Article

Safety of GNSS-like underwater positioning systems

Tomasz Abramowski [1], Mateusz Bilewski [2], Larisa Dobryakova [3], Evgeny Ochin [4,*], Janusz Uriasz [5] and Paweł Zalewski [6]

The names of the authors are sorted alphabetically:

[1] Intergovernmental consortium InterOceanMetal Joint Organization, CEO, Szczecin, Poland; t.abramowski@am.szczecin.pl

[2] Maritime University of Szczecin, Faculty of Navigation, Szczecin, Poland; m.bilewski@am.szczecin.pl

[3] West Pomeranian University of Technology, Faculty of Computer Science and Information Technologies, Szczecin, Poland; ldobryakova@wi.zut.edu.pl

[4] Maritime University of Szczecin, Faculty of Navigation, Szczecin, Poland; e.ochin@am.szczecin.pl

[5] Maritime University of Szczecin, Faculty of Navigation, Szczecin, Poland; j.uriasz@am.szczecin.pl

[6] Maritime University of Szczecin, Faculty of Navigation, Szczecin, Poland; p.zalewski@am.szczecin.pl

* Correspondence: e.ochin@am.szczecin.pl; Tel.: +48 608 437 562

Abstract: The formal transfer of GNSS under water is not possible. It probably makes sense to talk only about the transformation of GPS into LPS, that is, in the Local Position System. However, the basic methods that are used to solve the problem of Spoofing Detection above water can be used under water. It should be understood that engineering problems are significantly different, since the nature of the propagation of acoustic waves in water and electromagnetic waves in the atmosphere are fundamentally different. In this article, we will limit the navigation with acoustically passive receiver. The receiver "listens" to the buoys and solves the problem of finding its own position based on the coordinates of the buoys (such systems are called GNSS-like Underwater Positioning Systems or GNSS-like UPS). Depending on the scale of system service areas, GNSS-like UPS are divided into global, regional, zonal and local system. In this article, we will limit ourselves to considering only local GNSS-like UPS. The acoustic signal generator transmits a signal simulation of several satellites. If the level of the simulated signal exceeds the signal strength of real satellites, the receiver of UPS will "capture" the fake signal and calculate the false position based on it.

Keywords: antiterrorism, underwater GNSS, underwater GPS, spoofer, antispoofing, spoofing detection, underwater transport safety

I. Introduction

The increased likelihood of terrorist acts led to the adoption in 2002 of Chapter XI-2 of the SOLAS-74 Convention and the International Ship and Port Facility Security Code (ISPS Code)[1]. In the 20th century electronic devices such as radar and Loran were widely adopted for use in navigation. Today most vessels use an automatic pilot, an electronic device for controlling a vehicle without constant human intervention. The use of GNSS (GPS Navstar, GLONASS, BejDou 2, GALILEO) has become standard in navigation.

There are many manufacturers of underwater positioning systems in the world including iXblue [1], EvoLogics [2], Sonardyne [3] and Charles Stark Draper Laboratory [4]. The Positioning System for Deep

[1] SOLAS XI-2 and the ISPS Code http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Ocean Navigation (POSYDON) program [5] aims to develop an undersea system that provides omnipresent, robust positioning across ocean basins.

Guided by sonar beacons located on the ocean bed, the robots will be able to accurately determine their own location down to millimeters and exchange data with air, water and ground-based control stations in real time. Buoys have three modes of operation. At the first, the product receives information via satellite communication channels, memorizes it and, at the request of the robot, transmits it. In the second mode - “dialogue” - the buoy connects the coastal, aerial, sea control centers with underwater robots over the VHF radio channel in real-time mode. Such data exchange allows not only knowing where the robot is and what tasks it solves, but also to continuously control it. The third mode is the easiest. The robot operates completely autonomously and only checks its coordinates with buoys, adjusting the course. In an emergency, the drone can give an SOS signal, reporting the termination of a deep-sea mission.

Note the four main methods used in determining underwater positioning, which largely coincide with the methods of measuring the coordinates of mobile objects in radio networks.

1. Received Signal Strength (RSS) – distance to the object is estimated by the power of the signal. This method works well at short distances.
2. Angle of Arrival (AoA) – the location of the object is determined within the area of a triangle formed by the intersection of the axes of the antenna patterns of the sectors of three base stations (modified trilateration method).
3. Round TripTime (RTT) – the object sends a signal to the transceiver and waits for a response. The half-difference between the time of sending a signal by an object and receiving a signal by an object multiplied by the speed of light gives the distance to the object.
4. Time of Arrival (ToA) is a technique, in which the time of arrival of a specific signal with precisely synchronized time of sent, are calculated (this method requires time synchronization at the sender and recipient).

