Scientific Journals
Maritime University of Szczecin

Zeszyty Naukowe
Akademia Morska w Szczecinie

2013, 36(108) z. 2 pp. 159–165
ISSN 1733-8670

2013, 36(108) z. 2 s. 159–165

The study of the spoofer's some properties with help of GNSS signal repeater

Evgeny Ochin[1], Łukasz Lemieszewski[1], Eugeniusz Lusznikov[1], Larisa Dobryakova[2]

[1] Maritime University of Szczecin, Faculty of Navigation
70-500 Szczecin, ul. Wały Chrobrego 1–2, e-mail: e.ochin@am.szczecin.pl
[2] West Pomeranian University of Technology, Faculty of Computer Science and Information Technology
71-210 Szczecin, ul. Żołnierska 49, e-mail: ldobryakova@wi.zut.edu.pl

Key words: satelite navigation systems, transport equipment, spoofer, spoofing detection algorithm, signal receiver

Abstract
Satellite navigation systems are widely used in navigation for precise trajectory determination of transport equipment. In this article mathematical models and algorithms have been developed to solve the problems of precision and safety of satellite navigation. One of the problems is spoofing (substitution) – a situation in which a system (hardware, software, etc.) successfully masquerades as another by falsifying data system and performs illegal actions. What is considered in the paper is spoofing detection algorithm based on the analysis of a civil satellite signal generated by the two receivers but instead a fully functional Spoofer GNSS signal repeater was used.

This work is intended to equip GNSS users and receiver manufacturers with authentication methods that are effective against unsophisticated spoofing attacks. The work also serves to refine the civilian spoofing threat assessment by demonstrating the challenges involved in mounting a spoofing attack.

Notation and basic definitions[1]

GNSS– Global Navigation Satellite System.

NS_i – Navigation Spacecraft, $i = \overline{1,N}$, N – number of NS.

$(x_i\, y_i, z_i)$, $i = \overline{1,N}$ – true known location NS.

$(x_0\, y_0, z_0)$ – true unknown location of Vehicles.

TCM_j, $j = \overline{1,2}$ – Transceiver-Computing Module of GNSS.

ρ_i, $i = \overline{1,N}$ – true (exact) distance from GNSS-receiver into NS_i (for the static objects ρ_i can be known, but in general, are unknown quantities).

$\hat{\rho}_i$, $i = \overline{1,N}$ – pseudorange[2] from GNSS-receiver into NS_i.

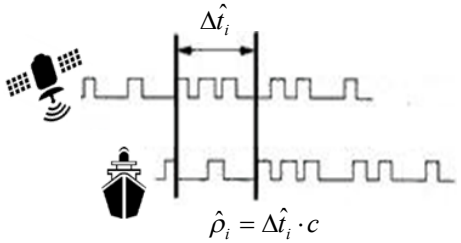

Fig. 1. Pseudorange $\hat{\rho}_i$ from GNSS-receiver into NS_i

$\Delta\rho_i = \rho_i - \hat{\rho}_i$, $i = \overline{1,N}$ – error in determining of ρ_i.

Additional designations for couples GNSS-receivers:

$\hat{\rho}_{1,i}$, $i = \overline{1,N}$ – pseudoranges from TCM_1 to NS_i;

$\hat{\rho}_{2,i}$, $i = \overline{1,N}$ – pseudoranges from TCM_2 to NS_i;

[1] All definitions are in accordance with the [1] and [2].

[2] Pseudorange is the *pseudo* distance between a satellite and a navigation satellite receiver. To determine its position, a satellite navigation receiver will determine the ranges to (at least) four satellites, as well as their positions at the time of transmitting. Knowing the satellites orbital parameters, these positions can be calculated for any point in time. The pseudoranges of each satellite are obtained by multiplying the speed of light by the time the signal has taken from the satellite to the receiver. As there are accuracy errors in the time measured, the term pseudo-ranges is used rather than ranges for such distances.

$(\hat{x}_1, \hat{y}_1, \hat{z}_1)$ – measured coordinates TCM_1;
$(\hat{x}_2, \hat{y}_2, \hat{z}_2)$ – measured coordinates TCM_2;
$(\tilde{x}_0, \tilde{y}_0, \tilde{z}_0)$ – false coordinates TCM_0;
$(\tilde{x}_1, \tilde{y}_1, \tilde{z}_1)$ – false coordinates TCM_1;
$(\tilde{x}_2, \tilde{y}_2, \tilde{z}_2)$ – false coordinates TCM_2;
D_{1-2} – the true distance between TCM_1 and TCM_2;
$\hat{D}_{1-2} = \sqrt{(\hat{x}_1 - \hat{x}_2)^2 + (\hat{y}_1 - \hat{y}_2)^2 + (\hat{z}_1 - \hat{z}_2)} + c\tau$ – measured the distance between TCM_1 and TCM_2;
τ – displacement of the consumer's timeline and system time;
SD – Spoofing Detector.

