Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2019, 57 (129), 38–46
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)
DOI: 10.17402/324

Received: 21.01.2019
Accepted: 14.02.2019
Published: 22.03.2019

Spoofing detection for underwater acoustic GNSS-like positioning systems

Evgeny Ochin

Maritime University of Szczecin, Faculty of Navigation
1–2 Wały Chrobrego St., 70-500 Szczecin, Poland, e-mail: ochin@am.szczecin.pl

Key words: antiterrorism, GNSS, spoofer, antispoofing, spoofing detection algorithm, underwater vehicle, underwater transport safety, acoustic communication

Abstract

The need for accuracy, precision, and data registration in underwater positioning and navigation should be viewed as no less stringent than that which exists on the sea surface. In the same way in which GNSS (Global Navigation Satellite System) receivers rely on the signals from multiple satellites to calculate a precise position, undersea vehicles discern their location by ranging to the acoustic signals originating from several fixed underwater acoustic sources using the Time-of-Arrival algorithm (ToA) through the Ordinary Least Squares method (OLS). In this article, the scope has been limited to only considering underwater positioning systems in which the navigation receiver is acoustically passive. The receiver "listens" to the buoys, receives their messages and solves the problem of finding its own position based on the geographical coordinates of the buoys. Often, such systems are called GNSS-like Underwater Positioning Systems (GNSS-like UPS). It is important to note the distinction between general purpose GNSS-like UPS (mainly civil systems) and special purpose GNSS-like UPS (mainly military systems). In this article, only general purpose GNSS-like UPS systems have been considered. Depending on the scale of system's service areas, GNSS-like UPS are divided into global, regional, zonal and local systems. Only local GNSS-like UPS systems have been considered in this article.

The spoofing of acoustic GNSS-like UPS works as follows: the acoustic GNSS signal generator transmits a simulated signal of several satellites. If the level of the simulated signal exceeds the signal strength of the real satellites, the acoustic receiver of an underwater object will "capture" the fake signal and calculate a false position based on it. All receivers that fall into the spoofing zone will calculate the same coordinates, while the receivers located in different places will have a mismatch in the XYZ coordinates.

Introduction

Marine surface and underwater floating tools can solve many positioning problems:

- positioning of drilling ships,
- positioning while loading at sea,
- positioning the laying of cables and pipelines,
- ensuring diving works,
- detection of gas leaks, etc.

There are many manufacturers of underwater positioning systems in the world (ROV, 2018), including HiPAP® – High Precision Acoustic Positioning (Kongsberg Maritime, 2016), iXblue (iXblue, 2018), EvoLogics (EvoLogics, 2018) Sonardyne (Sonardyne, 2018) etc. It is necessary to highlight the promising design programs of three companies: DARPA (Defense Advanced Research Projects Agency), BAE Systems (British Aerospace) and the Charles Stark Draper Laboratory (Figure 1) (BAE Systems, 2016).

DARPA has enlisted the services of BAE Systems, along with the not-for-profit research company Draper, to develop a system that will allow for GNSS-like precision underwater. The program is called the Positioning System for Deep Ocean Navigation (POSYDON) and, if all goes to plan, it will allow the navy's submersibles to remain concealed under the ocean while accurately navigating.

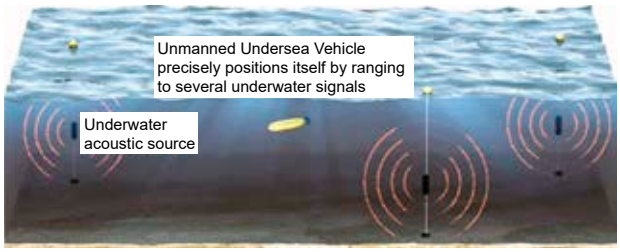

Figure 1. DARPA, BAE Systems and Draper are developing undersea positioning technology that will make use of long-range acoustic sources at fixed locations in the ocean (Lavars, 2016)

This system uses buoys that act as roving pseudolites and translate the GNSS service to an acoustic-based service under water. In the same way that GNSS receivers rely on the signals from multiple satellites to calculate a precise position, the undersea vehicles discern their location by ranging to the acoustic signals from several of the fixed underwater acoustic sources.

