**Scientific Journals**
Maritime University of Szczecin

**Zeszyty Naukowe**
Akademia Morska w Szczecinie

**2014, 38(110) pp. 118–124**
**ISSN 1733-8670**

**2014, 38(110) s. 118–124**

# Real-time GNSS spoofing detection in maritime code receivers

**Paweł Zalewski**

Maritime University of Szczecin, Faculty of Navigation, Centre of Marine Traffic Engineering
70-500 Szczecin, ul. Wały Chrobrego 1–2, e-mail: p.zalewski@am.szczecin.pl

**Key words:** GNSS, GPS, signal spoofing, transport security, non-cryptographic defence, satellite compass

**Abstract**
The paper presents an overview of methods for detecting the spoofing of GNSS open service code signals illustrated with the example of C/A GPS signals. GNSS signal spoofing is an attack method where a signal is transmitted that appears authentic but it induces the receiver under attack to compute an erroneous navigation solution, time, or both. Usage of commercially available satellite compasses and two antennas systems for the detection of such threat is described in detail.

## Introduction

Fundamental concepts of Global Navigation Satellite Systems (GNSS), contemporary covering GPS, Glonass, Bejdou, Galileo and their augmentation, evolved from GPS and can be found in [1, 2, 3]. To characterise code GNSS spoofing detection methods the GPS code measurement concept must be analysed.

The GNSS uses a number of satellite transmitters $S_i$ ($i = 1,2,3,\ldots,n$) which geocentric Cartesian locations $X_{Si}$ can be computed for any instant in time (epoch) based on Keplerian orbit model corrected for gravitational perturbations and effects of relativity. Satellite motion model parameters are input as ephemeris data into navigation message modulated onto individual satellite's pseudo-random-noise (PRN) digital code signal using modulo-2 addition procedure. Then, each transmitter, equipped with a synchronized clock offset to the exact system time $t_S$, broadcasts its PRN code modulated onto common frequency carrier radio wave via binary phase shift keying (BPSK) procedure. That is the basis of code division multiple access (CDMA), where several transmitters can send information simultaneously over a single communication channel or sharing a common bandwidth, assuming that propagated PRN codes have time stamps and low auto-/cross-correlation.

Each satellite signal of certain strength $s_i(t)$ propagates with assumed speed of electromagnetic wave in space $c$. A receiver $R$ located at the coordinates $X \in \mathbf{R}^3$ (to be determined) and using an omnidirectional antenna will receive the combined signal of all satellites in range. Due to the properties of the signals $s_i(t)$, the receiver can separate the individual terms of this sum and extract the relative propagated code phase, satellite ID, and data content using a replica of the used PRN code. Given the data and relative phase offsets, the receiver can identify the time delay for each satellite:

$$\begin{aligned}\Delta t_{SiR} &= \frac{1}{c}\left\|X - X_{Si}\right\|_2 = \\ &= \frac{1}{c}\sqrt{\left(x - x_{Si}\right)^2 + \left(y - y_{Si}\right)^2 + \left(z - z_{Si}\right)^2}\end{aligned} \tag{1}$$

where: $\left\|X\right\|_2$ – Euclidean norm of vector $X = [x\ y\ \mathrm{z}]^{\mathrm{T}}$ (matrix notation).

And from that it can calculate "ranges":

$$d_i = c \cdot \Delta t_{SiR} = \left\|X - X_{Si}\right\|_2 \tag{2}$$

Since GNSS receivers are not synchronized with the system time and they generally don't use accurate quartz oscillators, $R$ will have a clock offset $\Delta t_R$ to the exact system time. So the equation (2) will take form:

$$\begin{aligned} p_i &= d_i - c\Delta t_R = \\ &= \sqrt{(x - x_{Si})^2 + (y - y_{Si})^2 + (z - z_{Si})^2} - \delta \end{aligned} \qquad (3)$$

where the receiver can only infer the "pseudo-ranges" $p_i$. "$-\delta$" in eq. (3) determines that positive value of $\delta$ is in advance to the system time (transformed to metric distance) and negative is delayed.

