Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2017, 52 (124), 145–153
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)
DOI: 10.17402/256

Received: 19.08.2017
Accepted: 10.11.2017
Published: 15.12.2017

GPS/GNSS spoofing and the real-time single-antenna-based spoofing detection system

Evgeny Ochin

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

Key words: Global Navigation Satellite System, Global Positioning System, anti-terrorism, anti-spoofing, transport safety, spoofer, spoofing detection algorithm

Abstract
The idea of C/A codes GPS/GNSS Spoofing (Substitution), or the ability to mislead a satellite navigation receiver into establishing a position or time fix which is incorrect, has been gaining attention as spoofing has become more sophisticated. Various techniques have been proposed to detect if a receiver is being spoofed – with varying degrees of success and computational complexity. If the jammer signals are sufficiently plausible then the GNSS receiver may not realize it has been duped. There are various means of detecting spoofing activity and hence providing effective mitigation methods. In this paper, a novel signal processing method applicable to a single antenna handset receiver for spoofing detection has been described. Mathematical models and algorithms have been developed to solve the problems of satellite navigation safety. What has been considered in the paper is a spoofing detection algorithm based on the analysis of a civil satellite signal generated by mobile C/A GPS/GNSS single-antenna receivers. The work has also served to refine the civilian spoofing threat assessment by demonstrating the challenges involved in mounting a spoofing attack.

Introduction

Modern satellite navigation is based on the use of no-request range measurements between a navigational satellite and the user. It means that the information about the satellite's coordinates, given to the user, is included in the navigation signal. This method of range measurement is based on the calculation of the receiving signal's time delay compared with the signals generated by the user's equipment.

Satellite based positioning provides the world's most precise location information. It is possible to acquire positioning anywhere in the world that GNSS satellite signals are available, at any time of day, at data rates of up to 100 Hz. Measurements can be generated in real time or processed post-mission to achieve the highest level of accuracy.

GNSS technology is most frequently used to:

- Determine the location of an object on, or with respect to, the Earth for navigation;
- Locate an object with respect to another object for tracking purposes.

The positioning information typically provided includes a horizontal domain (latitude/longitude or easting/northing) and a vertical domain (height).

The definitions used in this article are:

1. **GNSS** – Global Navigation Satellite System {GLONASS: www.glonass-iac.ru, NAVSTAR GPS: www.navcen.uscg.gov, BEIDOU: en.beidou.gov.cn, GALILEO: www.gsc-europa.eu, QZSS: www.qzs.jp/en/services}.
2. **Sat$_i$**, $i=\overline{1,N}$, $N \geq 4$ – the navigation satellites as the spacefaring component of GNSS. {*In an ideal case, when the measurements are precise and satellite time is identical to the user's equipment time, the user's position can be realized with only 3 satellites. However the satellites time actually differs from the time on the user's equipment. So, one more coordinate is necessary to find the user's position – the time drift between the user's equipment and*

the satellite time. That is why four satellites are needed to solve the navigation problem.}

3. **Spoofing** – an attack on a GNSS signal, in an attempt to deceive the GNSS receiver by transmitting powerful false signals that mimic the signals from the true GNSS, exceeding the power of these true signals.
4. **Spoofer** – complex computer and radio equipment for the implementation of GNSS spoofing.
5. **(x, y, z)** – the real coordinates of a vehicle (victim). If the vehicle is a 2D vehicle (ship, vessel, boat, car, etc.), the height coordinate (z) can be omitted, and the minimum number of navigation satellites required can be reduced to three ($i = \overline{1,N}$, $N \geq 3$).
6. **(x_v, y_v, z_v)** – the precise coordinates of the vehicle.
7. **$(\hat{x}_v, \hat{y}_v, \hat{z}_v)$** – the calculated coordinates of the vehicle using the GNSS.
8. **(x_s, y_s, z_s)** – the precise coordinates of the reception antenna of the spoofer.
9. **$(\hat{x}_s, \hat{y}_s, \hat{z}_s)$** – the calculated coordinates of the reception antenna of the spoofer.
10. We also denote for $i = \overline{1,N}$, $N \geq 4$ (if the vehicle is a 2D vehicle (ship, vessel, boat, car, etc.), the height coordinate (z) can be omitted and the minimum number of navigation satellites can be reduced to three ($i = \overline{1,N}$, $N \geq 3$)):
    (x_i, y_i, z_i) – the coordinates of Sat$_i$;
    T_i^v – the propagation time from Sat$_i$ to the vehicle in a vacuum;
    $\hat{T}_i^v$ – the propagation time from Sat$_i$ to the vehicle in the real atmosphere;
    D_i^v – the measurement result of the distance from Sat$_i$ to the vehicle (the vehicle's pseudo-range);
    D_s^v – the distance from the spoofer to the victim;
    Δt_s^v – the signal transit time from the spoofer to the victim;
    $\Delta\rho_i$ – unknown error of the measurement result of the distance from Sat$_i$ to the vehicle.