II. The creation options of underwater acoustic GNSS-like positioning systems

A. Wire Buoyant GNSS UPS

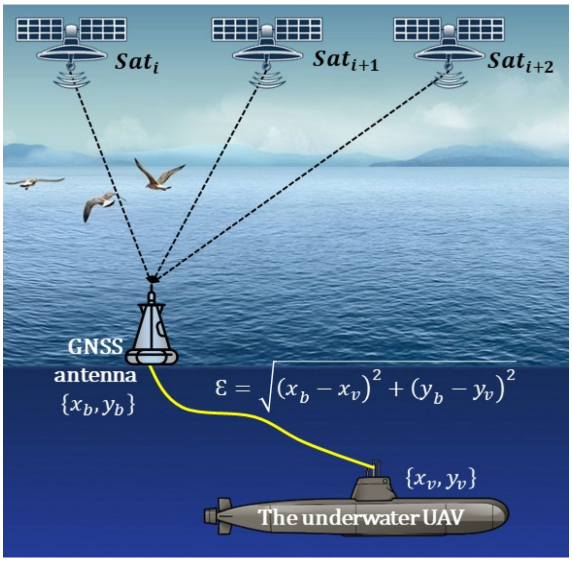


Figure 1. Wire buoyant GNSS UAV: Ɛ – position error

A GNSS receiver mounted on a buoy is towed on the surface by the underwater targets such as underwater vehicles (Fig. 1). This technique is named as wired underwater GNSS [8, 9]. Positioning accuracy determined by cable length, therefore, this type of positioning is sometimes called the “false” GNSS-like UPS [10].

B. Wireless Buoyant GNSS UPS

The wireless (acoustic) buoyant underwater GNSS (Fig. 2) also does not give the true position of the target. Positioning accuracy determined by the distance Underwater Positioning Systems from the buoy.

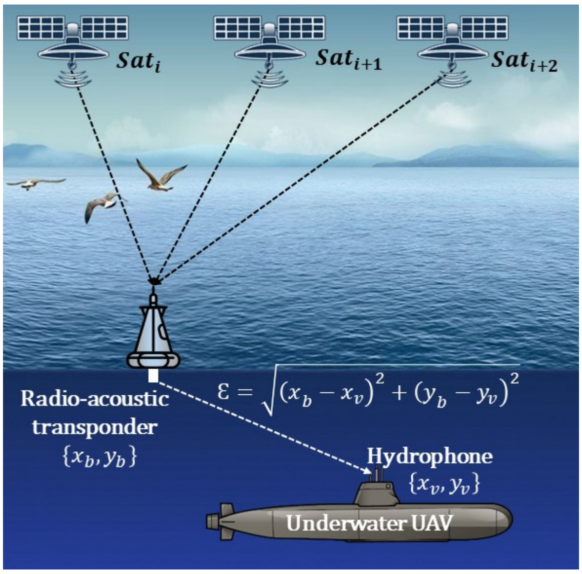


Figure 2. Wireless (acoustic) buoyant GNSS UAV

C. Direct GNSS-like UPS

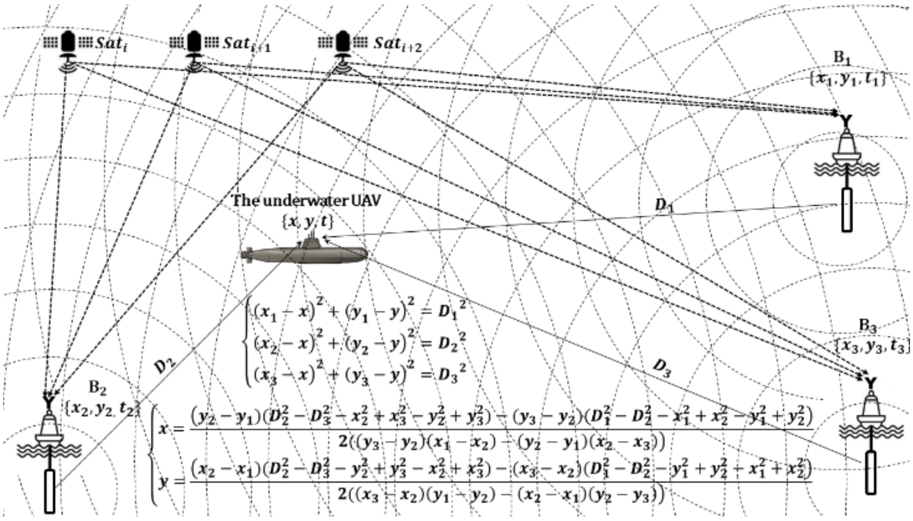
In 1992, Youngberg inspired a direct transposition of GNSS signal to underwater world [11-12](Fig. 3). Acoustic waves directly go from surface buoys replacing satellites to the underwater receivers. Then, the underwater platform computes its own position locally [13].

The surface buoys determines the XY coordinates (Z = 0) and time *T*, based on which the receiver of GNSS-like signals determines the own XYZ coordinates. In some applications for an underwater vessel, only the XY coordinates are significant, since the depth Z of the dive can be determined by a depth gauge, so we will focus only on the calculations of the XY coordinates.

In this case (2D) without loss of generality (3D) it can be shown that the system of equations (1)