Introduction

There are various approaches to design and production of the spoofer. An example is shown in figure 2. The Spoofing methods can be divided into two main categories [3, 4].

The Spoofers based on simulators of GNSS-signals

In this category of Spoofers [5] GNSS signal simulator is combined with the RF interface to mimic the original GNSS-signals. The signals generated by such a spoofer is not synchronized with the real GNSS-signals. Thus, the signals of spoofer look like noise for a receiver operating in the tracking mode (even if the power exceeds the power of authentic spoofer signals). Nevertheless, this type can effectively spoof commercial GNSS-receivers, especially, if the signal power exceeds the power of genuine signals. GNSS signal simulator is the simplest GNSS-spoofer and it can be detected by various methods such as anti-spoofing amplitude monitoring, checking consistency between different measurements and data integrity checking with inertial measurement units (IMUS).

The Spoofers based on reservoir of GNSS-signals

A more advanced type of spoofer consists of a receiver GNSS, coupled with the transmitter. This

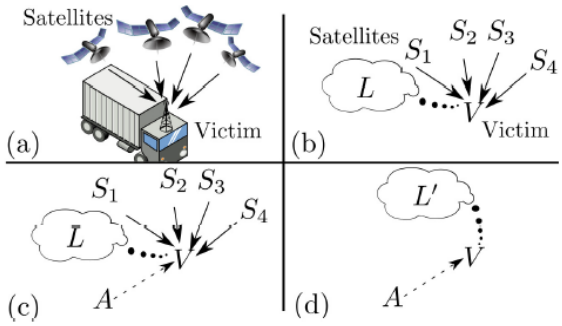

Fig. 3. The main scenario of the Spoofing: (a) vehicle travels in normal GNSS-navigation; (b) schematic representation of a scene (a); (c) jamming of GNSS- signals and starts sending the false GNSS-signals; (d) navigator of the vehicle switched to false GNSS-signals [6]

system is synchronized with the current GNSS-signals, it determines the position and time of satellite ephemeris, and then generates a signal substitution. This kind of a spoofer is difficult to distinguish from genuine signals and it is more complicated than the first category. The main problem in implementing this type of spoofing is calculating correct signal delay and power. It should be noted that the spoofer signal power should be slightly higher than the original signal power in order to successfully mislead the target receiver, but it should not be much larger than the typical signal power GNSS. Thus, it would be a great advantage for this type of a spoofer if the antenna of the spoofer was close to the antenna of the attacked receiver. This type of a spoofer is relatively difficult to detect, since they are synchronized with the actual satellite GNSS and receivers can mimic in the tracking mode.

The composite signal received by the antenna is:

$$S_{\text{ant}} = S_a + S_s + S_N \tag{1}$$

where S_a – genuine signal, S_s – false signal and S_N – noise. If $S_s >> S_a$, it can be assumed that $S_{\text{ant}} \approx S_s + S_N$.

The most common scenario of the Spoofing is depicted in figure 3.

A spoofer is a complex technical device. The easiest way to implement a spoofer is to use a GNSS-simulator. The acquisition of such a simu-

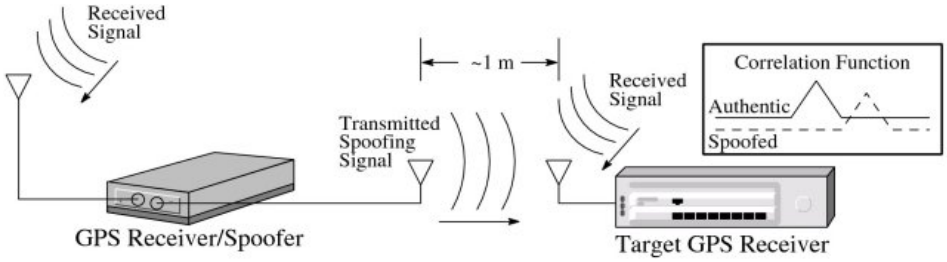

Fig. 2. Example of a spoofer's construction according UAS Vision [7]

lator is associated with significant financial costs. As a result of theoretical research, we came to the conclusion that for the purposes of testing many spoofing detection systems can use repeaters of GNSS-signals (the relays). The purpose of this article is to describe this approach.