In this article, the scope has been limited to considering only those underwater positioning systems in which the navigation receiver is acoustically passive. The receiver "listens" to the buoys, receives their messages and solves the problem of finding its own position based on the geographical coordinates of the buoys. Often, such systems are called GNSS-like underwater positioning systems (GNSS-like UPS).

It is important to note the distinction between general purpose GNSS-like UPS and special purpose GNSS-like UPS. In this article, only general purpose GNSS-like UPS has been considered.

Depending on the scale of the system's service areas, GNSS-like UPS is divided into global, regional, zonal and local systems. In this article, only local GNSS-like UPS systems have been considered.

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, should be noted:

1. Received Signal Strength (**RSS**) – the distance to the object is estimated from the power of the signal. This method works well over 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 triangulation 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 to an object and receiving a signal from an object multiplied by the speed of light gives the distance to the object.
4. Time of Arrival (**ToA**) – a technique in which the time of arrival of a specific signal, which is precisely synchronized with the time of origin, is calculated (**this method requires time synchronization between the sender and recipient**).

The creation options of underwater acoustic GNSS-like positioning systems

A. Wire GNSS-like UPS

The first type is wired or buoyant underwater GNSS. A GNSS receiver mounted on a buoy is towed on the surface by underwater targets such as underwater vehicles (Figure 2). A cable or fiber is used to send the GNSS position to the underwater target. This technique does not give the true position of the target but the false position even within a few tens of meters around the surface buoy, so that it is called a wired underwater GNSS (Kaushal & Kaddoum, 2016). Positioning accuracy is determined by cable length; therefore, this type of positioning is sometimes called "false" GNSS-like UPS (Scuba Diving Chicago, 2013).

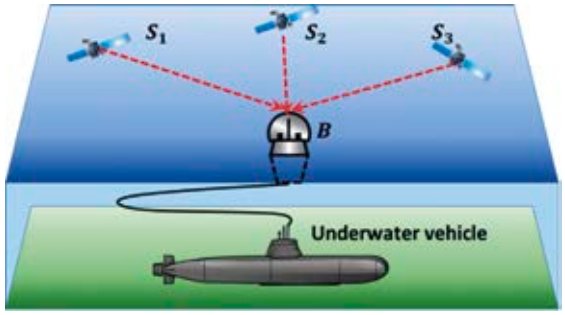

Figure 2. Wire GNSS-like UPS; S_1, S_2 and S_3 – satellites of GNSS; B – floating GNSS antenna of an underwater vehicle

B. Direct GNSS-like UPS

The second type is a "direct" underwater GNSS solution (Figure 3). In 1992, Youngberg inspired the direct transposition of a GNSS signal to the underwater world (Thomas, 1998). Acoustic waves but not radio electrical signals directly go from the surface buoys that are replacing the satellites to the underwater mobile units (receivers). Then, the underwater platform receives these acoustic messages from the buoys equipped with GNSS receptors and computes its own position. M. Youngberg of the US-AIR FORCE patented and published this solution (Youngberg 1991).

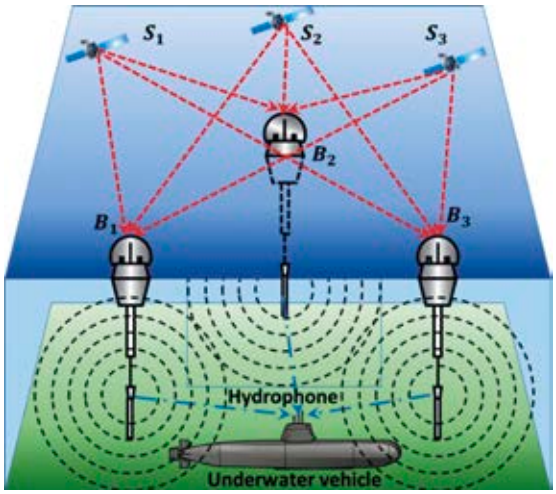

Figure 3. Direct GNSS-like UPS: S_1, S_2 and S_3 – satellites of GNSS; B_1, B_2 and B_3 – sonar transponders of the GNSS signals

The surface buoys determine the XY coordinates (Z = 0) and time *T*, based on which the receiver of the GNSS-like signals then determines its 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 the calculations of the XY coordinates have been solely focussed on in this paper.