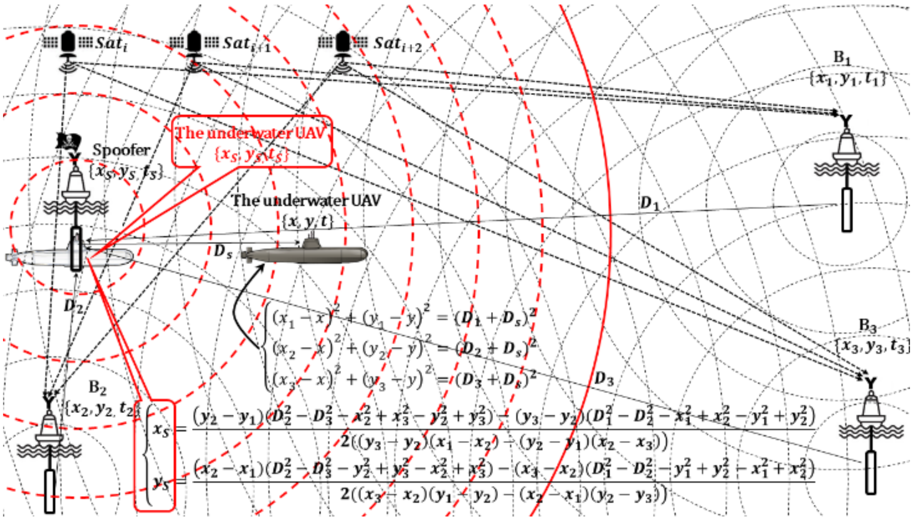
$$\begin{cases}(x_1 - x)^2 + (y_1 - y)^2 = D_1{}^2\\(x_2 - x)^2 + (y_2 - y)^2 = D_2{}^2\\(x_3 - x)^2 + (y_3 - y)^2 = D_3{}^2\end{cases} \quad (1)$$

describing the relationship of buoy coordinates and UAV coordinates has the following solution (2)



Sat_i
Sat_{i+1}
Sat_{i+2}
B$_1$ $\{x_1, y_1, t_1\}$
The underwater UAV $\{x, y, t\}$
D_1
D_2
D_3
B$_2$ $\{x_2, y_2, t_2\}$
B$_3$ $\{x_3, y_3, t_3\}$
$(x_1-x)^2+(y_1-y)^2=D_1^2$
$(x_2-x)^2+(y_2-y)^2=D_2^2$
$(x_3-x)^2+(y_3-y)^2=D_3^2$

Figure 3. Direct GNSS-like UPS: B$_1$, B$_2$ and B$_3$ – sonar transponders of GNSS signals (2D case simulation result



Sat_i
Sat_{i+1}
Sat_{i+2}
B$_1$ $\{x_1, y_1, t_1\}$
Spoofer $\{x_S, y_S, t_S\}$
The underwater UAV $\{x_S, y_S, t_S\}$
The underwater UAV $\{x, y, t\}$
D_1
D_S
D_2
D_3
B$_2$ $\{x_2, y_2, t_2\}$
B$_3$ $\{x_3, y_3, t_3\}$
$(x_1-x)^2+(y_1-y)^2=(D_1+D_S)^2$
$(x_2-x)^2+(y_2-y)^2=(D_2+D_S)^2$
$(x_3-x)^2+(y_3-y)^2=(D_3+D_S)^2$
x_S
y_S

Figure 4. The main strategy of spoofing (2D case simulation result):, D_1, D_2 *and* D_3 – the distances from a sonar transponders to spoofer; D_s – the distance from the spoofer to UAV; {x$_1$,y$_1$,t$_1$}, {x$_2$,y$_2$,t$_2$} and {x$_3$,y$_3$,t$_3$} – the coordinates of sonar transponders and the exact time received from navigation satellites; the red continuous circle shows the boundary of the effect of spoofing

$$\begin{cases} x = \dfrac{(y_2-y_1)(D_2^2-D_3^2-x_2^2+x_3^2-y_2^2+y_3^2)-(y_3-y_2)(D_1^2-D_2^2-x_1^2+x_2^2-y_1^2+y_2^2)}{2((y_3-y_2)(x_1-x_2)-(y_2-y_1)(x_2-x_3))} \\ y = \dfrac{(x_2-x_1)(D_2^2-D_3^2-y_2^2+y_3^2-x_2^2+x_3^2)-(x_3-x_2)(D_1^2-D_2^2-y_1^2+y_2^2-x_1^2+x_2^2)}{2((x_3-x_2)(y_1-y_2)-(x_2-x_1)(y_2-y_3))} \end{cases} \quad (2)$$

III. From TCP/IP spoofing to the underwater acoustic spoofing

The easiest way to mess with a GNSS receiver is to just put in radio interference or create a false noise signal (Jamming), which will be stronger than the real signal. However, in this case, the GNSS receiver simply stops working and the victim switches to INS positioning. In the more “intelligent” Spoofing, the victim does not know that the signal received by the GNSS receiver is incorrect. The spoofer creates a false signal and the victim determines the wrong time and location [14-20]. Initially, the term “spoofing” was used as a term for network security, implying the successful falsification of certain data in order to gain unauthorized access to a particular network resource (**Spoofing TCP/IP & UDP**). Over time, this term began to be used in other areas of information security:

- **Caller ID spoofing** – substitution of the calling phone number in VoIP-networks.

- **E-mail address spoofing** – substitution of the email address of the sender.
- **Extension Spoofing** – file extension spoofing.
- **File Name Spoofing** – clone of file name.
- **Source Code Spoofing** – substitution of page content and source code.
- **GNSS Spoofing** – substitution of navigation data from satellites in order to deceive the victim. Initially, the spoofer sends the correct coordinates, but gradually rejects the signal to the side. Doing this slowly is necessary so that the GNSS receiver does not block all signals due to an abrupt change in location.
- **Underwater Spoofing** – formally, it is not much different from telecommunications spoofing. The principal difference is the use of acoustic signals, often for military applications (Mortimer, 2016).
- **Underwater GNSS Spoofing** – substitution of navigation data from surface radio-acoustic or underwater acoustic buoys in order to deceive the victim. Spoofer can be a surface or underwater manned or unmanned vehicle.