Spoofing detection by measuring the distance between a pair of antennas NS

The coordinates of GNSS-receiver ($x_0\, y_0,\, z_0$) are unknown, therefore, theoretically true (exact) distance from the GNSS-receiver to NS_i measured as:

$$\rho_i = \Delta t_i \cdot c \tag{2}$$

where Δt_i – true (exact) signal propagation time from the GNSS-receiver into NS_i; c – speed of light.

It is known that there are many reasons because of which the accurate measurement of Δt_i impossible. Therefore, GNSS-receiver estimates the delay between the GNSS-receiver and NS_i with error:

$$\Delta t_i = \Delta \hat{t}_i + \varepsilon_i \tag{3}$$

where ε_i – unknown true measurement error of signal propagation time between the GNSS-receiver and NS_i.

Substituting (3) into (2), we obtain:

$$\rho_i = \left(\Delta \hat{t}_i + \varepsilon_i\right)\cdot c = \hat{\rho}_i + \varepsilon_i \cdot c \tag{4}$$

where $\hat{\rho}_i = \Delta \hat{t}_i \cdot c$ – approximate distances from GNSS-receiver into NS_i (pseudoranges).

Due to the fact that the true value ρ_i unknown, it is unknown and the true error $\Delta\rho_i = \varepsilon_i \cdot c$. Therefore, the task of finding the true value ρ_i formulated as the problem of finding some approximation to the true value, that is, as the computation of pseudorange:

$$\begin{aligned} &\hat{\rho}_i = \rho_i - \Delta\rho_i = \\ &\sqrt{\left(x_i - x_0\right)^2 + \left(y_i - y_0\right)^2 + \left(z_i - z_0\right)^2} - \Delta\rho_i \\ &\xrightarrow{\text{Iterative algorithm}} \left(x_0, y_0, z_0\right) \end{aligned} \tag{5}$$

As $\Delta\rho_i$ is an unknown quantity, instead of the exact value ($x_i\, y_i,\, z_i$) obtain approximate measurements ($\hat{x}_1, \hat{y}_1, \hat{z}_1$):

$$\begin{aligned} &\hat{\rho}_i = \rho_i - \Delta\rho_i = \\ &\sqrt{\left(x_i - \hat{x}_0\right)^2 + \left(y_i - \hat{y}_0\right)^2 + \left(z_i - \hat{z}_0\right)^2} \\ &\xrightarrow{\text{Iterative algorithm}} \left(\hat{x}_0, \hat{y}_0, \hat{z}_0\right) \end{aligned} \tag{6}$$

We assume that the two receiving-processing modules TCM_1 and TCM_2 independently make the coordinate measuring of own antenna A_1 and A_2 in accordance with (6):

$$\begin{cases} \left(\hat{x}_1, \hat{y}_1, \hat{z}_1\right) \\ \left(\hat{x}_2, \hat{y}_2, \hat{z}_2\right) \end{cases} \tag{7}$$

The measurement results differ by some unknown but substantially different values and thus the distance score $\hat{D}_{1-2}$ between the antennas will be D_{1-2} (Fig. 4):

$$\hat{D}_{1-2} = \sqrt{\left(\hat{x}_1 - \hat{x}_2\right)^2 + \left(\hat{y}_1 - \hat{y}_2\right)^2 + \left(\hat{z}_1 - \hat{z}_2\right)^2} \geq D_{1-2} \tag{8}$$

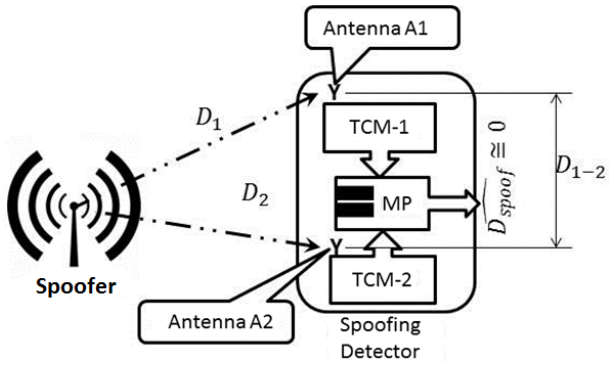

Fig. 4. The single-antenna Spoofer and two-antenna Spoofing Detector (SD): Y – antenna SD; D_1 and D_2 distance from the spoofer's antenna to antenna of SD, MP – microprocessor that calculates the distance between the antennas and implements the decision rule (18 or 19); D_{1-2} – the true distance between the antennas