GNSS positioning

The distance from a vehicle (Figure 1) to the satellites Sat$_i$, can be written as:

$$D_i^v = \sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} = cT_i^v$$
$$i = \overline{1,N}, \ N \geq 4 \tag{1}$$

Since the measurement of the distance from the vehicle to the satellites is carried out by measuring the propagation time $\hat{T}_i^v = T_i^v + \Delta T_i^v$ of the GNSS signals from Sat$_i$ to the vehicle, then (1) can be represented as (excluding time synchronization errors):

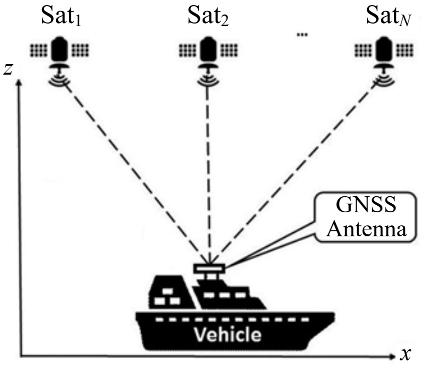


Figure 1. GNSS: Sat$_i$ – Satellites; $i = \overline{1,N}$, N ≥ 4; the visible part of GNSS satellite constellation

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} = c\left(\hat{T}_i^v - \Delta T_i^v\right)$$
$$i = \overline{1,N}, \ N \geq 4 \tag{2}$$

Since $\Delta\rho_i = c\Delta T_i^v$, then equation (2) can be written in the form:

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2 + (z_i - z_v)^2} - \Delta\rho_i = c\hat{T}_i^v$$
$$i = \overline{1,N}, \ N \geq 4 \tag{3}$$

The navigation processor in the vehicle solves the system of the equations (3), and calculates the position of the vehicle (x_v, y_v, z_v) and the timing errors on board Δt, which are then used to correct the GNSS navigation clock.

$$\left\{\begin{matrix} \sqrt{(x_1 - x_v)^2 + (y_1 - y_v)^2 + (z_1 - z_v)^2} - \Delta\rho_1 \\ \sqrt{(x_2 - x_v)^2 + (y_2 - y_v)^2 + (z_2 - z_v)^2} - \Delta\rho_2 \\ \sqrt{(x_3 - x_v)^2 + (y_3 - y_v)^2 + (z_3 - z_v)^2} - \Delta\rho_3 \end{matrix}\right\} \rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\, i=\overline{1,3}]{\text{Iteration algorithm}} (x_v, y_v, z_v) \tag{4}$$

The iterative algorithm is based on the mechanism of sequential reduction of the inaccurate (usually quartz) timer of the user, to the accurate (usually atomic) clocks onboard the navigation satellites (this article does not consider the timing errors, Δt).

Because $\Delta\rho_i$ is not an unknown value, instead of the exact value (x_v, y_v, z_v) we will get an approximate results of the measurements ($\hat{x}_v, \hat{y}_v, \hat{z}_v$):

$$\left\{\begin{matrix} \sqrt{(x_1 - x_v)^2 + (y_1 - y_v)^2 + (z_1 - z_v)^2} \\ \sqrt{(x_2 - x_v)^2 + (y_2 - y_v)^2 + (z_2 - z_v)^2} \\ \sqrt{(x_3 - x_v)^2 + (y_3 - y_v)^2 + (z_3 - z_v)^2} \end{matrix}\right\} \rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\, i=\overline{1,3}]{\text{Iteration algorithm}} (\hat{x}_v, \hat{y}_v, \hat{z}_v) \tag{5}$$

GNSS spoofing

A spoofer transmits the simulated signals of several satellites; (Hartman, 1996; Humphreys et al., 2008; Humphreys et al., 2009; Rawnsley, 2011; Tippenhauer et al., 2011; Broumandan et al., 2012; Zaragoza & Zumalt, 2013). If the level of the simulated signals exceeds the level of the signals from real satellites, the GNSS receiver captures the false signal and calculates the false coordinates.

We have distinguished the following spoofing modes:

A. A spoofer is motionless and broadcasts signals of the visible part of the GNSS satellite constellation, and then **a repeater of the GNSS signals** is used as the spoofer (Figure 2).

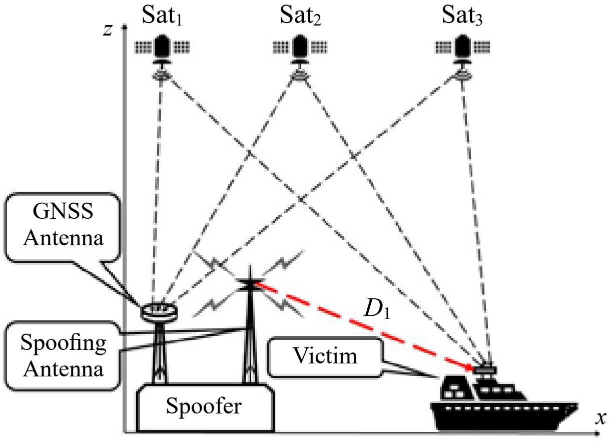


Figure 2. GNSS Spoofer broadcasts signals of the visible part of the GNSS satellite constellation

B. A spoofer is motionless and broadcasts a recorded signal of the visible part of the GNSS satellite constellation, and then the **GNSS recorder** is used as the spoofer (Figure 3).

C. A spoofer is motionless and broadcasts a signal of the visible part of the GNSS satellite constellation with the introduction of signal delays from each of the GNSS satellites, and then **a repeat of the GNSS signals with a programmed signal delay** from each of the GNSS satellites is used as a spoofer (Figure 4).

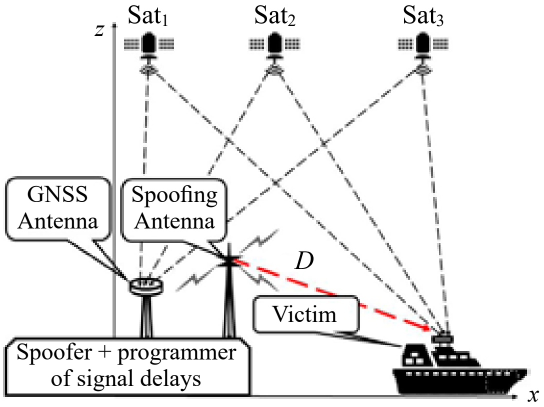


Figure 4. GNSS Spoofer broadcasts a recorded signal of the visible part of the GNSS satellite constellation with the possibility of a programmed signal delay for each satellite

D. A spoofer is motionless and broadcasts a simulated GNSS signals, and then **a GNSS-signal simulator** is used as a spoofer (Figure 5).