C. Reverse GNSS-like UPS

The third type is very similar to the second type of solution, but it is a "reverse" underwater GNSS solution. This method has been recently investigated by Hubert Thomas (Hubert, 1966) and is available commercially: the so-called GNSS Intelligent Buoy (GIB) system, developed by ACSA in 1999. This system is designed to track the position of an underwater target, equipped with an acoustic emitter, by measuring the times of arrival of the acoustic signals at a set of surface buoys equipped with submerged hydrophones and GNSS receivers.

Each buoy has a GNSS receiver, a clock synchronized with a GNSS clock, a sonar receiving system with a recessed transducer, and a radio modem (GIB technology – Global Intelligent Buoy). Each buoy measures its own coordinates and lag times at predetermined times and transmits them along with the coordinates in the NMEA standard via radio modem to the vessel. According to the data of the received delay times of the pinger signals, and taking into account the speed of sound in water, the distances from the underwater object to each of the buoys can be calculated on board the vessel. The coordinates of the underwater object and all the buoys are then calculated and displayed using an algorithm (Hubert, 1966).

In this article, the scope has been limited to direct underwater acoustic GNSS-like positioning systems.

From TCP/IP spoofing to underwater spoofing

The easiest way to interfere with a GNSS receiver is to just generate radio interference or create a false noise signal (Jamming), which is stronger than the real signal. However, in this case, the GNSS receiver will simply stop working and the victim will switch to INS positioning.

In the more "intelligent" Spoofing technique, the victim does not know that the signal received by the GNSS receiver is incorrect. The spoofer creates a false signal and thus the victim determines the wrong time and location.

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** –cloning the file name.
- **Source Code Spoofing** – substitution of page content and the 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. The spoofer can be a surface or underwater manned or unmanned vehicle.

Underwater acoustic GNSS-like positioning systems remain the predominant navigation solution for both commercial and military underwater applications. However, proven threats to GNSS-like UPS

from jamming, spoofing, and environmental blockages have convinced the military that, as well as many commercial technology firms, now is the time to find new navigation solutions that can enhance the security of GNSS-like UPS.

The main strategy of spoofing is as follows. A developed spoofer simulates the GNSS-like UPS signals in such a way that 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 (Figure 4).

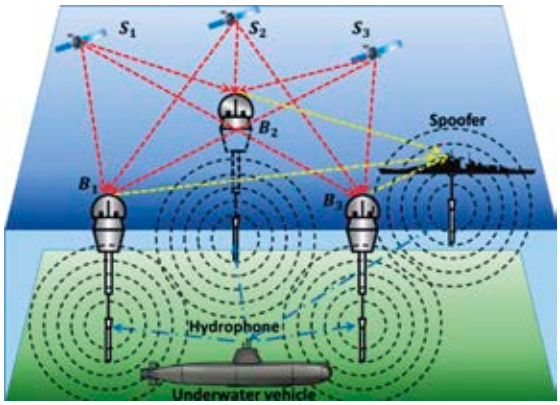

Figure 4. The main strategy of spoofing: S_1, S_2 and S_3 – satellites of GNSS; B_1, B_2 and B_3 – sonar transponders of GNSS signals

There are two strategies for underwater spoofing:
- spoofing based on receiving GNSS signals from navigation satellites,
- spoofing based on receiving acoustic signals from navigation buoys.

In this article, the scope has been limited to receiving acoustic signals from navigation buoys.

