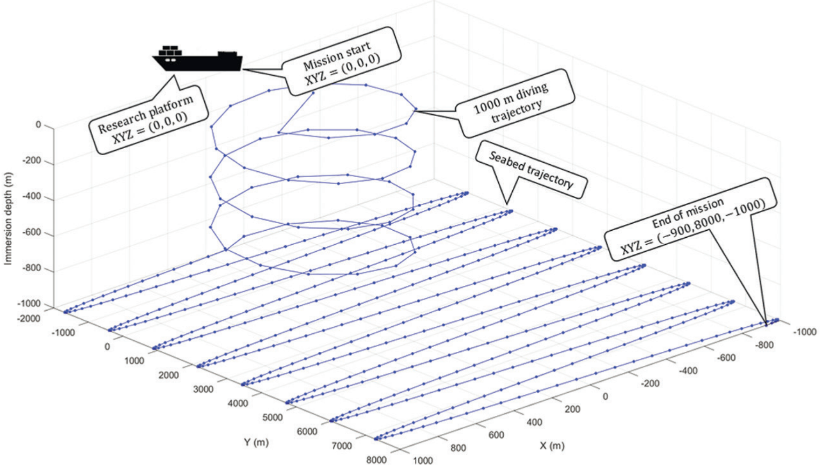


Fig. 13. Subsea LNSS Simulation

Рис. 13. Моделирование подводной LNSS

The basic techniques, which are used to solve the problem of spoofing detection above water, can also be used under water. Since conduction of physical experiments underwater is incomparably more complex task than surface experiments, at this stage of research we tested the principles of underwater spoofing detection using a simulation approach. We are planning to devote the next article "The Modelling and Simulation of the Undersea LNSS Vulnerabilities" to the problems of modelling UAUV trajectories in complex, including under-ice conditions.

9. Conclusion

The trend towards the melting of Arctic ice has led to the prospect of creating new sea routes and perhaps more important potential access to natural resources under the Arctic Ocean. Many countries have shown unusual activity in collecting bathymetric data to determine their sovereign Arctic territory.

Therefore, in conditions of fierce competition in the development of the Earth's hydrosphere, it is necessary not only to design the UAUV, but also to ensure safe sea diving.

References

1. *Official U.S. government information about the Global Positioning System (GPS) and related topics*. Available at: www.GPS.gov (Accessed: 17 July 2020)

2. Yang Y., Mao Y., Sun B. Basic performance and future developments of BeiDou global navigation satellite system. *Satellite Navigation*. 2020;1:1. DOI: 10.1186/s43020-019-0006-0.

3. *BeiDou's road to global service. GPS World*. 6 December 2016. Available at: https://www.gpsworld.com/directions-2017-beidous-road-to-global-service/ (Accessed: 17 July 2020)

4. *European Space Agency's Galileo website*. Available at: https://www.esa.int/Applications/Navigation/Galileo (Accessed: 17 July 2020)

5. *Indian Regional Navigation Satellite System/NavIC*. Available at: https://www.isro.gov.in (Accessed: 17 July 2020)

6. *Quasi-Zenith Satellite System*. Available at: https://qzss.go.jp (Accessed: 17 July 2020)

7. Datta A. *Multi-constellation GNSS receivers becoming a standard*. Available at: https://www.geospatialworld.net/blogs/multi-constellation-gnss-receivers-norm/ (Accessed: 17 July 2020)

8. Nacini F. *JANUS creates a new era for digital underwater communications*. Available at: https://robohub.org/janus-creates-a-new-era-for-digital-underwater-communications/ (Accessed: 17 July 2020)

9. Caparra G., Ceccato S., Laurenti N., Cramer J. Feasibility and Limitations of Self-Spoofing Attacks on GNSS Signals with Message Authentication. In: *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION*

GNSS+ 2017), Portland, Oregon, September 2017, pp. 3968–3984. DOI: 10.33012/2017.15402.

10. Stutters L., Liu H., Tiltman C., Brown D. Navigation technologies for autonomous underwater vehicles. In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*. 2008;38(4):581–589. 10.1109/TSMCC.2008.919147.

11. Miller P., Farrell J., Zhao Y., Djapic V. Autonomous underwater vehicle navigation. *IEEE Journal of Oceanic Engineering*. 2010;35(3):663–678. DOI: 10.1109/JOE.2010.2052691.

12. Webster S. E., Eustice R. M., Singh H., Whitcomb L. L. Advances in single-beacon one-way-travel-time acoustic navigation for underwater vehicles. *The International Journal of Robotics Research*. 2012;31(8):935–950. DOI: 10.1177/0278364912446166.