E. A spoofer is mobile and broadcasts signals of the visible part of GNSS satellite constellation, and then **a GNSS signal repeater** is used as the spoofer (Figure 6).

F. A spoofer is mobile and broadcasts a recorded signal of the visible part of the GNSS satellite constellation, and then the **GNSS recorder** is used as the spoofer (Figure 7).

G. A spoofer is mobile and broadcasts signals of the visible part of the GNSS satellite constellation

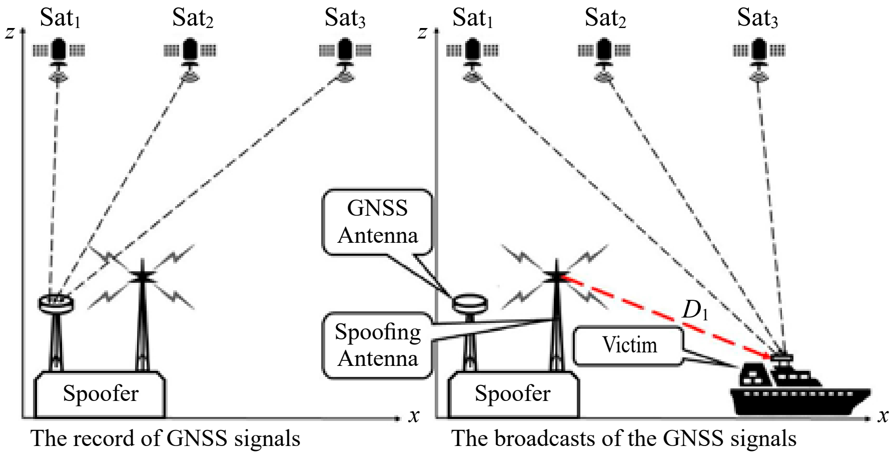


Figure 3. GNSS Spoofer broadcasts a recorded signal of the visible part of the GNSS satellite constellation

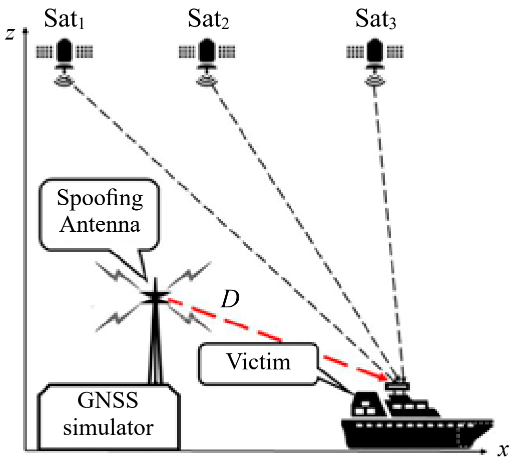


Figure 5. GNSS Spoofer broadcasts simulated GNSS signals

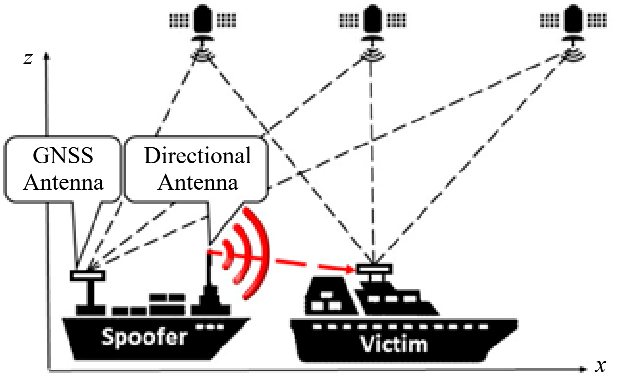


Figure 6. Mobile GNSS Spoofer broadcasts signals of the visible part of the GNSS satellite constellation

with the introduction of a signal delay from each of the satellites, and then **a repeater of the GNSS signals with a programmed signal delay** from each of the GNSS satellites is used as a spoofer (Figure 8).

H. A spoofer is mobile and broadcasts a simulated GNSS signals, and then **a simulated GNSS-signal** is used as a spoofer (Figure 9).

In this article, only mode A has been considered.

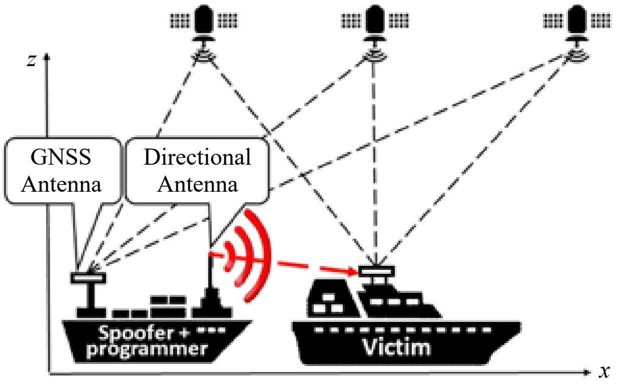


Figure 8. Mobile GNSS Spoofer broadcasts a recorded signal of the visible part of the GNSS satellite constellation with the possibility of a programmed signal delay for each satellite

In this mode a spoofer is motionless and broadcasts signals of the visible part of the GNSS satellite constellation, and then **a repeater of the GNSS signals** is used as the spoofer (Figure 2). A victim receives the same signal as the spoofer, but with some delay Δt_s^v. It means that all receivers in the spoofing zone calculate the same false coordinates, regardless of the distance from the spoofer to the victim:

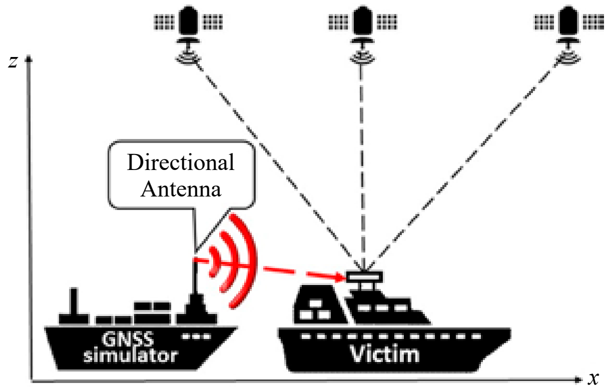
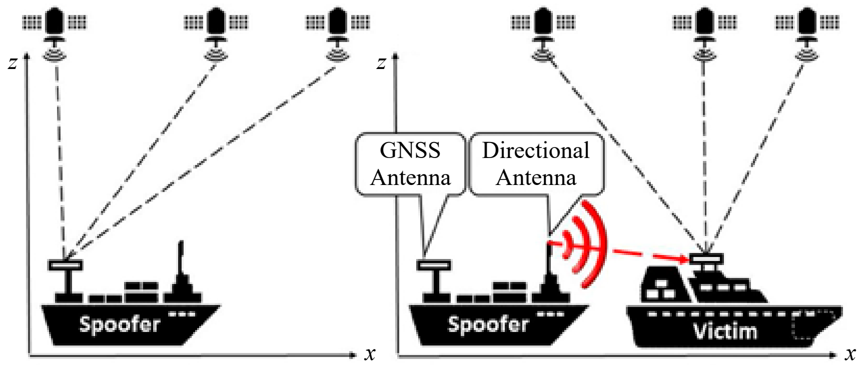


Figure 9. Mobile GNSS Spoofer broadcasts a simulated GNSS signals



The record of GNSS signals
The broadcasts of the GNSS signals

Figure 7. Mobile GNSS Spoofer broadcasts a recorded signal of the visible part of the GNSS satellite constellation

$$\left\{\begin{array}{l}\sqrt{(x_1-x_v)^2+(y_1-y_v)^2+(z_1-z_v)^2}+D_s^v\\ \sqrt{(x_2-x_v)^2+(y_2-y_v)^2+(z_2-z_v)^2}+D_s^v\\ \sqrt{(x_3-x_v)^2+(y_3-y_v)^2+(z_3-z_v)^2}+D_s^v\end{array}\right\}\rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\, i=\overline{1,3}]{\text{Iteration algorithm}}(\hat{x}_s,\hat{y}_s,\hat{z}_s) \quad (6)$$

where $D_s^v = c\Delta t_s^v$.

Detection of spoofing

For the detection of GNSS spoofing, various methods have been suggested. We have listed some of them.

- Detection based on the determination of the direction to the radiation source of the spoofer, comparing the phases of the signal to several antennas.
- Detection based on the definition of the Doppler frequency shift.
- Using the military GNSS signal as a reference (without the need to know the encryption key).
- Comparing the indications of the inertial navigation system and the data from the GNSS receiver.

Dual-antenna spoofing detector

The Spoofing Detector (SD) requires the use of two antennas (Figure 10) (Dobryakova, Lemieszewski & Ochin, 2012; 2013; 2014; Ochin et al., 2013; Dobryakova & Ochin, 2014; Psiaki et al., 2014). The distance between the antennas is denoted as D_{1-2}.

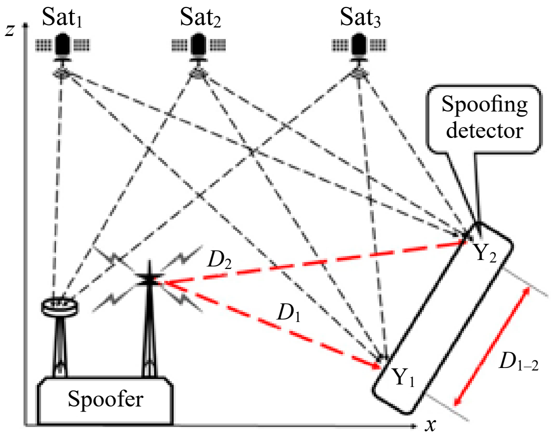


Figure 10. The spoofer and the dual-antenna spoofing detector (SD): Y$_1$ and Y$_2$ – antennas of the SD; *D*$_1$ and *D*$_2$ – the distances from the antenna of the spoofer to the antennas of the SD, *D*$_{1-2}$ – the distance between the antennas of the SD

Measuring the distance between antennas in normal navigation mode

The spoofing detector measures the coordinates of the antennas Y$_1$ and Y$_2$:

$$\left\{\begin{array}{l}\sqrt{(x_1-x_{v1})^2+(y_1-y_{v1})^2+(z_1-z_{v1})^2}\\ \sqrt{(x_2-x_{v1})^2+(y_2-y_{v1})^2+(z_2-z_{v1})^2}\\ \sqrt{(x_3-x_{v1})^2+(y_3-y_{v1})^2+(z_3-z_{v1})^2}\end{array}\right\}\rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\, i=\overline{1,3}]{\text{Iteration algorithm}}(\hat{x}_{v1},\hat{y}_{v1},\hat{z}_{v1}) \quad (7)$$

where (x_{v1}, y_{v1}, z_{v1}) – denotes the unknown precise coordinates of the antenna Y$_1$, and $(\hat{x}_{v1},\hat{y}_{v1},\hat{z}_{v1})$ – denotes the calculated coordinates of the antenna Y$_1$.

$$\left\{\begin{array}{l}\sqrt{(x_1-x_{v2})^2+(y_1-y_{v2})^2+(z_1-z_{v2})^2}\\ \sqrt{(x_2-x_{v2})^2+(y_2-y_{v2})^2+(z_2-z_{v2})^2}\\ \sqrt{(x_3-x_{v2})^2+(y_3-y_{v2})^2+(z_3-z_{v2})^2}\end{array}\right\}\rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\, i=\overline{1,3}]{\text{Iteration algorithm}}(\hat{x}_{v2},\hat{y}_{v2},\hat{z}_{v2}) \quad (8)$$

where (x_{v2}, y_{v2}, z_{v2}) – denotes the unknown precise coordinates of the antenna Y$_2$, and $(\hat{x}_{v2},\hat{y}_{v2},\hat{z}_{v2})$ – denotes the calculated coordinates of the antenna Y$_2$.