Detection in mode of spoofing

The pseudorange from antennas A_1 and A_2 into NS_i can be represented as:

$$\left.\begin{aligned} &\hat{\rho}_{1,i} = \rho_{1,i} - \Delta\rho_{1,i} = \\ &= \sqrt{\left(x_i - \hat{x}_1\right)^2 + \left(y_i - \hat{y}_1\right)^2 + \left(z_i - \hat{z}_1\right)^2} \\ &\hat{\rho}_{2,i} = \rho_{2,i} - \Delta\rho_{2,i} = \\ &= \sqrt{\left(x_i - \hat{x}_2\right)^2 + \left(y_i - \hat{y}_2\right)^2 + \left(z_i - \hat{z}_2\right)^2} \end{aligned}\right\}, \; i = \overline{1, N} \tag{9}$$

where $\rho_{1,i}$ and $\rho_{2,i}$ – the true distance from the antennas A_1 and A_2 into NS_i; $\Delta\rho_{1,i}$ and $\Delta\rho_{2,i}$ – unknown errors of distances from the antennas A_1 and A_2 into NS_i. Solutions of system's equations (9) are the coordinates estimation of antennas A_1 and A_2:

$$\begin{aligned} &\left.\begin{aligned} &\hat{\rho}_{1,i} = \rho_{1,i} - \Delta\rho_{1,i} \\ &\hat{\rho}_{2,i} = \rho_{2,i} - \Delta\rho_{2,i} \end{aligned}\right\}, \; i = \overline{1, N} \\ &\xrightarrow{\text{Iterative algorithm}} \begin{pmatrix} \hat{x}_1, \hat{y}_1, \hat{z}_1 \\ \hat{x}_2, \hat{y}_2, \hat{z}_2 \end{pmatrix} \end{aligned} \tag{10}$$

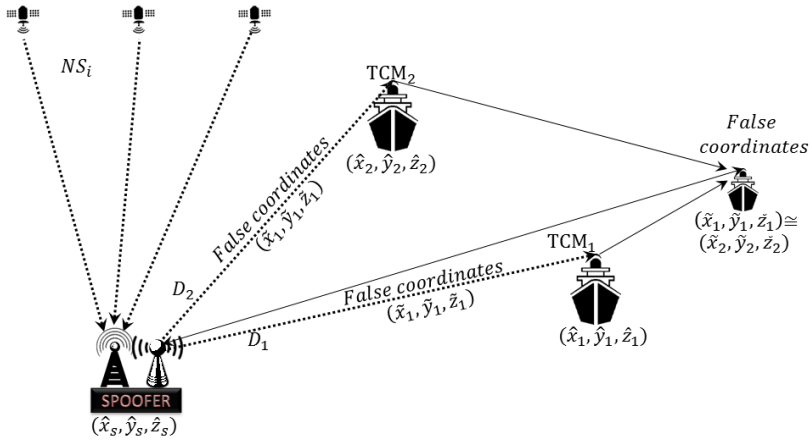

Fig. 5. The pseudoranges TCM$_1$ and TCM$_2$ in mode of spoofing

The main properties of the detection in mode of spoofing

The property 1

The difference between pseudoranges $\hat{\rho}_{1,i} - \hat{\rho}_{2,i}$ *from antennas* A$_1$ *and* A$_2$ *into* NS$_i$[3] *is equal to the difference in distance from the antennas* A$_1$ *and* A$_2$ *into antennas of spoofer, that is:*

$$\hat{\rho}_{1,i} - \hat{\rho}_{2,i} = D_1 - D_2, \quad i = \overline{1,N} \tag{11}$$

The proof of property 1

The pseudorange from antennas A$_1$ and A$_2$ into NS_i can be represented as:

$$\begin{pmatrix} \hat{\rho}_{1,i} = \hat{\rho}_{s,i} + \Delta\hat{\rho}_{s,i} + c\tau + D_1 \\ \hat{\rho}_{2,i} = \hat{\rho}_{s,i} + \Delta\hat{\rho}_{s,i} + c\tau + D_2 \end{pmatrix}, \; i = \overline{1,N} \tag{12}$$

where: $\hat{\rho}_{s,i}$ – pseudoranges of spoofer; $\Delta\hat{\rho}_{s,i}$ – artificial errors introduced in the pseudoranges $\hat{\rho}_{s,i}$; c – speed of light; τ – the propagation time of the signal from the GNSS-antenna of spoofer through his amplifier to the transmitting antenna of spoofer; D_1, D_2 – distance from the transmitting antenna of spoofer to the TCM$_1$ and TCM$_2$ respectively (Fig. 5).