Geometrically equation (3) can be interpreted as a sphere with the centre of $X_{Si}$ and the radius of $p_i + \delta$. The set of equations (3) is over-determined for more than four satellites and generally does not have a unique solution for $X$ because of data noise (propagation, multi-path, technical, unidentified random noise). This noise can be minimized by code differential or carrier phase RTK and static measurements but, in widely available code receivers used in marine and other transportation, it is simply neglected nevertheless satisfying the accuracy of several metres in kinematic applications [4]. So, the problem is limited to the solution of (3). It can be achieved by iterative numerical method after transformation of the set (3) to convex form (set of linear equations) [5] and then usage of weighted least squares estimation technique. Generally, the algorithm looks as follows:

1. Initial approximated (provisional and later estimated) metric values of $x_0$, $y_0$, $z_0$, $\delta_0$ in Cartesian ECEF WGS84 are adopted and related to $x$, $y$, $z$, $\delta$ with unknown adjustment vector $\Delta$:

$$\begin{cases} x = x_0 + \Delta_x \\ y = y_0 + \Delta_y \\ z = z_0 + \Delta_z \\ \delta = \delta_0 + \Delta_\delta \end{cases} \qquad (4)$$

2. The system of linear algebraic equations (SLAE) is built:

$\Delta_x$, $\Delta_y$, $\Delta_z$, $\Delta_\delta$ are new unknowns. Using a Taylor's series expansion of (3) with respect to the approximated point and receiver's clock offset:

$$\begin{aligned} p_i &= f(x,y,z,\delta) = f(x_0,y_0,z_0,\delta_0) + \\ &+ \frac{\partial f(x_0,y_0,z_0,\delta_0)}{\partial x_0}\Delta_x + \frac{\partial f(x_0,y_0,z_0,\delta_0)}{\partial y_0}\Delta_y + \\ &+ \frac{\partial f(x_0,y_0,z_0,\delta_0)}{\partial z_0}\Delta_z + \frac{\partial f(x_0,y_0,z_0,\delta_0)}{\partial \delta_0}\Delta_\delta + \\ &+ \frac{1}{2!}\frac{\partial^2 f(x_0,y_0,z_0,\delta_0)}{\partial {x_0}^2}{\Delta_x}^2 + \ldots \end{aligned} \qquad (5)$$

Equation (5) is intentionally truncated to the linear terms obtained as first partial derivatives:

$$\begin{aligned} a_{i1} &= \frac{\partial f(x_0,y_0,z_0,\delta_0)}{\partial x_0} = \\ &= \frac{x_0 - x_{Si}}{\sqrt{(x_0 - x_{Si})^2 + (y_0 - y_{Si})^2 + (z_0 - z_{Si})^2}} \\ a_{i2} &= \frac{\partial f(x_0,y_0,z_0,\delta_0)}{\partial y_0} = \\ &= \frac{y_0 - y_{Si}}{\sqrt{(x_0 - x_{Si})^2 + (y_0 - y_{Si})^2 + (z_0 - z_{Si})^2}} \\ a_{i3} &= \frac{\partial f(x_0,y_0,z_0,\delta_0)}{\partial z_0} = \\ &= \frac{z_0 - z_{Si}}{\sqrt{(x_0 - x_{Si})^2 + (y_0 - y_{Si})^2 + (z_0 - z_{Si})^2}} \\ a_{i4} &= \frac{\partial f(x_0,y_0,z_0,\delta_0)}{\partial \delta_0} = -1 \end{aligned} \qquad (6)$$

so:

$$\begin{aligned} p_i &= \sqrt{(x_0 - x_{Si})^2 + (y_0 - y_{Si})^2 + (z_0 - z_{Si})^2} + \\ &- \delta_0 + a_{i1}\Delta_x + a_{i2}\Delta_y + a_{i3}\Delta_z + a_{i4}\Delta_\delta \end{aligned} \qquad (7)$$

Separating the unknown and known terms of each side of (7):

$$\begin{aligned} & a_{i1}\Delta_x + a_{i2}\Delta_y + a_{i3}\Delta_z + a_{i4}\Delta_\delta = \\ & = p_i - \sqrt{(x_0 - x_{Si})^2 + (y_0 - y_{Si})^2 + (z_0 - z_{Si})^2} + \delta_0 \end{aligned} \qquad (8)$$

and introducing:

$$b_i = p_i - \sqrt{(x_0 - x_{Si})^2 + (y_0 - y_{Si})^2 + (z_0 - z_{Si})^2} + \delta_0 \qquad (9)$$

we got the SLAE:

$$a_{i1}\Delta_x + a_{i2}\Delta_y + a_{i3}\Delta_z + a_{i4}\Delta_\delta = b_i \qquad (10)$$

or in matrix form: $A \cdot \Delta = B$.