The measurement results differ by some unknown value and, accordingly, the distance estimate $\hat{D}_{1-2}$ between the antennas will be comparable with the magnitude of D_{1-2}:

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{v1}-\hat{x}_{v2})^2+(\hat{y}_{v1}-\hat{y}_{v2})^2+(\hat{z}_{v1}-\hat{z}_{v2})^2}\cong$$
$$\cong D_{1-2} \quad (9)$$

Measurement of the spacing setween the antennas in spoofing mode

A victim receives the same signal as the spoofer, but with some delay Δt_s^v. It means that all the receivers in the spoofing zone calculate the same false coordinates, regardless of the distance from the spoofer to the victim:

$$\left\{\begin{array}{l}\sqrt{(x_1-x_{v1})^2+(y_1-y_{v1})^2+(z_1-z_{v1})^2}+D_s^{v1}\\ \sqrt{(x_2-x_{v1})^2+(y_2-y_{v1})^2+(z_2-z_{v1})^2}+D_s^{v1}\\ \sqrt{(x_3-x_{v1})^2+(y_3-y_{v1})^2+(z_3-z_{v1})^2}+D_s^{v1}\end{array}\right\}\rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\, i=\overline{1,3}]{\text{Iteration algorithm}}(\hat{x}_{s'},\hat{y}_{s'},\hat{z}_{s'}) \quad (10)$$

where $D_s^{v1} = c\Delta t_s^{v1}$ – the distance from the spoofer to the antenna Y$_1$, and ($\hat{x}_{s'}, \hat{y}_{s'}, \hat{z}_{s'}$) – the calculated coordinates of the spoofer using an antenna Y$_1$.

$$\left\{\begin{matrix} \sqrt{(x_1 - x_{v2})^2 + (y_1 - y_{v2})^2 + (z_1 - z_{v2})^2} + D_s^{v2} \\ \sqrt{(x_2 - x_{v2})^2 + (y_2 - y_{v2})^2 + (z_2 - z_{v2})^2} + D_s^{v2} \\ \sqrt{(x_3 - x_{v2})^2 + (y_3 - y_{v2})^2 + (z_3 - z_{v2})^2} + D_s^{v2} \end{matrix}\right\} \rightarrow$$

$$\xrightarrow[\text{for Sat}_i,\, i=\overline{1,3}]{\text{Iteration algorithm}} (\hat{x}_{s''}, \hat{y}_{s''}, \hat{z}_{s''}) \tag{11}$$

where $D_s^{v2} = c\Delta t_s^{v2}$ – the distance from the spoofer to the antenna Y$_2$, and ($\hat{x}_{s''}, \hat{y}_{s''}, \hat{z}_{s''}$) – the calculated coordinates of the spoofer using an antenna Y$_2$.

In this case, the distance between the antennas Y$_1$ and Y$_2$ is defined as:

$$\hat{D}_{1-2} = \sqrt{(\hat{x}_{s'} - \hat{x}_{s''})^2 + (\hat{y}_{s'} - \hat{y}_{s''})^2 + (\hat{z}_{s'} - \hat{z}_{s''})^2} \cong 0 \tag{12}$$

The Decisive Rule 1

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

$$\text{if } \hat{D}_{1-2} \le \breve{D} \text{ then } \langle\text{Spoofing}\rangle \text{ else } \langle\text{GNSS}\rangle \tag{13}$$

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

The algorithm for spoofing detection by estimating the dispersion of the pseudorange difference of two antennas

In the normal navigation mode, the pseudoranges of the antennas Y$_1$ and Y$_2$ differ from each other by some unknown, but significantly different value:

$$\Delta\hat{\rho}_i = (\hat{\rho}_{i'} - \hat{\rho}_{i''}) \tag{14}$$

Therefore, the root-mean-square deviation (RMSD) in the differences in the pseudoranges of the antennas Y$_1$ and Y$_2$ will be significantly different from zero:

$$\sigma_{gnss} = \sqrt{\frac{\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''})^2 - \frac{1}{N}\left(\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''})\right)^2}{N-1}} >> 0 \tag{15}$$

In the spoofing mode, the pseudoranges of the antennas Y$_1$ and Y$_2$ differ from each other by a certain constant value equal to $D_1 – D_2$. In this case the RMSD difference in the pseudoranges of antennas Y$_1$ and Y$_2$ is practically zero, that is:

$$\sigma_s \cong 0 \tag{16}$$

The decisive rule 2

Comparing (15) and (16), the decisive rule for spoofing detection can be written as:

$$\text{if } \sqrt{\frac{\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''})^2 - \frac{1}{N}\left(\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''})\right)^2}{N-1}} <$$

$$< \frac{\sigma_{gnss} - \sigma_s}{2} \text{ then } \langle\text{Spoofing}\rangle \text{ else } \langle\text{GNSS}\rangle \tag{17}$$

If we take $\sigma_{gnss} >> \sigma_s$, then the decisive spoofing detection rule can be written as:

$$\text{if } \sqrt{\frac{\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''})^2 - \frac{1}{N}\left(\sum_{i=1}^{N}(\hat{\rho}_{i'} - \hat{\rho}_{i''})\right)^2}{N-1}} <$$

$$< \frac{\sigma_{gnss}}{2} \text{ then } \langle\text{Spoofing}\rangle \text{ else } \langle\text{GNSS}\rangle \tag{18}$$

Discussion of the decisive rules

The spoofing detector can be designed on the basis of one of the decisive rules or on the basis of any combination of decision rules. In any case, it is necessary to calculate the probabilities of the “False alarm (false positives)” and “Missing target (false negatives)” events (Table 1).