The difference between pseudoranges from antennas A$_1$ and A$_2$ into NS$_i$ is equal:

$$\hat{\rho}_{1,i} - \hat{\rho}_{2,i} = D_1 - D_2, \quad i = \overline{1,N} \tag{13}$$

The property 2

The unknown errors $\Delta\rho_{1,i}$ *and* $\Delta\rho_{2,i}$ *of measuring the distances from the antenna* A$_1$ *and* A$_2$ *into* NS$_i$ *are the same, that is:*

$$\Delta\rho_{1,i} = \Delta\rho_{2,i}, \quad i = \overline{1,N} \tag{14}$$

The proof of property 2

The single-antenna spoofer cannot convey the difference between the measurement errors for two or more points in space. Signals from the spoofer in any two points in space are different from each other only by the delayed signal level. The difference signal can be neglected since near antennas A$_1$ and A$_2$ (~1÷2 m).

The property 3

The apparent distance between the antennas TCM$_1$ *and* TCM$_2$ *in mode of spoofing is approximately zero, i.e.:*

$$\hat{D}_{1-2} = \overrightarrow{\tilde{x}_1, \tilde{y}_1, \tilde{z}_1} - \overrightarrow{\tilde{x}_2, \tilde{y}_2, \tilde{z}_2} \cong 0 \tag{15}$$

The proof of property 3

On the basis of its own measured coordinate $(\hat{x}_s, \hat{y}_s, \hat{z}_s)$ and some (possible visual) coordinates estimation of vehicle V_1 spoofer defines false coordinates $\tilde{x}_1, \tilde{y}_1, \tilde{z}_1$ of vehicle V_1, which have TCM$_1$.

Solving the problem, which is inverse problem of (6), spoofer makes modifications in the pseudoranges so that TCM$_1$ calculated to false coordinates[4]:

$$\begin{aligned} &\hat{\rho}_i = \rho_i - (\Delta\rho_i + e_i) = \\ &= \sqrt{(x_i - \hat{x}_0)^2 + (y_i - \hat{y}_0)^2 + (z_i - \hat{z}_0)^2} \\ &\xrightarrow{\text{Iterative algorithm}} (\tilde{x}_1, \tilde{y}_1, \tilde{z}_1) \end{aligned} \tag{16}$$

where e_i – modifications in the pseudoranges, introduced by spoofer.

As a result, TCM$_1$ determines false coordinates (Fig. 5). If in the area there is one more vehicle V_2 with TCM$_2$, then also for TCM$_2$ the spoofer will generate the same false coordinates $(\tilde{x}_1, \tilde{y}_1, \tilde{z}_1)$.

[3] It is necessary to clarify that the spoofer generates artificial GNSS-signals based on real almanac.

[4] In this article the scenarios and algorithms of spoofer are not considered.