Notations and definitions

$z_0(x, y)$ – the known depth of the sea at the point (x, y).
$B_i \rightarrow \{x_i, y_i, z_i\}$, $i = \overline{1, N}$ – buoys of GNSS-like UPS, N – the number of buoys.
Acoustic Spoofing – an attack on a GNSS-like UPS, in an attempt to deceive the victim's receiver by transmitting powerful false signals that mimic the signals from the true GNSS-like UPS, exceeding the power of the true signal.
Acoustic Spoofer – special purpose computer, radio and acoustic equipment for the implementation of acoustic spoofing.
$\{x_s, y_s\}$ – spoofer's XY coordinates ($z_s = 0$, because in this article, the scope has been limited to surface spoofers only).
$\{x_v, y_v, z_v\}$ – victim's XYZ coordinates, as measured by the victim.
$\{\tilde{x}_v, \tilde{y}_v, \tilde{z}_v\}$ – victim's XYZ coordinates, as measured by the spoofer.
$\{\Delta x_v, \Delta y_v, \Delta z_v\}$ – amendment of the victim's coordinates to take the victim away from a given route.
$T_i = (t_i^{\text{arrival}} - t_i^{\text{sent}})$ – the measured signal's propagation time from the buoy B_i to the spoofer using the buoy's signals, or to the victim with the help of a false signal from the spoofer.
c – the speed of light.

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

Solving the system of equations (1) allows for the victim's coordinates to be calculated:

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

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

The system of equations (1) can be written as:

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

In the general case, the solution (2) is carried out using the numerical minimization methods (3):

$$\{x_v, y_v, z_v\} = \arg \min_{x_v, y_v, z_v} \varepsilon(x_v, y_v, z_v) \tag{3}$$

There is enough data from three buoys to determine $\{x_v, y_v, z_v\}$, 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 to determine z_v, the system of equations (1) takes the form:

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2} \approx cT_i, \quad i = \overline{1, N} \tag{4}$$

In this case, the solution (4) can be carried out as:

$$\{x_v, y_v\} = = \arg \min_{x_v, y_v} \left[\sum_{i=1}^{N} \left(\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2} - cT_i \right) \right] \tag{5}$$

Solving the system of equations (6) allows the spoofer's coordinates $\{x_s, y_s\}$ to be calculated:

$$\{x_s, y_s\} = \\ = \arg\min_{x_s, y_s}\left[\sum_{i=1}^{N}\left(\sqrt{(x_i - x_s)^2 + (y_i - y_s)^2} - cT_i\right)\right] \quad (6)$$

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

Supposing that the victim's coordinates $\{x_v, y_v, z_v\}$ are known; for example, by using a sonar range finder and a measured direction to the victim. If the victim does not use a barometric depth gauge for determining z_v, then in this case it is possible to determine the corrections ΔT_i for the measured time T_i so that the victim's receiver would calculate the fake coordinates that are equal to the true ones (7):

$$\{x_v, y_v, z_v\} = \arg\min_{x_v, y_v, z_v} \\ \left\{\sum_{i=1}^{N}\left(\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} - (cT_i + \Delta T_i)\right)\right\} \quad (7)$$

If the power of the spoofer's signal exceeds the power of the buoys signals, the victim's receiver will switch to receiving the false signal. Furthermore, the spoofer then applies an escaping spoofing strategy in accordance with the equation:

$$\sqrt{[x_i - (x_v + \Delta x_v)]^2 + [y_i - (y_v + \Delta y_v)]^2 + (z_v + \Delta z_v)^2} \approx \\ \approx cT_i + \Delta T_i, \quad i = \overline{1, N} \quad (8)$$

where $\{\Delta x_v, \Delta y_v, \Delta z_v\}$ – the amendment of the victim's coordinates; taking the victim away from their route. In this situation, the spoofer is in an active state on the sea surface and the value $z_i = 0$, i.e. corresponding to a zero sea level. The algorithm for finding ΔT_i, $i = \overline{1, N}$ with given vectors $\{x_v, y_v, z_v\}$ and $\{\Delta x_v, \Delta y_v, \Delta z_v\}$ has not been considered in this article.

In the conclusion of this section, the working method of 2D GNSS-like UPS (Figures 5 and 6) and a 2D GNSS-like Underwater Spoofing has been shown using an example of a sonar signal repeater (Figures 7 and 8).

Consider an extremely simplified case when underwater positioning is implemented in only one plane (2D GNSS-like UPS, Figures 5 and 6). The clock on the buoys and the underwater vehicle are synchronized. The appropriate processing of the data from the navigation satellites ensures the high accuracy of the clock on the buoys.