Table 1. Mistakes of a decision of the first kind (False alarm) and the second kind (Missing target)

The decisive rule or combination of decision rules		Valid mode	
		GNSS	SPOOFING
Solving of Spoofing Detector	GNSS	The solution is right	**Missing target**
	SPOOFING	**False alarm**	The solution is right

The questions of optimal design and selection of boundary conditions with the aim of minimizing the probabilities of “false alarm” and “missing target” are beyond the scope of this article. Here it should be noted that one of the widely used techniques is the application of Bayes theorem (or Bayesian formula) (Dobryakova, Lemieszewski & Ochin, 2012).

Single-antenna spoofing detector in case the vehicle is moving

Suppose that the vehicle is moving in an arbitrary direction. On the spoofing detector we install a single-antenna Y (Figure 11). The position of the antenna at the time t' is denoted as Y′, the position of the antenna at the time $t'' = t' + \Delta t$ is denoted as Y″ and the distance between the two antenna positions is denoted as D_{1-2}.

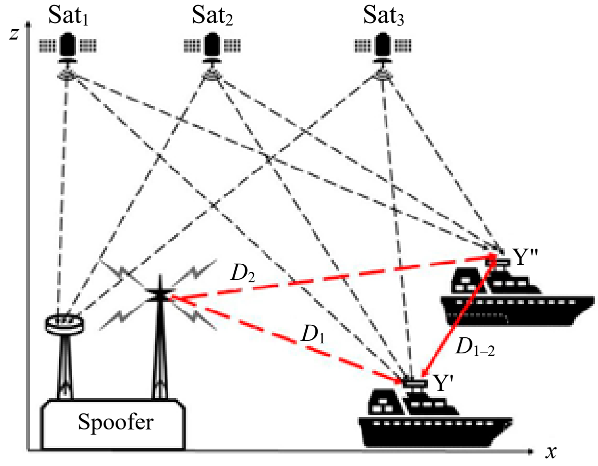


Figure 11. Spoofer and single-antenna spoofing detector (SD): Y′ and Y″ – two positions of single-antenna Y; D_1 and D_2 – the distances from the spoofer's antenna to the SD antenna Y; D_{1-2} – the distance between two positions of single-antenna Y

Measuring the distance between two positions of single-antenna in normal navigation mode

The spoofing detector measures the coordinates of the antenna Y in two positions:

$$\left\{\begin{matrix}\sqrt{(x_1-x_{v'})^2+(y_1-y_{v'})^2+(z_1-z_{v'})^2}\\ \sqrt{(x_2-x_{v'})^2+(y_2-y_{v'})^2+(z_2-z_{v'})^2}\\ \sqrt{(x_3-x_{v'})^2+(y_3-y_{v'})^2+(z_3-z_{v'})^2}\end{matrix}\right\}\rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\,i=\overline{1,3}]{\text{Iteration algorithm}}(\hat{x}_{v'},\hat{y}_{v'},\hat{z}_{v'}) \qquad (19)$$

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

$$\left\{\begin{matrix}\sqrt{(x_1-x_{v''})^2+(y_1-y_{v''})^2+(z_1-z_{v''})^2}\\ \sqrt{(x_2-x_{v''})^2+(y_2-y_{v''})^2+(z_2-z_{v''})^2}\\ \sqrt{(x_3-x_{v''})^2+(y_3-y_{v''})^2+(z_3-z_{v''})^2}\end{matrix}\right\}\rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\,i=\overline{1,3}]{\text{Iteration algorithm}}(\hat{x}_{v''},\hat{y}_{v''},\hat{z}_{v''}) \qquad (20)$$

where $(x_{v''}, y_{v''}, z_{v''})$ – the unknown precise coordinates of the antenna Y at the time $t'' = t' + \Delta t$, and, $(\hat{x}_{v''},\hat{y}_{v''},\hat{z}_{v''})$ – the calculated coordinates of the antenna Y at the time $t'' = t' + \Delta t$.

The distance between the antenna Y at the time t' and the antenna Y at the time $t'' = t' + \Delta t$ will be comparable with the magnitude D_{1-2}:

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{v'}-\hat{x}_{v''})^2+(\hat{y}_{v'}-\hat{y}_{v''})^2+(\hat{z}_{v'}-\hat{z}_{v''})^2}\cong$$
$$\cong D_{1-2} \qquad (21)$$

Measurement of the spacing between two positions of a single-antenna in spoofing mode

A victim receives the same signal as the spoofer, but with some delay Δt_s^{v}. It means that all the receivers in the spoofing zone calculate the same false coordinates, regardless of the distance from the spoofer to the victim:

$$\left\{\begin{matrix}\sqrt{(x_1-x_{v'})^2+(y_1-y_{v'})^2+(z_1-z_{v'})^2}+D_s^{v'}\\ \sqrt{(x_2-x_{v'})^2+(y_2-y_{v'})^2+(z_2-z_{v'})^2}+D_s^{v'}\\ \sqrt{(x_3-x_{v'})^2+(y_3-y_{v'})^2+(z_3-z_{v'})^2}+D_s^{v'}\end{matrix}\right\}\rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\,i=\overline{1,3}]{\text{Iteration algorithm}}(\hat{x}_{s'},\hat{y}_{s'},\hat{z}_{s'}) \qquad (22)$$

where $D_s^{v'} = c\Delta t_s^{v'}$ – the distance from the spoofer to the antenna Y at the time t', and $(\hat{x}_{s'},\hat{y}_{s'},\hat{z}_{s'})$ – the calculated coordinates of the spoofer using the antenna Y at the time t':