Notations and definitions

$z_0(x, y)$ – the known depth.

$B_i \to \{x_i, y_i, z_i\}$, $i = \overline{1, N}$ – buoys of GNSS-like UPS.

$\{x_v, y_v, z_v\}$ – coordinates, measured by the victim.

$\{\tilde{x}_v, \tilde{y}_v, \tilde{z}_v\}$ – coordinates, measured by the spoofer.

$\{\Delta x_v, \Delta y_v, \Delta z_v\}$ – amendment of victim's coordinates.

$T_i = (t_i^{arrival} - t_i^{sent})$ – the measured signal's propagation time from the buoy B_i to the spoofer.

The main strategy of the underwater spoofing

At the moment of the victim's capture, the false coordinates coincide with the real ones and then simulate the movement of the victim along a certain trajectory. As a spoofer, we will use an acoustic signal repeater (highlighted in red). It can be shown that by solving the system of equations

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

by analogy with (2) are the coordinates of the spoofer $\{x_S, y_S\}$. In this case, the system of equations

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

describing the relationship between the coordinates of buoys, the repeater of acoustic signals and the coordinates of the UAV has the only solution (4) **under the condition $D_s = 0$** (Fig. 5), that is, all the UAVs that are in the range of the spoofer (acoustic repeater) define their coordinates as (x_S, y_S).

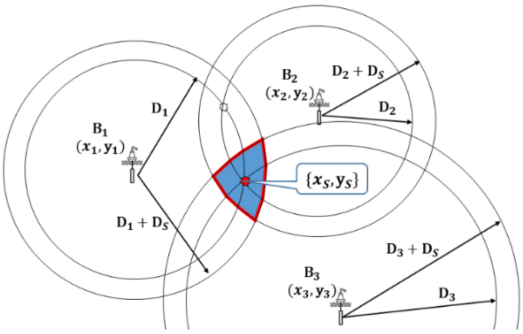


Figure 5. The relationship of the coordinates of the buoys, the spoofer (follower of acoustic signals) and the coordinates of the UAV has a unique solution (2) under the condition $D_s = 0$

IV. The underwater UAV trajectory examples

The motion's law of the mass center of a UAV in general may be represented by the system of two equations

$$\begin{cases} x = x(t) \\ y = y(t) \end{cases} \tag{5}$$

The UAV autopilot implements the discrete path calculation process (Fig. 6)

$$\begin{cases} x_{i+1} = x_i + \Delta x_i \\ y_{i+1} = y_i + \Delta y_i \end{cases} \tag{6}$$

where $\{x_i, y_i\}$ − current position of the mass center of the UAV; $\{\Delta x_i, \Delta y_i\}$ − estimated route correction values.

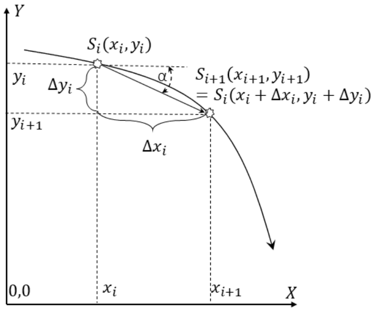


Figure 6. Estimated route correction values

To reach the point $\{x_{i+1}, y_{i+1}\}$ UAV moves at an angle

$$\alpha = arctan\frac{y_{i+1} - y_i}{x_{i+1} - x_i}, -\pi \le \alpha \le \pi \tag{7}$$

Moving the mass center of the UAV from the position $\{x_i, y_i\}$ in position $\{x_{i+1}, y_{i+1}\}$ accompanied by random deviations from the route $\{\mathcal{E}x_i, \mathcal{E}y_i\}$, i.e

$$\begin{cases} x_{i+1} := x_{i+1} + \mathcal{E}x_i \\ y_{i+1} := y_{i+1} + \mathcal{E}y_i \end{cases} \tag{8}$$

Suppose a UAV performs underwater circulation of a radius $R = 1000\, m$ with speed $V_{UAV} = 16\, km/h$ with discretization on time $\Delta t = 60\, sec$. In this case

$$\begin{cases} x_{i+1} = x_i + V_{UAV}\Delta t cos\alpha + \aleph_i x_i/100 \\ y_{i+1} = y_i + V_{UAV}\Delta t sin\alpha + \aleph_i y_i/100 \end{cases} \tag{9}$$

where $\aleph_i$ − random number uniformly distributed in the interval [0÷1].

When the acoustic signal is low, the circulation is performed normally (Fig. 7). As the power of the acoustic signal increases, a truncated (limited) circulation is performed (Fig. 8).