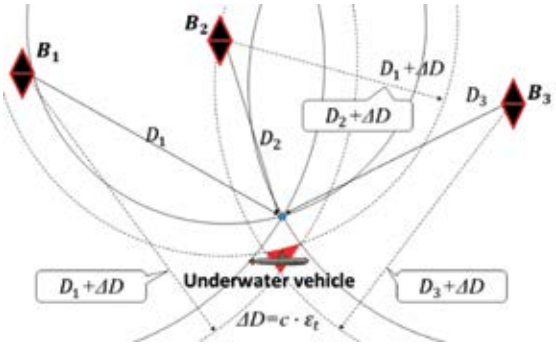

Figure 5. 2D GNSS-like UPS: B_1, B_2 and B_3 – sonar transponders of GNSS signals; D_1, D_2 and D_3 – real distances from the vehicle to the transponders; $D_1 + \Delta D$, $D_2 + \Delta D$ and $D_3 + \Delta D$ – measured distances from the vehicle to the transponders; ΔD – the distance measurement error due to the mismatch between the transponder's clock and the vehicle's clock

The transit time of the navigation signal from the satellite to the hydrophone depends not only on the distance, but also on the state of the ionosphere, the atmosphere and water, therefore an accurate measurement of the distance from the satellite to the hydrophone is impossible.

The significant error ΔD in the measurement is caused by the inaccuracy of the vehicle's on-board clock, creating a zone of uncertainty, shown in Figure 5 as a red figure, close to a triangle.

Based on an iterative process of successive approximations, this zone can be compressed and moved to a point as close as possible to the exact coordinates of the vehicle (Figure 6).

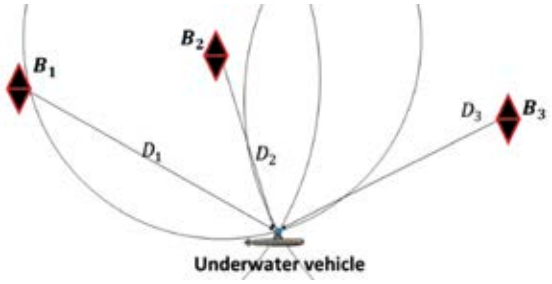

Figure 6. The final stage of the procedure of successive approximations of 2D GNSS-like UPS: B_1, B_2 and B_3 – sonar transponders of GNSS signals; D_1, D_2 and D_3 – real distances from the vehicle to the transponders

The spoofer-translator (Figure 7) receives acoustic signals from the transponders and transmits them with more power, which is sufficient to shift the vehicle's attention from the real signals to the false ones. The distance $\Delta D'$ from the spoofer-translator to the vehicle is added to the results of the measured distances (pseudo-distances).

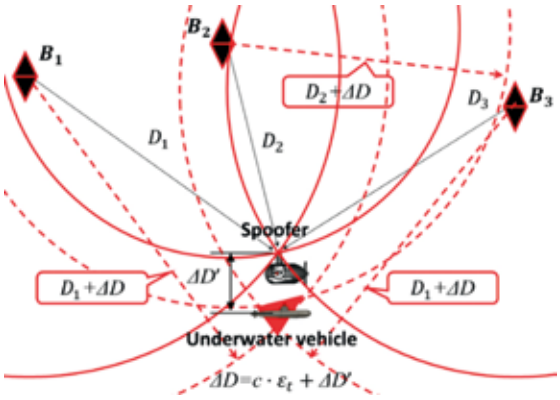

Figure 7. 2D GNSS-like Underwater Spoofing: B_1, B_2 and B_3 – sonar transponders of GNSS signals; D_1, D_2 and D_3 – real distances from the spoofer to the transponders; $D_1 + \Delta D$, $D_2 + \Delta D$ and $D_3 + \Delta D$ – measured distances from the vehicle to the transponders; $c \cdot \varepsilon_t$ – the distance measurement error due to the mismatch between the transponder's clock and the vehicle's clock; $\Delta D'$ – the distance between the spoofer and the vehicle

Based on an iterative process of successive approximations, this zone $\Delta D = c \cdot \varepsilon_t + \Delta D'$ will then be compressed and moved to a point as close as possible to the exact coordinates of the spoofer-translator (Figure 8).