$$\left\{\begin{matrix}\sqrt{(x_1-x_{v''})^2+(y_1-y_{v''})^2+(z_1-z_{v''})^2}+D_s^{v''}\\ \sqrt{(x_2-x_{v''})^2+(y_2-y_{v''})^2+(z_2-z_{v''})^2}+D_s^{v''}\\ \sqrt{(x_3-x_{v''})^2+(y_3-y_{v''})^2+(z_3-z_{v''})^2}+D_s^{v''}\end{matrix}\right\}\rightarrow$$
$$\xrightarrow[\text{for Sat}_i,\,i=\overline{1,3}]{\text{Iteration algorithm}}(\hat{x}_{s''},\hat{y}_{s''},\hat{z}_{s''}) \qquad (23)$$

where $D_s^{v''}=c\Delta t_s^{v''}$ – the distance from the spoofer to the antenna Y at the time $t''=t'+\Delta t$, and $(\hat{x}_{s''},\hat{y}_{s''},\hat{z}_{s''})$ – the calculated coordinates of the spoofer using the antenna Y at the time $t'' = t' + \Delta t$.

In this case, the distance between the antenna Y at the time t' and the antenna Y at the time $t'' = t' + \Delta t$ is defined as:

$$\hat{D}_{1-2}=\sqrt{(\hat{x}_{s'}-\hat{x}_{s''})^2+(\hat{y}_{s'}-\hat{y}_{s''})^2+(\hat{z}_{s'}-\hat{z}_{s''})^2}\cong 0 \qquad (24)$$

The decisive rule

Comparing (21) and (24), the decisive rule for detecting spoofing can be written as:

$$\text{if } \hat{D}_{1-2} \leq \breve{D} \text{ then } \langle\text{Spoofing}\rangle \text{ else } \langle\text{GNSS}\rangle \quad (25)$$

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

Rotating single-antenna spoofing detector

The antenna can be installed on a rotating turret, the radius of which is about one meter. In this case, the diameter of the antenna's rotation circle is equal to two meters. The spoofing detector measures the coordinates of the antenna in two positions (Figure 12):

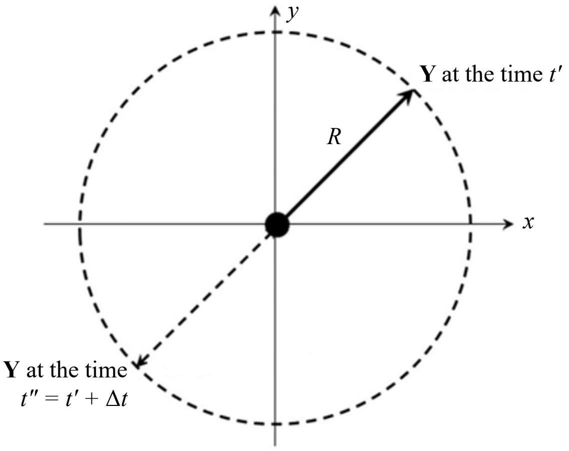


Figure 12. Rotating single-antenna spoofing detector, in the case when the vehicle is in motionless: Δ*t* = *T*/2, where *T* – rotation period of antenna Y

The measurements are performed in accordance with (23–24), and the decisive rule in accordance with (25).

The equipment for experimental studies

For the experimental studies, standard equipment was used, including two Holux GR-213u GNSS receivers (Figure 13).

This equipment allowed for experimental studies in the following four modes (Figure 14).

1. The ship is moving or not moving. Two fixed antennas are in two separate positions (https://goo.gl/1Fk5Na).
2. The ship is moving or not moving. One antenna is used in series in two positions. After the first position measurement is taken, the antenna is transferred to another position and the second measurement is performed.

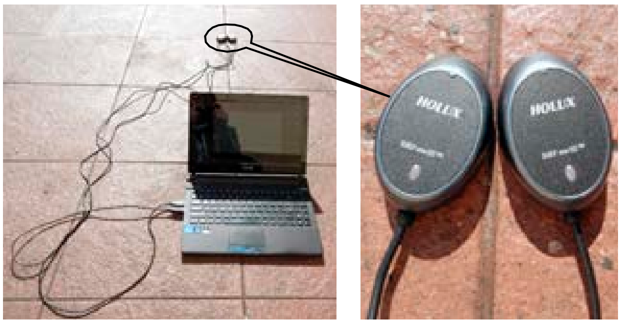


Figure 13. The equipment used for experimental studies: HOLUS – GNSS-receiver (Dobryakova, Lemieszewski & Ochin, 2014)