3. The solution vector $\Delta$ to the constructed SLAE is sought:

In general, the set (10) is an overdetermined system. Due to the fact that the actual data contain observational errors and noise, this SLAE is inconsistent. So taking into account the noise vector $\eta$ eq. (10) becomes:

$$A \cdot \Delta = B - \eta \qquad (11)$$

The "noise vector" $\eta$ represents residuals, i.e. differences between observations ($B$) and model ($A \cdot \Delta$). The least squares solution to eq. (11) is:

$$\Delta = (A^T \cdot W \cdot A)^{-1} \cdot A^T \cdot W \cdot B \qquad (12)$$

where $W$ is the diagonal weight matrix diag($w_1$, $w_2$, $w_3$, ... ,$w_n$) which is equal to inverse of a priori covariance matrix of the observations. The values in this matrix are interpreted as weights [0, 1] of individual equations. In many transport receivers these weights are usually somewhat arbitrary assumed to change in respect to elevation angle $\alpha_i$ according to the sample trigonometric formula discussed in [6]:

$$w_i = \frac{1}{2}\left(\sin\left(2\alpha_i - 90°\right) + 1\right) \tag{13}$$

4. If max $|\Delta| > 0.0001$ m (submillimetre solution is usually satisfactory for transport and survey applications) the algorithm is repeated from step 1) substituting previous provisional values of $x_0$, $y_0$, $z_0$, $\delta_0$ with $x_0 + \Delta_x$, $y_0 + \Delta_y$, $z_0 + \Delta_z$, $\delta_0 + \Delta_\delta$.

Finally, the unknowns $x$, $y$, $z$, $\delta$ in set (3) are found.

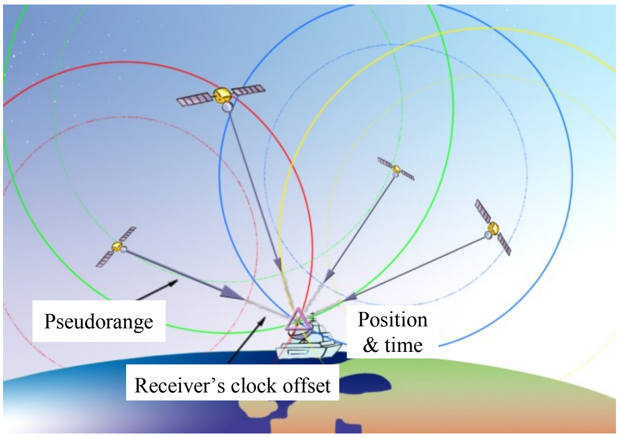


Fig. 1. Geometric representation of GNSS measurement model

## GNSS Spoofing Problem

Since the beginning of present century malicious interference with the civilian GPS signal has been identified as a serious problem. Deliberate jamming and spoofing scenarios, their detection and countermeasures were discussed in several publications [7, 8, 9, 10, 11, 12, 13, 14]. As for scenario, it was identified that discrete spoofing attack would involve four phases [8]:

1. Alignment of the authentic and spoofed GPS signals at the target receiver.
2. Increase the power of the spoofed signals above the authentic.
3. Move the spoofed signals slowly away from the authentic signals.
4. Take complete control of the target receiver's position, velocity and timing (PVT) solution once the spoofed and authentic signals no longer interfere.

During practical research [9, 15, 16] the tested receivers have not successfully defended against this type of attack, if the challenge of gaining accurate knowledge of the target receiver antenna's position and velocity was overcome in step 1). This knowledge required precise positioning counterfeit signals relative to the genuine signals from the target antenna. An attack via portable receiver-spoofer overcomes this difficulty by construction. The receiver-spoofer can be made small enough for inconspicuous placement near the target receiver's antenna. The receiver component draws in genuine GNSS signals to estimate its own position, velocity, and time. Due to proximity, these apply approximately to the target antenna. Based on these estimates, the receiver-spoofer can generate counterfeit signals. The detailed requirements for successful GNSS spoofing attacks have been presented in [12].