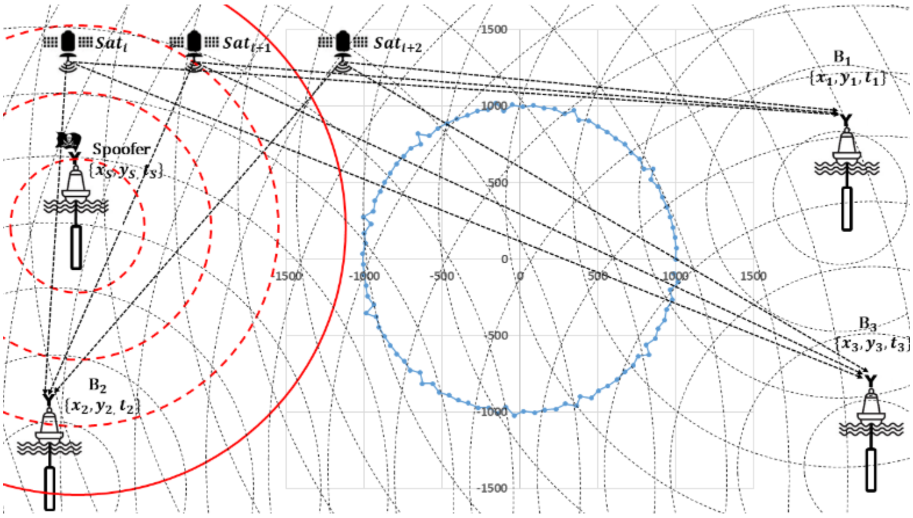


Figure 7. Normal circulation of UAV (2D case simulation result); $\{x_S, y_S\} = \{-3000\ m, 200\ m\}$; the red continuous circle with radius 1900 m shows the boundary of the effect of spoofing. On the UAV movement trajectory (marked in blue), we see the divergence of the one-step calculated and observational coordinates of the UAV in normal driving. The direction of the discrepancy is determined from the calculated UAV location to the observational coordinates.

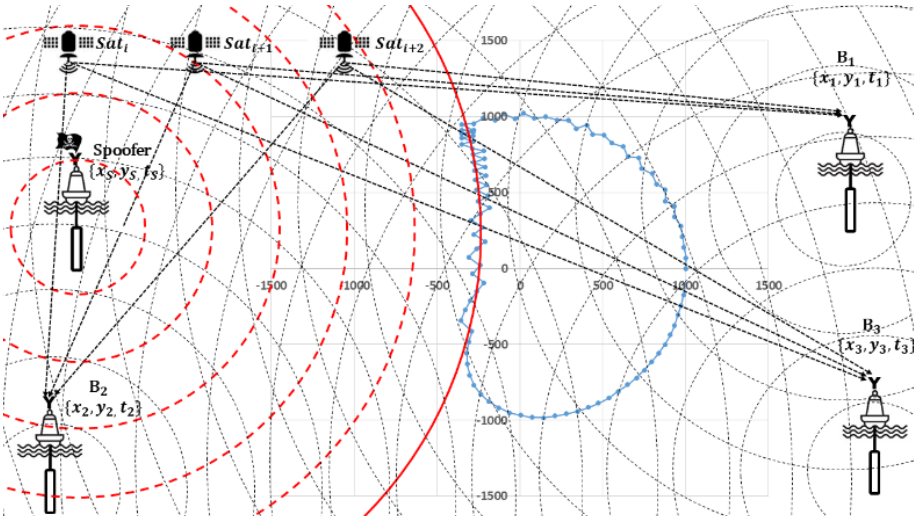


Figure 8. Truncated (restricted) circulation of UAV as a result of spoofing (2D case simulation result); $\{x_S, y_S\} = \{-3000\ m, 200\ m\}$; the red continuous circle with radius 2800 m shows the boundary of the effect of spoofing. On the UAV movement trajectory (marked in blue), we see the divergence of the one-step calculated and observational coordinates of the UAV in the spoofing mode.

V. The underwater acoustic GNSS-like positioning of a spoofer and a victim

Solving the system of equations (1) allows us to calculate the victim's coordinates

$$\{x_v, y_v, z_v\} = \sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} \approx cT_i, \quad i = \overline{1, N} \tag{10}$$

where T_i – measured propagation time of a real signal from a buoy B_i to the victim.

The system of equations (10) is written as

$$\varepsilon(x_v, y_v, z_v) = \sum_{i=1}^{N} \left(\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} - cT_i \right) \tag{11}$$

In the general case, the solution (11) is carried out by numerical methods of minimization (12):

$$\{x_v, y_v, z_v\} = \arg \min_{x_v, y_v, z_v} \varepsilon(x_v, y_v, z_v) \tag{12}$$

To determine $\{x_v, y_v, z_v\}$, there is enough data from three buoys, however, as the software simulation of GNSS-like UPS shows, due to the approximate nature of the measurement of pseudoranges ($\rho_i \approx cT_i$, $i = \overline{1, N}$) the positioning accuracy $\{x_v, y_v, z_v\}$ will depend on the number of buoys N.

If the victim uses a barometric depth gauge for determining z_v, the system of equations (1) takes the form

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2} \approx cT_i, \quad i = \overline{1, N} \tag{13}$$

In this case, the solution (4) is carried out as

$$\{x_v, y_v\} = \arg \min_{x_v, y_v} \left[\sum_{i=1}^{N} \left(\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2} - cT_i \right) \right] \tag{14}$$

Solving the system of equations (15) allows us to calculate the spoofer's coordinates $\{x_s, y_s\}$.

$$\{x_s, y_s\} = \arg \min_{x_s, y_s} \left[\sum_{i=1}^{N} \left(\sqrt{(x_i - x_s)^2 + (y_i - y_s)^2} - cT_i \right) \right] \tag{15}$$

To determine the coordinates $\{x_s, y_s\}$ there is enough data from three buoys or three GNSS satellites if the spoofer is on the surface of the sea.