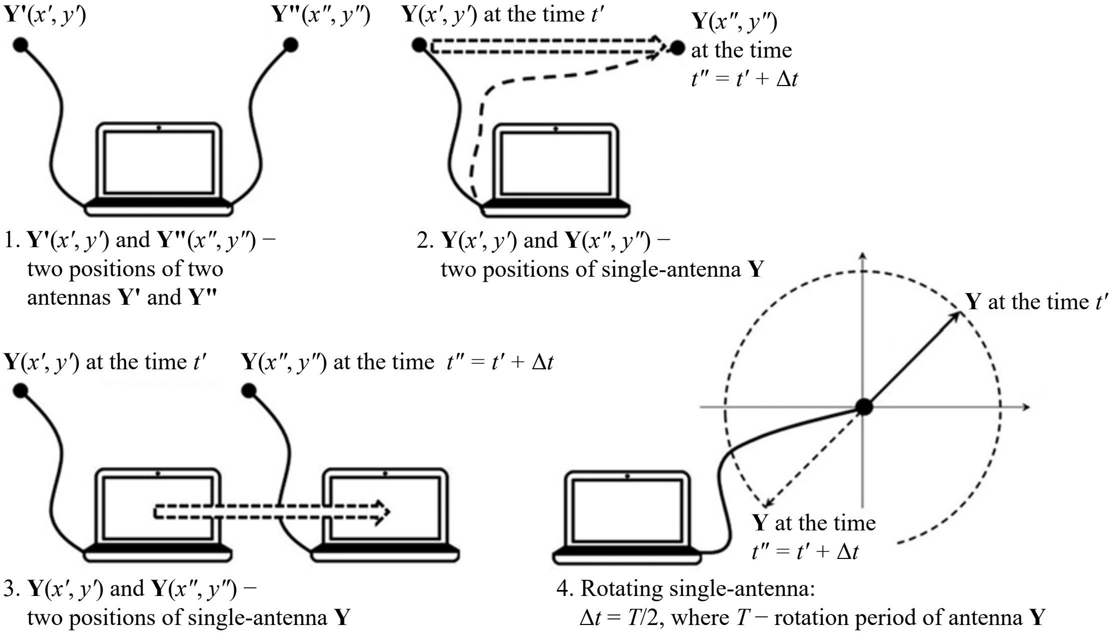

Y'(x′, y′)
Y"(x″, y″)
1. Y'(x′, y′) and Y"(x″, y″) – two positions of two antennas Y' and Y"
Y(x′, y′) at the time t′
Y(x″, y″) at the time t″ = t′ + Δt
2. Y(x′, y′) and Y(x″, y″) – two positions of single-antenna Y
Y(x′, y′) at the time t′
Y(x″, y″) at the time t″ = t′ + Δt
3. Y(x′, y′) and Y(x″, y″) – two positions of single-antenna Y
Y at the time t′
Y at the time t″ = t′ + Δt
4. Rotating single-antenna: Δt = T/2, where T – rotation period of antenna Y

Figure 14. The four modes used in the experimental studies

3. The ship is moving. One antenna is used in series in two positions. The second measurement is performed after a certain period of time Δt.
4. The ship is moving or not moving. One antenna is used in series in two positions (rotating single-antenna). The first measurement is performed with the angle of antenna's rotation α, and the second measurement with the angle of antenna's rotation $\alpha + 180°$.

Comparing methods 2, 3 and 4, it can be noted that there is not a fundamental difference between these methods in terms of performing a sequence of measurements, using an algorithm to process the signals, and interpreting the results of the measurements.

Summary and conclusions

The risk of losing the GNSS signal is growing every day. The equipment necessary to manufacture GNSS "jamming" and/or "spoofing" systems are now widely available, and this type of attack cannot only be deployed 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 electronic equipment of the victim and, therefore, the operator if there is one on board the vehicle. The price of one chipset for such equipment is in the range of 1–10 thousand Euros, depending on the dimensions and weight parameters.

It is important to emphasize that GNSS is not only used for navigation. In the framework of the current threat model, GNSS interference is needed in order to drown out the reference signal of synchronous time that is used in a distributed network of electronic radio devices. That is, GNSS allows you to synchronize with a very accurate time signal on stand-alone passive devices.

Synchronous time is also necessary for data transfer in a low-visibility communication mode: receivers and repeaters must have a total time to correctly adjust the correlation parameters, allowing them to isolate the masked signal, which is indistinguishable from noise for an outside observer. And this, of course, is not a complete list.

References

1. Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J. & Lachapelle, G. (2012) *GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation*. Position Location and Navigation Symposium (PLANS), April 23–26, 2012, Myrtle Beach, SC, USA. Available from: http://ieeexplore.ieee.org/abstract/document/6236917/ [Accessed: August 15, 2017]
2. Dobryakova, L. & Ochin, E. (2014) On the application of GNSS signal repeater as a spoofer. *Scientific Journals of the Maritime University of Szczecin, Zeszyty Naukowe Akademii Morskiej w Szczecinie* 40 (112), pp. 53–57.
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. Hartman, R.G. (1996) *Spoofing Detection System for a Satellite Positioning System*. U.S. Patent No. 5,557,284, Sept. 1996. Available from: https://www.google.ch/patents/US5557284
7. Humphreys, T.E., Kintner, P.M., Jr., Psiaki, M.L., Ledvina, B.M. & O'Hanlon, B.W. (2009) Assessing the Spoofing Threat. *GPS World* 20 (1), pp. 28–38.
8. Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W. & Kintner, P.M. Jr. (2008) Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. Preprint of the 2008 ION GNSS Conference Savannah, GA, September 16–19, 2008 https://radionavlab.ae.utexas.edu/images/stories/files/papers/ion2008r01_for_distributionW.pdf
9. Ochin, E., Lemieszewski, Ł., Lusznikov, E. & Dobryakova, L. (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, 159–165.
10. Psiaki, M.L., O'Hanlon, B.W., Powell, S.P., Bhatti, J.A., Humphreys, T.E. & Schofield, A. (2014) GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase. *GPS World* 25, (11), pp. 36–44.
11. Rawnsley, A. (2011) *Iran's Alleged Drone Hack: Tough, but Possible*. [Online] December 2011. Available from: http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/ [Accessed: August 15, 2017]
12. Tippenhauer, N.O., Pöpper, C., Rasmussen, K.B. & Čapkun, S. (2011) *On the Requirements for Successful GPS Spoofing Attacks*. Proceedings of the 18th ACM conference on Computer and communications security CCS'11, Chicago, Illinois, USA, October 17–21, 2011. Available from: https://www.cs.ox.ac.uk/files/6489/gps.pdf [Accessed: August 15, 2017]
13. Zaragoza, S. & Zumalt, E. (2013) *Spoofing a Superyacht at Sea*. [Online] July 2013. Available from: http://www.utexas.edu/know/2013/07/30/spoofing-a-superyacht-at-sea/ [Accessed: August 15, 2017]