Table 1. Spoofing Defences [8]

| Spoofing Defences | | |
|---|---|---|
| Cryptographic | | Non-Cryptographic |
| Stand-Alone | Networked | |
| SSSC on L1C | P(Y) Cross-Correlation | J/N Sensing |
| NMA on L1C, L2C, L5 | | Sensor Diversity |
| SSSC or NMA on WAAS | | Single Antenna Spatial Correlation |
| | | Correlation Anomaly |
| | | Multi-Element Antenna |

Proposed methods for detecting spoofing attacks include examining changes to certain signal characteristics, incorporation of external hardware such as an inertial measurement unit (INS, IMU), use of multiple receiver antennas, or cryptographic techniques. Detailed description of potential spoofing defences has been presented in the table 1 where SSSC stands for spread spectrum security code, NMA is navigation message authentication, J/N is jamming (or spoofing signal) to noise ratio.

The Homeland Security Institute, a research arm of the U.S. Department of Homeland Security, has also considered the threat of civil GPS spoofing [13, 14]. Similarly the U.S. MITRE Organization recommended following techniques to counter spoofing [8]: amplitude discrimination (requires monitoring and recording average and relative signal strength, J/N sensing), time-of-arrival discrimination (requires external timing data from an accurate, continuously running clock to compare to the time derived from the GPS signal), consistency of navigation inertial measurement unit cross-check (requires external accelerometer and compass), polarization discrimination (requires linearly polarized antenna to monitor the change in received signal strength with change in polarization direction), angle-of-arrival discrimination (requires multiple antennas), cryptographic authentication (requires changes to the standard GPS signal). J/N techniques could be implemented in software on GPS receivers, but would be effective against only the most simplistic attacks. Other tactics would be effective against some, but imaginably not all, more sophisticated attacks. However, they require additional hardware.

The best solution to be globally adopted in GNSS seems to be the cryptographic defence, but it is unlikely to be implemented in near future given the static nature of GPS and other GNSS signal definitions. This and J/N Sensing are also the only defences enabling proper work of the receiver under attack by identifying and rejecting false signals.

As for detection methods, practically, angle-of-arrival discrimination, which exploits differential carrier-phase measurements taken between multiple antennas, could only be the one commercially viable, as GNSS compasses and attitude sensors are available for transportation purposes since 1990s [17]. This could be overcome only by a very sophisticated, coordinated attack which theoretically could be performed from distance only, if criteria derived by Tippenhauer et al. [12] are met.

## Spoofing detection by two antennas system

The easiest spoofing attack, and therefore most probably performed, is transmission of a malicious signal from a single point. Respectively the detection of such an attack is also easy (at least theoretically) and the idea of this was developed in [12] and later presented in Poland by Ochin et al. [18]. The work [12] rather concentrated on spoofing generation and the work of Ochin [18] missed necessary detailed mathematical model background to evaluate its usefulness. For maritime two GPS C/A code receivers and two antennas GPS compasses the theory of "single point" spoofing detection is as follows.

The attacker's physical location $X_A \in \mathbf{R}^3$, his transmission time offsets $p_{Ai}$ (transformed to metric distances), and the claimed satellites positions $S_{Ai}$ influence the location $X$ computed by a victim. By setting his physical location $X_A$ and transmission offsets $p_{Ai}$ the attacker can influence the pseudorange measurement at the victim receiver according to the formula:

$$p_i = d_{AR} + p_{Ai} \tag{14}$$

where: $d_{AR}$ – distance between attacker antenna and victim antenna phase centres.

If, as it is assumed, the signal reaches two victim antennas and is transmitted from the same location (Fig. 2) then eq. (14) at both victim antennas (indexed 1 and 2):

$$\begin{aligned} p_{1i} &= d_{1AR} + p_{Ai} \\ p_{2i} &= d_{2AR} + p_{Ai} \end{aligned} \tag{15}$$

and the difference between corresponding satellites pseudoranges in both victim receivers is constant:

$$p_{1i} - p_{2i} = \left| d_{1AR} - d_{2AR} \right| = \text{const.} \tag{16}$$

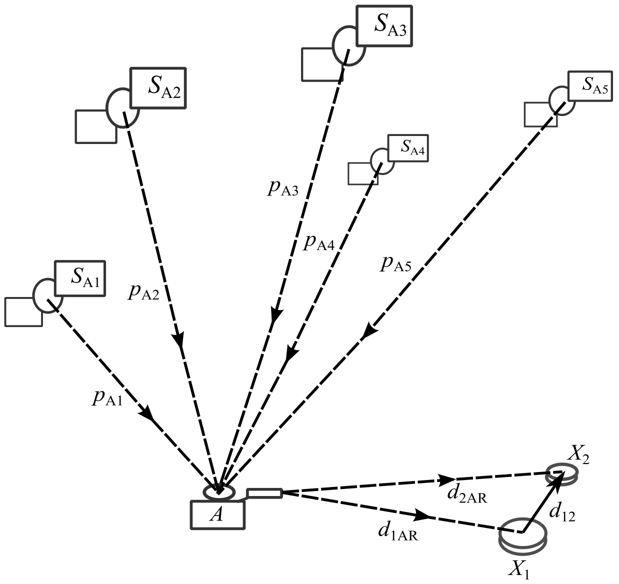


Fig. 2. Reception of spoofed signal transmitted from a single location by two GNSS antennas

After a small transformation of SLAE (10) to:

$$a_{i1}\Delta_x + a_{i2}\Delta_y + a_{i3}\Delta_z = p_i + \Delta_\delta - d_{0i} + \delta_0 \tag{17}$$

one could easily notice that applying identical changes to all $p_i$ will only propagate to changes in unknown $\Delta_\delta$, and not into $\Delta_x$, $\Delta_y$, $\Delta_z$. That is why also the final solution to (3) will only differ in $\delta$ if all $p_i$ are changed by the same value (in case of spoofer this is value from eq. (16)). The numeric simulation example of this problem is provided in the Appendix encoded in Matlab$^{\text{TM}}$.

The conclusion is that using two synchronous GNSS receivers, with separated antennas, the 3D position fixes will be the same but their calculated time offsets $\delta$ will differ exactly by the value from eq. (16). However, the problem is that autonomous (not augmented) code receivers measure signals transmitted from spoofer with different error budget, and even if propagation noise can be neglected (the distances to the spoofer are much smaller than to satellites) still multipath and individual receiver noise during codes correlation is present. Assuming the remaining white noise budget as approx. 1 m the distance between antennas should be approximately 10 times higher (more than 10 m) to obtain statistical confidence of the spoofing attack via criterion:

$$\|X_1 - X_2\| \leq 1 \tag{18}$$

That is consistent with current GPS performance standards [4] which state horizontal error budget for all satellites in view as 9 m (0.95). So overall such receivers / antennas system will calculate eq. (18) as > 1 m (0,95) and if eq. (18) ≤ 1 m (0,95) then alarm should be triggered. Even better results could be achieved with DGPS systems. Practical experiments confirming these fundamentals, but applied to heading measurement, were discussed in [19, 20]. Due to the fact all SOLAS vessels must have several GPS-es onboard, implementation of such spoofing defence should not be a problem and it can be performed by monitoring of the measured distances among GNSS antennas on the flying deck.

Another method, a little more demanding financially, is installation of satellite compass (heading or attitude GPS sensor). The general principle of attitude determination was presented in [9, 17] and in Poland by Felski [21]. It exploits, already mentioned, differential carrier-phase measurements taken between multiple antennas.

Satellite compass produces L1 carrier phase measurements from both antennas referenced to a common internal oscillator. For the satellite $S_i$, an equation for the L1 carrier phase difference $\Delta\varphi_i$ between the two antennas is given (in units of L1 cycles) by:

$$\Delta\varphi_i = D_{12} R_{ENU-B} L + n_i + \delta_b + \gamma_i \tag{19}$$

where:

$D_{12}$ – is the baseline vector between the antennas (in the ship-body frame LLF where $y_b$ to fore, $x_b$ to the starboard, and $z_b$ up) in units of L1 cycles: $D_{12} = [d_{12xb}\ d_{12yb}\ d_{12zb}]^{\mathrm{T}}$. $D_{12}$ can be simplified to $D_{12} = [d_{12}\ 0\ d_{12zb}]^{\mathrm{T}}$ or $D_{12} = [0\ d_{12}\ d_{12zb}]^{\mathrm{T}}$ if the baseline vector is fixed along or athwart ship;