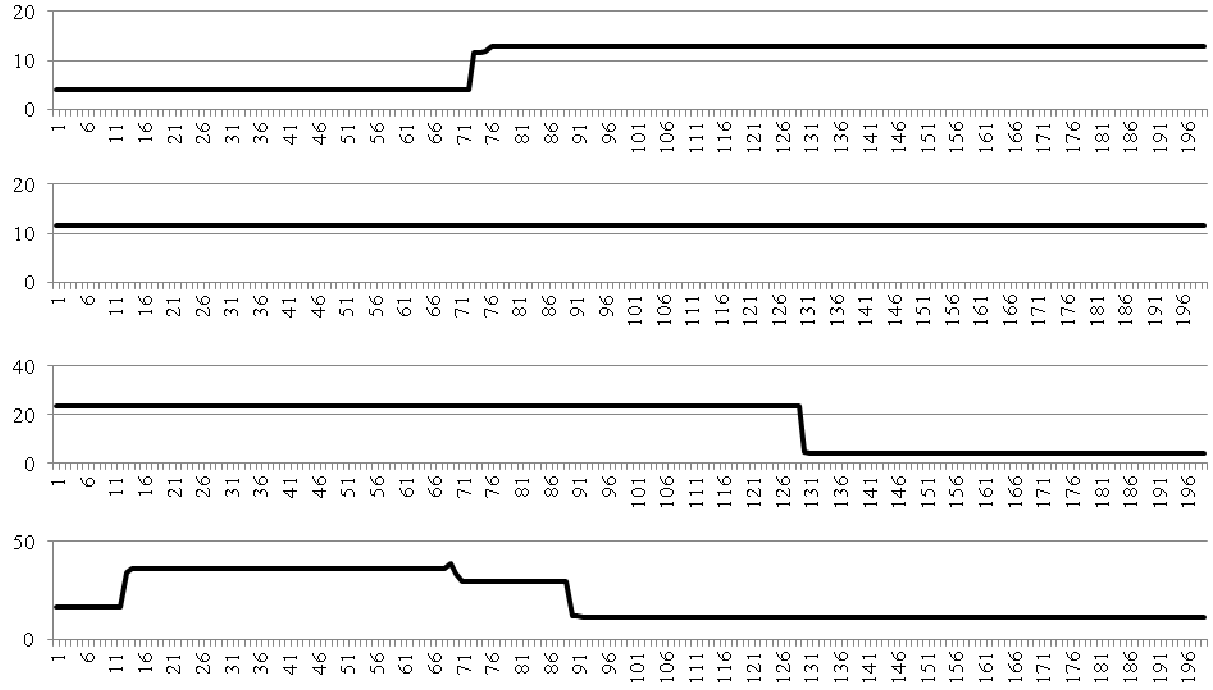

Fig. 6. The measured distance between the antennas in the mode of "Spoofing", while the actual distance between the antennas was equal D_{1-2} = 4 cm (the two top graphs) and D_{1-2} = 100 cm (the two bottom graphs)

Thus, measured coordinate of the two TCM_1 and TCM_2 will be similar:

$$\overrightarrow{\tilde{x}_1, \tilde{y}_1, \tilde{z}} \cong \overrightarrow{\tilde{x}_2, \tilde{y}_2, \tilde{z}_2} \tag{17}$$

The decision rule No. 1

Comparing (8) and (15) can be written the spoofing detection decision rule:

$$\text{if } \sigma_k \le \breve{D} \text{ then } \langle \text{Spoofing} \rangle \text{ else } \langle \text{GNSS} \rangle \tag{18}$$

where:

$\sigma_k = \sqrt{\frac{1}{N}\sum_{i=k}^{k+N}\left\{\left(\hat{D}_{1-2}\right)_i - \left(\hat{D}_{1-2}\right)_k\right\}}$ – standard deviation of the measured distance between the antennas on the moving interval of N measurement; $\overline{\left(\hat{D}_{1-2}\right)_k}$

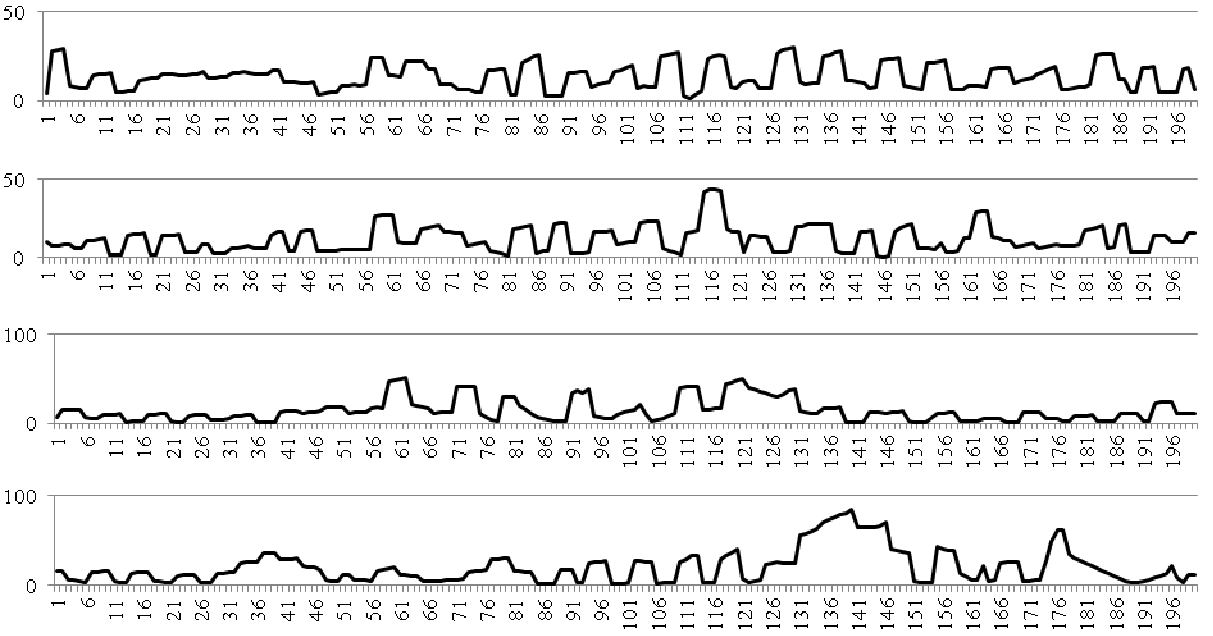

Fig. 7. The measured distance between the antennas in the mode of "GNSS", while the actual distance between the antennas was equal D_{1-2} = 4 cm (the two top graphs) and D_{1-2} = 100 cm (the two bottom graphs)

– the average value of measured distances between the antennas on the moving interval of N measurement; $\breve{D}$ – discriminant, determined on the basis of statistical studies in the design phase of a real system detection.