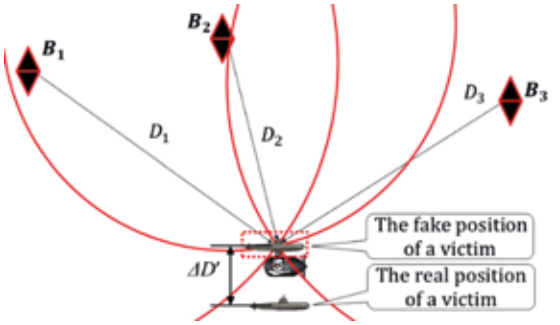

Figure 8. The final stage of the procedure of successive approximations for 2D GNSS-like Underwater Spoofing: B_1, B_2 and B_3 – sonar transponders of GNSS signals; D_1, D_2 and D_3 – real distances from the spoofer to the transponders; the vehicle determines its coordinates, which coincide with the coordinates of the spoofer-translator; $\Delta D'$ – the distance between the spoofer-translator and the vehicle

Spoofing detection using a single hydrophone

In two next sections, the results obtained in the literature (Caparrini et al., 2007, Humphreys at al., 2008, Jafarnia-Jahromi at al., 2012) and the author's own research results (Dobryakova, Lemieszewski & Ochin, 2012; 2013; 2014; Dobryakova et al., 2013) have been introduced and the two methods of spoofing detection have been discussed:

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

A fixed single hydrophone can be installed on the spoofing detector. **Note that the victim may be in motion.**

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

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

$$\{\hat{x}_{v'}, \hat{y}_{v'}, \hat{z}_{v'}\} = \arg \min_{x_{v'}, y_{v'}, z_{v'}} \left\{ \sum_{i=1}^{N} \left(\sqrt{(x_i - x_{v'})^2 + (y_i - y_{v'})^2 + (z_i - z_{v'})^2} - cT_i \right) \right\} \quad (9)$$

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

The spoofing detector again measures the XYZ coordinates of the hydrophone H at the time t'':

$$\{\hat{x}_{v''}, \hat{y}_{v''}, \hat{z}_{v''}\} = \arg \min_{x_{v''}, y_{v''}, z_{v''}} \left\{ \sum_{i=1}^{N} \left(\sqrt{(x_i - x_{v''})^2 + (y_i - y_{v''})^2 + (z_i - z_{v''})^2} - cT_i \right) \right\} \quad (10)$$

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

The measured distance between the hydrophone at the times t' and t'':

$$\hat{D}_{1-2} = \sqrt{(\hat{x}_{v'} - \hat{x}_{v''})^2 + (\hat{y}_{v'} - \hat{y}_{v''})^2 + (\hat{z}_{v'} - \hat{z}_{v''})^2} \quad (11)$$

this must be commensurate with the distance travelled by the vehicle over time $(t'' - t)$, i.e.:

$$\hat{D}_{1-2} \approx V(t'' - t') \quad (12)$$

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

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

$$\left\{\hat{x}_{v'}, \hat{y}_{v'}, \hat{z}_{v'}\right\} = \arg \min_{x_{v'}, y_{v'}, z_{v'}} \left\{\sum_{i=1}^{N}\left(\sqrt{\left(x_i - x_{v'}\right)^2 + \left(y_i - y_{v'}\right)^2 + \left(z_i - z_{v'}\right)^2} - cT_i\right)\right\} \tag{13}$$