$R_{ENU-B}$ – is the rotation matrix of vectors from the local metric East-North-Up (ENU) frame to the metric body frame (theory behind reference frames coordinates transformations ECEF→ENU→LLF is presented in [22]) (20);

$\theta$, $\phi$ and $\psi$ are the pitch, roll and yaw angles;

$L$ – is the unit line of sight (LOS) vector to $S_i$ in the ENU frame:

$$L = \begin{bmatrix} -\sin\lambda & -\cos\lambda\sin\varphi & \cos\lambda\cos\varphi \\ \cos\lambda & -\sin\lambda\sin\varphi & \sin\lambda\cos\varphi \\ 0 & \cos\varphi & \sin\varphi \end{bmatrix} \tag{21}$$

$\varphi$ and $\lambda$ are either spherical or ellipsoidal coordinates of latitude and longitude;

$n_i$ – is an integer ambiguity of wave period for $S_i$, for the purpose of attitude determination arbitrary set;

$\delta_b$ – is a constant "line bias";

$\gamma_i$ – is the summation of all carrier phase error terms for $S_i$.

Unknown attitude i.e. pitch, roll and yaw (heading) angles and $\delta_b$ are obtained from the solution to the overdetermined set of equations (19) via algorithm corresponding to the one in introduction.

In order to detect a single or even multiple transmitter spoofing attack the monitoring of the $\Delta\varphi_i(t)$ can be implemented into satellite compasses. In case wherein all $\Delta\varphi_i$ or group of several $\Delta\varphi_i$ overlie each other (which occurs during transmission of several satellite signals from single antenna) within an error budget sufficient to accommodate worst-case multipath and carrier noise the spoofing alarm should be triggered. Also monitoring of sudden heading changes in case of single spoofing transmitter should be sufficient.

## Conclusions

Two non-cryptographic methods of spoofing attack detection have been presented. Their strength lies in simplicity of implementation into currently used maritime GNSS code receivers and compasses.

The first one is based on synchronous monitoring of at least two independent receiver-antenna systems. In case of single transmitter spoofer the basis of detection is identity of 3D position fixes in both receivers taking into account remaining receivers' noises. This requires relatively big separation between the receivers' antennas which does not pose a problem onboard marine transport and offshore vessels.

The second one is based on differential carrier-phase measurements taken between two antennas in GNSS compass's systems. The basis of detection is

$$R_{ENU-B} = \begin{bmatrix} \cos\psi\cos\phi - \sin\psi\sin\theta\sin\phi & \sin\psi\cos\phi - \cos\psi\sin\theta\sin\phi & -\cos\theta\sin\phi \\ -\sin\psi\cos\theta & \cos\psi\cos\theta & \sin\phi \\ \cos\psi\sin\phi + \sin\psi\sin\theta\cos\phi & \sin\psi\sin\phi - \cos\psi\sin\theta\cos\phi & \cos\theta\cos\phi \end{bmatrix} \tag{20}$$

identity of phase changes for all (single spoofer) or group (multiple spoofer) satellites. This method seems to be the most universal, but would have to deal with rare cases where the true satellite geometry happens to cause all carrier phase differences to be very close to each other. This situation will occur rarely, but if not handled will lead to a false alarm condition.

It must be stressed that navigators are obliged to position monitoring from two independent sources according to IMO resolutions. During offshore DP classified operations such monitoring is even more redundant (at least three systems for class 2) and performed autonomously by computer control stations. Nevertheless, till autonomous spoofing detection implementation into GNSS, the best way to detect its spoofing is comparison of positions achieved from radar, terrestrial, astro or other radio, laser or hydroacoustic navigation systems and headings from magnetic compasses, gyros or IMUs if available.