A significant difference of standard deviation of the measured distance between the antennas in the modes "GNSS" and "Spoofing" show graphs on figures 6–9. It should be noted that the actual distance between the antennas has little influence on the results of spoofing detection.

The results of measurements of the distance between the antennas in the mode of "GNSS" correspond to the standard representations of the accuracy of the measurement locations of vehicles.

The histogram of the measured distance between the antennas in the mode of "GNSS" shows smoothly varying nature of the change of the measured distances (Fig. 8).

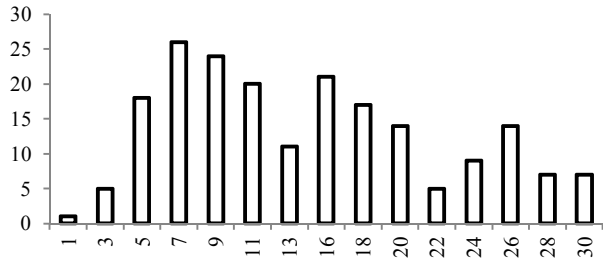

Fig. 8. Typical histogram of measured distances between the antennas in the mode "GNSS"

The results of measuring the distance between antennas in mode of "Spoofing" are characterized by relatively long sections of constancy of the measured distances between the antennas. This property shows a typical histogram (Fig. 9).

A histogram of the measured distance between the antennas in the mode "Spoofing" shows the abrupt nature of the change of the measured distances.

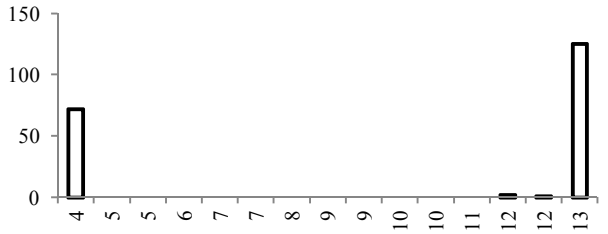

Fig. 10. The typical histogram of the measured distances between antennas in mode "Spoofing"

The decision rule No. 2

The rule No. 1 can give rise to two well-known in the theory of statistical decision-making situations.

False alarm – in the absence of spoofing SD takes a wrong decision ⟨Spoofing⟩.

Skip goal – SD is under attack spoofing, but does not "see" spoofing and decides ⟨GNSS⟩.

To minimize the probability a false alarm and missing the target decision rule number 1 can be modified as follows:

$$\begin{cases} \langle \text{Spoofing} \rangle, \ \sigma_k \le \left(\breve{D} - k\breve{D}\right) \\ \langle ? \rangle, \ \left(\breve{D} - k\breve{D}\right) < \sigma_k < \left(\breve{D} + k\breve{D}\right) \\ \langle \text{GNSS} \rangle, \ \sigma_k \ge \left(\breve{D} + k\breve{D}\right) \end{cases} \qquad (19)$$

where ⟨?⟩ – area of uncertainty, where solution temporarily cannot be decided; k – allowable ratio of non-acceptance solutions, determined on the basis of statistical studies in the design phase of a real system detection.

The main properties of the repeater of real GNSS-signals

Change the scheme of the experiment (Fig. 4) as follows. Instead of a full-function spoofer will use repeaters (Fig. 10). In this case, the main function of the spoofer – the generation of false GNSS-

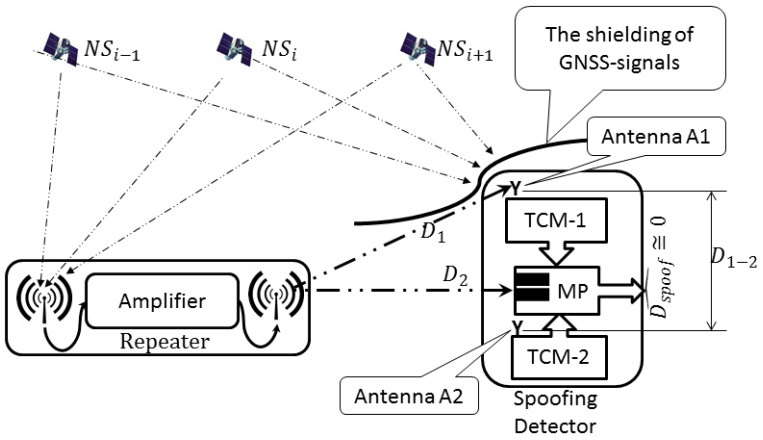

Fig. 9. The GNSS-signal repeater as the physical models of some properties of spoofer

signals is not possible. However, there remains an important property for the purpose of measuring the distance between two antennas TCM, connected with the fact that the repeater broadcasts a GNSS-signal via one antenna, unlike the GNSS-signal a plurality of antennas in normal navigation. Note that this change does not alter the properties (11, 14 and 15), but changes the proof of *Properties 1*.