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

The spoofing detector again measures the XYZ coordinates of the hydrophone H at the time t'':

$$\left\{\hat{x}_{v''}, \hat{y}_{v''}, \hat{z}_{v''}\right\} = \arg \min_{x_{v''}, y_{v''}, z_{v''}} \left\{\sum_{i=1}^{N}\left(\sqrt{\left(x_i - x_{v''}\right)^2 + \left(y_i - y_{v''}\right)^2 + \left(z_i - z_{v''}\right)^2} - cT_i\right)\right\} \tag{14}$$

where $(x_{v''}, y_{v''}, z_{v''})$ – the unknown precise coordinates of the hydrophone H at the time t''; $(\hat{x}_{v''}, \hat{y}_{v''}, \hat{z}_{v''})$ – the 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'' can be written as:

$$\hat{D}_{1-2} = \sqrt{\left(\hat{x}_{v'} - \hat{x}_{v''}\right)^2 + \left(\hat{y}_{v'} - \hat{y}_{v''}\right)^2 + \left(\hat{z}_{v'} - \hat{z}_{v''}\right)^2} \approx 0 \tag{15}$$

since all the hydrophones in the spoofing zone will calculate the same false coordinates and $\hat{D}_{1-2}$ must be incommensurable with the distance travelled by the vehicle over time $(t'' - t')$, i.e.:

$$\hat{D}_{1-2} << V\left(t'' - t'\right) \tag{16}$$

C. The decisive rule

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

$$\text{if } \hat{D}_{1-2} \le \check{D} \text{ then go to Spoofing} \tag{17}$$

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

It should be noted 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, and it is necessary to minimize the parameter Δt. From the point of view of detecting spoofing, it is necessary to maximize the parameter Δt. In order to resolve this contradiction, the minimax methods of parametric optimization can be used (Ehrgott, Ide & Schöbel, 2014). Minimax is a type of backtracking algorithm that is used in decision making and game theory in order to find the optimal move for a player, assuming that the player's opponent also plays optimally. It is widely used in two player turn-based games such as Tic-Tac-Toe, Backgammon, Mancala, Chess, etc.

Spoofing detection using dual hydrophones

Two fixed hydrophones H' and H'' can be installed on the spoofing detector at a distance D from each other. **Note that the spoofing detector may be stationary or in motion.**

D. The measurement of the distance between the hydrophones in navigation mode

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

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

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

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

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

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

The measured distance between H' and H'' can be calculated from:

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

where D – the real distance between the hydrophones.

E. The measurement of the distance between the hydrophones in spoofing mode

Due to the fact that all the hydrophones in the spoofing zone calculate the same false coordinates, the equation (20) takes the form:

$$\hat{D}_{1-2} = \sqrt{\left(\hat{x}_{v'} - \hat{x}_{v''}\right)^2 + \left(\hat{y}_{v'} - \hat{y}_{v''}\right)^2 + \left(\hat{z}_{v'} - \hat{z}_{v''}\right)^2} \approx 0 \tag{21}$$

F. The decisive rule

Comparing equations (20) and (21), the decisive rule for detecting spoofing can be written as:

$$\text{if } \hat{D}_{1-2} \leq \check{D} \text{ then go to Spoofing} \tag{22}$$

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

Conclusions

This paper has discussed the spoofing detection of underwater acoustic GNSS-like positioning systems through the use of single and dual hydrophones and the key to solving the challenge of providing reliable positioning.

The accessories that are necessary for the manufacture of systems for underwater acoustic "jamming" and/or "spoofing" are now widely available and this type of attack can be utilized by the military, but also by terrorists. The distortion of the signal includes signal capture and playback at the same frequency with a slight shift in time and with greater intensity, in order to deceive the acoustic equipment of an underwater vessel.

The main characteristics of spoofing detection methods have been shown in Table 1.

The ratio of the allowable velocities of the spoofer and the victim, for the method using a single hydrophone, requires additional investigation.

Table 1. The main characteristics of spoofing detection methods

Type of spoofing detection	Using a single hydrophone	Using dual hydrophones
Type of victim	Underwater vessel	Underwater vessel
Number of spoof hydrophones	1	1
Number of victim's hydrophones	1	2
Need for victim's movement	Yes	No