Suppose we know the victim's coordinates $\{x_v, y_v, z_v\}$, for example, using a sonar range finder and a measured direction to the victim. If the victim does not use barometric depth gauge for determining z_v, then in this case it is possible to determine the corrections ΔT_i for measured time T_i so that the receiver of the victim would calculate the fake coordinates equal to the true ones (16).

$$\{x_v, y_v, z_v\} = \arg \min_{x_v, y_v, z_v} \left\{ \sum_{i=1}^{N} \left(\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} - (cT_i + \Delta T_i) \right. \right\} \tag{16}$$

If the power of the spoofer's signal exceeds the power of the buoys signals, the victim's receiver switches to receiving a false signal. Further, the spoofer applies an escaping spoofing strategy in accordance with the equation system

$$\sqrt{\left[x_i - (x_v + \Delta x_v)\right]^2 + \left[y_i - (y_v + \Delta y_v)\right]^2 + (z_v + \Delta z_v)^2} \approx cT_i + \Delta T_i, \quad i = \overline{1, N}, \tag{17}$$

where $\{\Delta x_v, \Delta y_v, \Delta z_v\}$ – amendment of victim's coordinates, taking away the victim from its route. In this situation, the spoofer is in an active state on the sea surface and the values $z_i = 0$, i.e. correspond to zero sea level.

The algorithm of finding ΔT_i, $i = \overline{1, N}$ with given vectors $\{x_v, y_v, z_v\}$ and $\{\Delta x_v, \Delta y_v, \Delta z_v\}$ this article is not considered.

VI. Spoofing detection using a single hydrophone

In two next sections, we will mainly follow the results obtained in [15, 16, 20] and own research results [17-19, 21] and will discuss the two methods of spoofing detection:

1) the method of measuring coordinates of a moving victim at two points on the route using a single hydrophone (in this case we use a conventional hydrophone, that is, the problem of practical implementation of spoofing detection of GNSS-like UPS is reduced only to programming);
2) the method of measuring coordinates of a victim at two points of space using a dual hydrophone.

We install a fixed single hydrophone on the spoofing detector. **Note that the victim may be in motion.**

A. The measurement of spacing between two positions of the single hydrophone in navigation mode

The spoofing detector measures the coordinates of the hydrophone *H*, **based on real signal from buoys**:

$$\left\{\hat{x}_{v'},\hat{y}_{v'},\hat{z}_{v'}\right\}=\arg\min_{x_{v'},y_{v'},z_{v'}}\left\{\sum_{i=1}^{N}\left(\sqrt{\left(x_i-x_{v'}\right)^2+\left(y_i-y_{v'}\right)^2+\left(z_i-z_{v'}\right)^2}-cT_i\right)\right\} \tag{18}$$

where ($x_{v'}$, $y_{v'}$, $z_{v'}$) – unknown precise coordinates of the hydrophone *H* at the time *t′*, $(\hat{x}_{v'},\hat{y}_{v'},\hat{z}_{v'})$ – calculated coordinates of the hydrophone *H* at the time *t′*.

The spoofing detector again measures the XYZ of the hydrophone *H* at the time *t″*:

$$\left\{\hat{x}_{v''},\hat{y}_{v''},\hat{z}_{v''}\right\}=\arg\min_{x_{v''},y_{v''},z_{v''}}\left\{\sum_{i=1}^{N}\left(\sqrt{\left(x_i-x_{v''}\right)^2+\left(y_i-y_{v''}\right)^2+\left(z_i-z_{v''}\right)^2}-cT_i\right)\right\} \tag{19}$$

where ($x_{v''}$, $y_{v''}$, $z_{v''}$) – unknown precise coordinates of the hydrophone *H* at the time *t″*, $(\hat{x}_{v''},\hat{y}_{v''},\hat{z}_{v''})$ – calculated coordinates of the hydrophone *H* at the time *t″*.

The measured distance between the hydrophone at the times *t′* and *t″*

$$\hat{D}_{1-2}=\sqrt{\left(\hat{x}_{v'}-\hat{x}_{v''}\right)^2+\left(\hat{y}_{v'}-\hat{y}_{v''}\right)^2+\left(\hat{z}_{v'}-\hat{z}_{v''}\right)^2} \tag{20}$$

must be commensurate with the distance traveled by the vehicle over time (*t″* – *t*), i.e.

$$\hat{D}_{1-2}\approx V\left(t''-t'\right) \tag{21}$$

B. The measurement of spacing between two positions of the single hydrophone in spoofing mode

The spoofing detector measures the coordinates of the hydrophones *H*, **based on false signal from spoofer**:

$$\left\{\hat{x}_{v'},\hat{y}_{v'},\hat{z}_{v'}\right\}=\arg\min_{x_{v'},y_{v'},z_{v'}}\left\{\sum_{i=1}^{N}\left(\sqrt{\left(x_i-x_{v'}\right)^2+\left(y_i-y_{v'}\right)^2+\left(z_i-z_{v'}\right)^2}-cT_i\right)\right\} \tag{22}$$

where ($x_{v'}$, $y_{v'}$, $z_{v'}$) – unknown precise coordinates of the hydrophone *H* at the time *t′*, $(\hat{x}_{v'},\hat{y}_{v'},\hat{z}_{v'})$ – calculated coordinates of the hydrophone *H* at the time *t′*.