13. Dobryakova L., Ochin E. On the application of GNSS signal repeater as a spoofer (GNSS signal repeater = Meaconing). *Scientific Journals Maritime University of Szczecin*. 2014;(40):53–57. Available at: http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-27082d5c-1bbf-405f-b164-96d0e7e91dd5/c/Dobryakova_Ochin_112-8.pdf (Accessed: 18 July 2020)

14. Dobryakova L., Lemieszewski Ł., Ochin E. The vulnerability of unmanned vehicles to terrorist attacks such as Global Navigation Satellite System Spoofing. *Scientific Journals of the Maritime University of Szczecin*. 2016;(46):181–188. DOI: 10.17402/135.

15. Dobryakova L., Lemieszewski Ł., Ochin E. Protecting vehicles vulnerable to terrorist attacks, such as GNSS Jamming, by electromagnetic interference shielding of antenna. *Scientific Journals Maritime University of Szczecin*. 2017;(50). DOI: DOI: 10.17402/219.

16. Ochin E. Detection of Spoofing using Differential GNSS. *Scientific Journals Maritime University of Szczecin*. 2017;(50). DOI: 10.17402/217.

17. Ochin E. GPS/GNSS spoofing and the real-time single-antenna-based spoofing detection system. *Scientific Journals Maritime University of Szczecin*. 2017;(52):145–153. DOI: 10.17402/256.

18. Ochin E. GNSS and DGNSS Spoofing Detection. *Ural Radio Engineering Journal*. 2017;1(1):55–79. DOI: 10.15826/urej.2017.1.1.003.

19. Dobryakova L., Lemieszewski Ł., Ochin E. Protecting of vehicles with help of anti-jamming and anti-spoofing by shielding of GNSS antenna. In: *REIT 2017 Autumn, Submission 31*. Available at: http://reit-rtf.ru/2017b.html (Accessed: 18 July 2020)

20. Dobryakova L. A., Lemieszewski Ł. S., Ochin E. F. Global Navigation Satellite Systems attacks and a cloud-based spoofing detection for unmanned ships. *Ural Radio Engineering Journal*. 2017;2(2):40–56. DOI: 10.15826/urej.2018.2.2.003.

21. L Dobryakova., Lemieszewski Ł., Ochin E. GNSS Spoofing Detection Using Static or Rotating Single-Antenna of a Static or Moving Victim. IEEE Access. 2018;6:79074–79081. DOI: 10.1109/ACCESS.2018.2879718.

22. Dobryakova L., Lemieszewski Ł., Ochin E. Cloud-based GNSS navigation spoofing detection. *Scientific Journals Maritime University of Szczecin*. 2019;(57):29–37. DOI: 10.17402/323.

23. Ochin E. Spoofing detection for underwater acoustic GNSS-like positioning systems. *Scientific Journals Maritime University of Szczecin*. 2019;(57):38–46. DOI: 10.17402/324.

24. Abramowski T., Bilewski M., Dobryakova L., Ochin E., Uriasz J., Zalewski P. Safety of GNSS-Like Underwater Positioning Systems. *Preprints*. 2019:2019090052. DOI: 10.20944/preprints201909.0052.v1.

Information about the author

Evgeny Ochin received the M.S. degree in 1969, the Ph.D. degree in 1974, and the Ph.D. Hub. degree in 1997 in ITMO University (Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Russia). From 1974 to 2004, he was an assisted professor and professor in the department of computer technology and vice-rector on scientific work at ITMO University. From 1996 to 2001, he was vice-rector on informatization of Baltic State Technical University "Voenmeh" D.F. Ustinov. From 2002 to 2008, he was director of the Institute "Architecture of Computers and Telecommunications" and head of the department "Computer networks" of Szczecin Technological University, Poland. From 2008 to 2019, he is a professor at the Maritime University in Szczecin, Faculty of Navigation, Department of Marine Information Technology, where he continues to work as Professor Emeritus. Evgeny Ochin is the author of 4 books, more than 160 articles, and more than 20 inventions. His research interests include CS&IT, the safety of satellite navigation on land, sea, and air, including anti-jamming and GNSS anti-spoofing, based on the inertial navigation system.

Информация об авторе

Очин Евгений получил звание инженера в 1969 г., к.т.н. в 1974 г. и д.т.н. в 1997 г. в Университете ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики). С 1974 по 2004 г. был доцентом и профессором на кафедре компьютерных технологий и проректором по научной работе в Университете ИТМО. С 1996 по 2001 г. был проректором по информатизации Балтийского государственного технического университета «Военмех» Д.Ф. Устинов. С 2002 по 2008 г. он был директором Института «Архитектура компьютеров и телекоммуникаций» и зав. каф. «Компьютерные сети» Щецинского технологического университета, Польша. С 2008 по 2019 г. является профессором Морского университета в Щецине, факультет навигации, кафедра морских информационных технологий, где и продолжает работать в качестве заслуженного профессора.Автор 4 книг, более 160 статей и более 20 изобретений. Его исследовательские интересы включают CS&IT, безопасность спутниковой навигации на суше, на море и в воздухе, включая защиту от помех и спуфинга ГНСС на основе инерциальной навигационной системы.

Поступила / Received: 11.07.2020
Принята в печать / Accepted: 25.07.2020