## References

1. Hofmann-Wellenhof B., Lichtenegger H., Wasle E.: GNSS – Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and more. Springer-Verlag, 2008.
2. Kaplan E., Hegarty C. (Ed.): Understanding GPS Principles and Applications. Second Edition, Artech House Inc., London 2006.
3. Specht C.: System GPS. In Polish, Wyd. Bernardinum Sp. z o.o, Pelplin 2007.
4. U.S. DoD: GPS Standard Positioning Service Performance Standards. 4th Edition, September 2008.
5. Boyd S., Vandenberghe L.: Convex Optimization. Cambridge University Press, Seventh printing with corrections, U.K., 2009.
6. Zalewski P.: Techniki radionawigacyjne na wodach śródlądowych. In Polish, Logistyka 6/2011, 5117–5130.
7. Daneshmand S., Jafarnia-Jahromi A., Broumandan A., Lachapelle G.: A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array.
8. Humphreys T., Ledvina B., Psiaki M., O'Hanlon B., Kitner P.: Assessing the Spoofing Threat. GPS World, No. 1, January 2009.
9. Montgomery P., Humphreys T., Ledvina B.: Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer. ION 2009 International Technical Meeting, January 26–28, 2009, Anaheim 2009.
10. Scott L.: Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems. ION GNSS, 2003.
11. Shepard D., Humphreys T.: Characterization of Receiver Response to Spoofing Attacks. Proceedings of ION GNSS, Portland, Oregon, 2011.
12. Tippenhauer N., Pöpper C., Rasmussen K., Čapkun S.: 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.
13. Warner J., Johnston R.: GPS Spoofing Countermeasures. U.S. Homeland Security Journal, December 12, 2003.
14. Warner J., Johnston R.: Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. U.S. Homeland Security Journal, December 12, 2003.
15. http://www.engr.utexas.edu/features/humphreysspoofing
16. http://www.engr.utexas.edu/features/superyacht-gps-spoofing
17. Jyh-Ching J., Guo-Shing H.: Development of GPS-Based Attitude Determination Algorithms. IEEE Transactions on Aerospace and Electronic Systems, 33, 3 July 1997.
18. Ochin E., Lemieszewski Ł., Lusznikov E., Dobryakova L.: The study of the spoofer's some properties with help of GNSS signal repeater. Scientific Journals of Maritime University of Szczecin 36(108) z. 2, 2013, 159–165.
19. Zalewski P., Tomczak A.: Method of Probabilistic Evaluation of Ship's Contour Inclusive Area for a Pilot Navigation System. Proc. of 2nd Congress of Seas and Oceans, AM, Szczecin 2005.
20. Zalewski P.: Applying Two DGPS Receivers to the Direction Measurement in Marine Traffic Engineering Research. Proc. of IX International Conference on Marine Traffic Engineering, WSM, Szczecin 2001.
21. Felski A.: Specyfika pomiarów kursu kompasem satelitarnym. In Polish, Zeszyty Naukowe Akademii Marynarki Wojennej w Gdyni, rok LI nr 1 (180), 2010.
22. Noureldin A. et al.: Fundamentals of Inertial Navigation, Satellite-based Positioning and their Integration. Springer-Verlag, Berlin, Heidelberg 2013.