References

1. BAE Systems (2016) *Undersea navigation and positioning system development to begin for U.S. Navy*. [Online] May 16. Available from: https://www.baesystems.com/en-us/article/undersea-navigation-and-positioning-system-development-to-begin-for-u-s—navy [Accessed: January 20, 2018].
2. Caparrini, M., Egido, A., Soulat, F., Germain, O., Farres, E., Dunne, S. & Ruffini, G. (2007) *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
3. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2012) Antiterrorism – design and analysis of GNSS antispoofing algorithms. *Scientific Journals of the Maritime University of Szczecin, Zeszyty Naukowe Akademii Morskiej w Szczecinie* 30(102), pp. 93–101.
4. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2013) The analysis of the detecting algorithms of GNSS-spoofing. *Scientific Journals of the Maritime University of Szczecin, Zeszyty Naukowe Akademii Morskiej w Szczecinie* 36(108) z. 2, pp. 30–36.
5. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014) Design and Analysis of Spoofing Detection Algorithms for GNSS Signals. *Scientific Journals of the Maritime University of Szczecin, Zeszyty Naukowe Akademii Morskiej w Szczecinie* 40 (112), pp. 47–52.
6. Dobryakova, L., Lemieszewski, Ł., Lusznikov, E. & Ochin, E. (2013) The study of the spoofer's some properties with help of GNSS signal repeater. *Scientific Journals of the Maritime University of Szczecin, Zeszyty Naukowe Akademii Morskiej w Szczecinie* 36 (108) z. 2, pp. 159–165.
7. Ehrgott, M., Ide, J. & Schöbel, A. (2014) Minmax robustness for multi-objective optimization. *European Journal of Operational Research* 239, 1, pp. 17–31.
8. EvoLogics (2018) *Underwater Acoustic LBL Positioning Systems*. [Online]. Available from: https://www.evologics.de/en/products/LBL/index.html [Accessed: January 20, 2018].
9. Hubert, T. (1966) Method and device for the monitoring and remote control of unmanned, mobile underwater vehicles. United States Patent 5,579.285 https://patentimages.storage.googleapis.com/d2/73/89/6cd7173d154977/US5579285.pdf
10. Humphreys, T.E., Ledvina, B. M., Psiaki, M.L., O'Hanlon, B.W. & Kintner, P.M. Jr. (2008) *Assessing the Spoofng Threat: Development of a Portable GNSS Civilian Spoofer*. Preprint of the 2008 IONGNSS Conference Savanna, GA, September 16–19.

11. iXblue (2018) *High performance USBL positioning system*. [Online]. Available from: https://www.ixblue.com/products/gaps [Accessed: January 20, 2018]
12. 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.
13. Kaushal, H. & Kaddoum, G. (2016) Underwater Optical Wireless Communication. *IEEE Access* 4, pp. 1518–1547.
14. KongsbergMaritime(2016)*HighPrecisionAcousticPositioning*. [Online]. Available from: https://www.km.kongsberg.com/ks/web/nokbg0397.nsf/AllWeb/D3F9B693E19302BBC12571B6003DD0AE/$file/HiPAP_Family_brochure_v3_lowres.pdf [Accessed: January 20, 2018].
15. Lavars, N. (2016) *DARPA program plunges into underwater positioning system*. [Online] 23 May. Available from: https://newatlas.com/darpa-underwater-navigation/43472/ [Accessed: January 20, 2018].
16. Mortimer, C. (2016) *Russia testing new underwater nuclear drone amid growing tensions with the West*. [Online] 10 December. Available from https://www.independent.co.uk/news/world/europe/russia-nuclear-test-submarine-drone-us-intelligence-trump-a7467301.html/ [Accessed: January 20, 2018].
17. ROV (2018) *Remotely Operated Vehicle (ROV) Manufacturers (includes Manufacturers who are also Operators)*. [Online]. Available from: http://www.rov.org/industry_manufacturers.cfm [Accessed: January 20, 2018].
18. Scuba Diving Chicago (2013) *Underwater Vehicles. Underwater GPS navigation*. [Online] 18 Apr. Available from: https://www.scubadivingchicago.us/underwater-vehicles/underwater-gps-navigation.html [Accessed: January 20, 2018].
19. Sonardyne (2018) *Subsea technology for energy, science and security*. [Online] Available from: https://www.sonardyne.com [Accessed: January 20, 2018].
20. Thomas, H.G. (1998) *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 20, 2018].
21. Youngberg, J.W. (1991) A Novel Method for Extending GPS to Underwater Applications. *Navigation* 38, pp. 263–271.