The spoofing detector again measures the XYZ of the hydrophone *H* at the time *t″*

$$\left\{\hat{x}_{v''},\hat{y}_{v''},\hat{z}_{v''}\right\}=\arg\min_{x_{v''},y_{v''},z_{v''}}\left\{\sum_{i=1}^{N}\left(\sqrt{\left(x_i-x_{v''}\right)^2+\left(y_i-y_{v''}\right)^2+\left(z_i-z_{v''}\right)^2}-cT_i\right)\right\} \tag{23}$$

where ($x_{v''}$, $y_{v''}$, $z_{v''}$) – unknown precise coordinates of the hydrophone *H* at the time *t″*, $(\hat{x}_{v''},\hat{y}_{v''},\hat{z}_{v''})$ – calculated coordinates of the hydrophone *H* at the time *t″*.

The measured distance between the hydrophone *H* at the time *t′* and the hydrophone Y at the time *t″*

$$\hat{D}_{1-2}=\sqrt{\left(\hat{x}_{v'}-\hat{x}_{v''}\right)^2+\left(\hat{y}_{v'}-\hat{y}_{v''}\right)^2+\left(\hat{z}_{v'}-\hat{z}_{v''}\right)^2}\approx 0 \tag{24}$$

because all hydrophones in the spoofing zone calculate the same false coordinates and $\hat{D}_{1-2}$ must be incommensurable with the distance traveled by the vehicle over time (*t″* – *t′*), i.e.

$$\hat{D}_{1-2}<<V\left(t''-t'\right) \tag{25}$$

C. The decisive rule

Comparing (24) and (25), we can write down the decisive rule for detecting spoofing

$$\text{if } \hat{D}_{1-2}\le\breve{D} \text{ then go to Spoofing,} \tag{26}$$

where $\breve{D}$ – discriminant, determined on the basis of statistical studies at the stage of designing a real detection system. At present, we are carrying out theoretical studies and relevant real sea tests at various speeds V and various values $\Delta t = (t'' - t')$ in order to find acceptable values $\breve{D}$.

Note that the spoofing detector may be in motion. During the time $\Delta t = (t'' - t')$, the parameters of the spoofer's signals may change, therefore solving the problem of optimizing the parameters of the spoofing detector, it is necessary to minimize the parameter Δt. From the point of view of detecting spoofing, it is necessary to maximize the parameter Δt. To resolve this contradiction, minimax methods of parametric optimization are used [22]. Minimax is a kind of backtracking algorithm that is used in decision making and game theory to find the optimal move for a player, assuming that your opponent also plays optimally. It is widely used in two player turn-based games such as Tic-Tac-Toe, Backgammon, Mancala, Chess, etc.

VII. Spoofing detection using a dual hydrophone

We install a fixed two hydrophones H' and H'' on the spoofing detector at distance D from each other. **Note that the spoofing detector may be in immobile or in motion.**

The measurement the distance between hydrophones in navigation mode

The spoofing detector measures the coordinates of the hydrophone H':

$$\{\hat{x}_{v'},\hat{y}_{v'},\hat{z}_{v'}\} = \arg\min_{x_{v'},y_{v'},z_{v'}} \left\{\sum_{i=1}^{N}\left(\sqrt{(x_i-x_{v'})^2+(y_i-y_{v'})^2+(z_i-z_{v'})^2}-cT_i\right)\right\} \tag{27}$$

where $(x_{v'}, y_{v'}, z_{v'})$ – unknown precise coordinates of the hydrophone H', $(\hat{x}_{v'},\hat{y}_{v'},\hat{z}_{v'})$ – calculated coordinates of the hydrophone H'.

The spoofing detector measures the coordinates of the hydrophone H'':

$$\{\hat{x}_{v''},\hat{y}_{v''},\hat{z}_{v''}\} = \arg\min_{x_{v''},y_{v''},z_{v''}} \left\{\sum_{i=1}^{N}\left(\sqrt{(x_i-x_{v''})^2+(y_i-y_{v''})^2+(z_i-z_{v''})^2}-cT_i\right)\right\} \tag{28}$$

where $(x_{v''}, y_{v''}, z_{v''})$ – unknown precise coordinates of the hydrophone H'' at the time t', $(\hat{x}_{v''},\hat{y}_{v''},\hat{z}_{v''})$ – calculated coordinates of the hydrophone H''.

The measured distance between H' and H'' is

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{v'}-\hat{x}_{v''})^2+(\hat{y}_{v'}-\hat{y}_{v''})^2+(\hat{z}_{v'}-\hat{z}_{v''})^2}\approx D \tag{29}$$

where D – the real distance between hydrophones.

A. The measurement the distance between hydrophones in spoofing mode

Because all hydrophones in the spoofing zone calculate the same false coordinates the equation (29) takes the form

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{v'}-\hat{x}_{v''})^2+(\hat{y}_{v'}-\hat{y}_{v''})^2+(\hat{z}_{v'}-\hat{z}_{v''})^2}\approx 0. \tag{30}$$

B. The decisive rule

Comparing (29) and (30), we can write down the decisive rule for detecting spoofing

$$\text{if } \hat{D}_{1-2}\le\breve{D} \text{ then go to Spoofing,} \tag{31}$$

where $\breve{D}$ – discriminant, determined on the basis of statistical studies at the stage of designing a real detection system.

VIII. Conclusions

The formal transfer of GNSS under water is not possible. It probably makes sense to talk only about the transformation of GPS into LPS, that is, in the Local Position System. However, the basic methods that are used to solve the problem of **Spoofing Detection** above water can be used under water. It should be understood that engineering problems are significantly different, since the nature of the propagation of acoustic waves in water and electromagnetic waves in the atmosphere are fundamentally different.