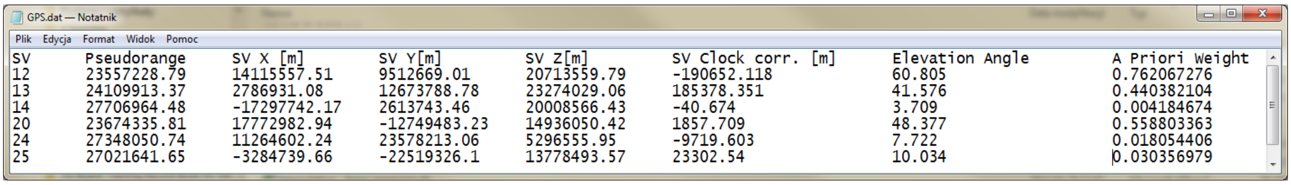
## Appendix

Matlab™ code for simulation of spoofing from single transmitting point by changing pseudoranges with step of 10 m:

```
% Simulation of spoofing from single
  transmitter by change of pseudoranges

% Import of data
GPS = importdata('GPS.dat','\t',1);
c = 299792458;          % m/s
svn = GPS.data(:,1);
prange = GPS.data(:,2); % m
svx = GPS.data(:,3:6);  % m
w = GPS.data(:,8);

% Start of simulation
for count = 1:3
 prange = prange+10;
 % Vector of position provisional esti-
   mates
 x = zeros(1,4);

 % Start of iteration
 dx = ones(1,4);
 dxlimit = 1e-4;
 while max(abs(dx)) > dxlimit

  % Geometric distance
  d = sqrt((x(1)-svx(:,1)).^2+(x(2)-
  svx(:,2)).^2+(x(3)-svx(:,3)).^2);

  % Matrix A (partial derivatives of meas-
  urement model)
  for i = 1:size(svx,1)
   A(i,1) = (x(1)-svx(i,1))/d(i);
   A(i,2) = (x(2)-svx(i,2))/d(i);
  A(i,3) = (x(3)-svx(i,3))/d(i);
  A(i,4) = -1;
 end

% Vector b (measurement minus estimate)
 b = prange+svx(:,4)-d+x(4);

% Vector  dx  (adjustments  to  estimates
  from set: A*dx=b)
 dx = lscov(A,b,w);

% Application of adjustments
 x = x+dx';
end
% DOP calculation
[b,l,h,phi,lambda] = cart2geo(x,5);
D = inv(A'*A);
Dc = D(1:3,1:3);
R = [-sind(phi)*cosd(lambda),
  -sind(phi)*sind(lambda), cosd(phi);
               -sind(lambda),
  cosd(lambda),          0;
       cosd(phi)*cosd(lambda),
  cosd(phi)*sind(lambda), sind(phi)];
Dt = R*Dc*R';
GDOP = sqrt(trace(D));
PDOP = sqrt(trace(Dt));
HDOP = sqrt(Dt(1,1)+Dt(2,2));
VDOP = sqrt(Dt(3,3));
TDOP = sqrt(D(4,4));

% Output of results
fprintf('%3.0f: GDOP =%5.2f PDOP =%5.2f
  HDOP =%5.2f VDOP =%5.2f
  TDOP =%5.2f\n',count,GDOP,PDOP,HDOP,VDO
  P,TDOP);
fprintf('       X =%14.3f m\n',x(1));
fprintf('       Y =%14.3f m\n',x(2));
fprintf('       Z =%14.3f m\n',x(3));
fprintf('    c*dT =%14.3f m\n',x(4));
fprintf('     lat =%4.0f %2.0f
  %8.5f\n',b(1),abs(b(2)),abs(b(3)))
fprintf('     lon =%4.0f %2.0f
  %8.5f\n',l(1),abs(l(2)),abs(l(3)))
 fprintf('       h =%14.3f m\n',h)
 fprintf('      dT =%20.9f s\n\n',x(4)/c);
end
```

```
  1: GDOP = 2.03 PDOP = 1.84 HDOP = 1.18
   VDOP = 1.42 TDOP = 0.85
         X =   3326447.888 m
         Y =   -177061.064 m
         Z =   5421000.234 m
      c*dT =  -2291527.533 m
       lat =  58 36  3.75553
       lon =  -3  2 48.76740
         h =        99.577 m
        dT =        -0.007643713 s

  2: GDOP = 2.03 PDOP = 1.84 HDOP = 1.18
   VDOP = 1.42 TDOP = 0.85
         X =   3326447.888 m
         Y =   -177061.064 m
         Z =   5421000.234 m
      c*dT =  -2291537.533 m
       lat =  58 36  3.75553
       lon =  -3  2 48.76740
         h =        99.577 m
        dT =        -0.007643746 s

  3: GDOP = 2.03 PDOP = 1.84 HDOP = 1.18
   VDOP = 1.42 TDOP = 0.85
         X =   3326447.888 m
         Y =   -177061.064 m
         Z =   5421000.234 m
      c*dT =  -2291547.533 m
       lat =  58 36  3.75553
       lon =  -3  2 48.76740
         h =        99.577 m
        dT =        -0.007643780 s
```

Contents of file "GPS.dat" retrieved from RINEX navigation (satellite positions calculated from ephemerides) and observation files for fixed epoch:



```
SV      Pseudorange     SV X [m]        SV Y[m]         SV Z[m]         SV Clock corr. [m]      Elevation Angle         A Priori Weight
12      23557228.79     14115557.51     9512669.01      20713559.79     -190652.118             60.805                  0.762067276
13      24109913.37     2786931.08      12673788.78     23274029.06     185378.351              41.576                  0.440382104
14      27706964.48     -17297742.17    2613743.46      20008566.43     -40.674                 3.709                   0.004184674
20      23674335.81     17772982.94     -12749483.23    14936050.42     1857.709                48.377                  0.558803363
24      27348050.74     11264602.24     23578213.06     5296555.95      -9719.603               7.722                   0.018054406
25      27021641.65     -3284739.66     -22519326.1     13778493.57     23302.54                10.034                  0.030356979
```