References

[1] EvoLogics, Underwater Acoustic LBL Positioning Systems, 2018 // https://evologics.de/underwater-positioning [Accessed: January 5, 2019]

[2] Sonardyne, Subsea technology for energy, science and security // https://www.sonardyne.com [Accessed: January 5, 2019]

[3] BAE Systems (2016) Undersea navigation and positioning system development to begin for U.S. Navy. // https://www.baesystems.com/en-us/what-we-do/cyber-security---intelligence [Accessed: January 5, 2019]

[4] N. Lavars, DARPA program plunges into underwater positioning system. [Online] 23 May 2016. Available from: https://newatlas.com/darpa-underwater-navigation/43472/ [Accessed: January 5, 2019]

[5] J. Waterston, Positioning System for Deep Ocean Navigation (POSYDON) https://www.darpa.mil/program/positioning-system-for-deep-ocean-navigation

[6] K. Osborn, DARPA Discovers "GPS-Like" undersea drone connectivity, Feb 14, 2017 // https://defensesystems.com/articles/2017/02/14/darpauuv.aspx

[7] Russian Underwater Communications and Navigation System to be Deployed on Arctic Shelf, December 13, 2016 // https://www.ecomagazine.com/news/industry/russian-underwater-communications-and-navigation-system-to-be-deployed-on-arctic-shelf [Accessed: January 5, 2019]

[8] H. Kaushal, G. Kaddoum Underwater Optical Wireless Communication // https://ieeexplore.ieee.org/document/7450595 [Accessed: January 5, 2019]

[9] Semenov, D., and others, How to get coordinates of underwater objects by using UV-light identification devices, (2017) https://findpatent.ru/patent/262/2626244.html [Accessed: January 5, 2019]

[10] Scuba Diving Chicago, Underwater Vehicles, 18 Apr 2013 Underwater GPS navigation // https://www.scubadivingchicago.us/underwater-vehicles/underwater-gps-navigation.html [Accessed: January 5, 2019]

[11] H.G. Thomas, GIB buoys: an interface between space and depths of the oceans. Proceedings of the 1998 Workshop on Autonomous Underwater Vehicles, 21 Aug. 1998, pp. 181–184. Available from: https://ieeexplore.ieee.org/abstract/document/744453 [Accessed: January 5, 2019]

[12] Hubert, T. Method and device for the monitoring and remote control of unmanned, mobile underwater vehicles. United States Patent 5,579.285, (1966) https://patents.google.com/patent/US5579285A/en [Accessed: January 5, 2019]

[13] J.W. youngberg, A Novel Method for Extending GPS to Underwater Applications. Navigation 38, 1991, pp. 263–271.

[14] M. Caparrini, A. Egido, F. Soulat, O. Germain, E. Farres, S. Dunne & G. Ruffini, Oceanpal®: monitoring sea state with a GNSS-R coastal instrument. Paper presented at the International Geoscience and Remote Sensing Symposium. IEEE, Barcelona, Spain, 23–28 July 2007, doi:10.1109/IGARSS.2007.4424004

[15] T.E. Humphreys, B. M. Ledvina, M.L Psiaki, B.W. O'hanlon, & P.M. Jr. Kintner, Assessing the Spoofng Threat: Development of a Portable GNSS Civilian Spoofer. Preprint of the 2008 IONGNSS Conference Savanna, GA, Septemb. 16–19, 2008.

[16] Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. & Lachapelle, G. (2012) GNSS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. Hindawi Publishing Corporation International Journal of Navigation and Observation 2012, Article ID127072, doi: 10.1155/2012/127072.

[17] L. Dobryakova, Ł. Lemieszewski, and E. Ochin, Antiterrorism – design and analysis of GNSS antispoofing algorithms. Scientific Journals Maritime University of Szczecin, 30(102), 2012, pp. 93–101.

[18] L. Dobryakova, Ł. Lemieszewski, and E. Ochin, The analysis of the detecting algorithms of GNSS-spoofing. Scientific Journals of the Maritime University of Szczecin 36(108) 2013 z. 2, pp. 30–36.

[19] L. Dobryakova, Ł. Lemieszewski, E. Lusznikov and E. Ochin, The study of the spoofer's some properties with help of GNSS signal repeater. Scientific Journals of the Maritime University of Szczecin 36 (108) 2013 z.2, pp. 159–165.

[20] P. Zalewski, Real-time GNSS spoofing detection in maritime code receivers. 2014, 38(110) pp. 118–124

[21] L. Dobryakova, Ł. Lemieszewski, and E. Ochin, Design and Analysis of Spoofing Detection Algorithms for GNSS Signals. Scientific Journals of the Maritime University of Szczecin 40 (112), 2014 pp. 47–52.

[22] M. Ehrgott, J. Ide & A. Schöbel, Minmax robustness for multi-objective optimization. European Journal of Operational Research 239, 1, 2014, pp. 17–31.

[23] International Maritime Organization. "December 2000 amendments" // https://clck.ru/GwEbz [Accessed: January 5, 2019]

[24] Federal Standard 1037C, August 7, 1996: transducer// https://www.its.bldrdoc.gov/fs-1037/dir-037/_5539.htm [Accessed: January 5, 2019]