For shielding of the electromagnetic waves a standard shipping container was used (Fig. 11).

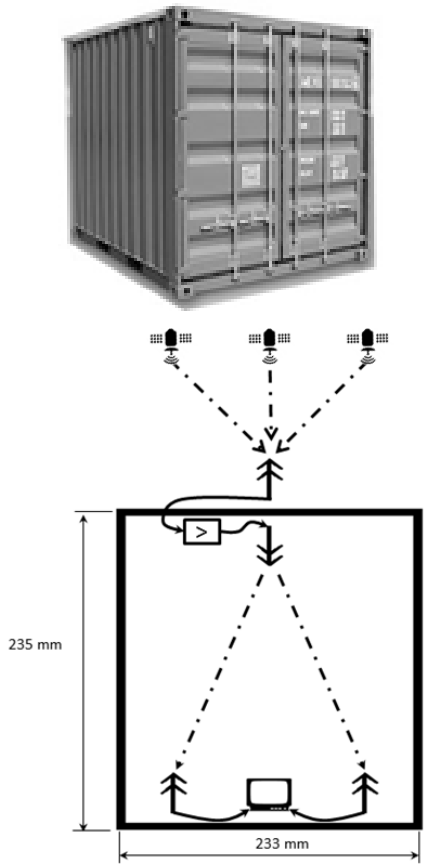

Fig. 11. The standard 10-foot sea container (10' Dry Freight Container) and experimental scheme: ↟ — installed on the roof of the container GNSS-antenna; through a hole of 5 mm diameter cable is held in a container, the signal is amplified and transmitted by the transmitting antenna ↓ on the ceiling of the container; there is a navigator equipped with two antennas with receivers located on the floor of the container ↟ ↟; positioning results are entered into the computer, which is measured by the distance between the antennas navigators.

The proof of property 1 for the use of a repeater

The difference between pseudoranges $\hat{\rho}_{1,i} - \hat{\rho}_{2,i}$ from antennas A_1 and A_2 into NS_i consists of the *actual* path of the signal from NS_i into repeater and the actual path from the transmitting antenna to the repeater antennas A_1 and A_2 (Fig. 11), that is:

$$\begin{aligned}\hat{\rho}_{1,i} - \hat{\rho}_{2,i} &= \left(D_{\text{NS}-\text{spoofer}} + D_1\right) + \\ &- \left(D_{\text{NS}-\text{spoofer}} + D_2\right) = D_1 - D_2\end{aligned} \tag{20}$$

The conclusion of the proof of property 1 for the use of a repeater

The decision rules spoofing detection (18 and 19) has not changed.

Conclusions

This approach to modeling of some physical properties of the spoofer is described for the first time and allows you to proceed with the engineering design of real systems for spoofing detection.

References

1. GPS Standard Positioning Service (SPS) Performance Standard. 4th Edition (now in effect), September 2008.
2. The Global Navigation Satellite Systems. Ship multi-system, multi-channel GNSS user equipment GLONASS /GPS/GALILEO. Technical specifications, methods of testing and required test results. National Standard of the Russian Federation, GOST P 54119-2010.
3. MONTGOMERY P.Y., HUMPHREYS T.E., LEDVINA B.M.: Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil. GPS Spoofer ION 2009 International Technical Meeting, 2009.
4. JAFARNIA-JAHROMI A., BROUMANDAN A., NIELSEN J., LACHAPELLE G.: GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. Hindawi Publishing Corporation International Journal of Navigation and Observation, Vol. 2012, Article ID127072.
5. http://www.rohde-schwarz.com/en/product/gnss-product startpage_63493-11461.html
6. http://diydrones.com/profiles/blogs/how-to-spoof-gps-to-potentially-take-over-a-drone
7. http://goo.gl/lkZDJ

Others

8. SPECHT C.: System GPS. Biblioteka Nawigacji nr 1. Wydawnictwo Bernardinum. Pelplin 2007.
9. COCARD M.: High precision GPS processing in kinematic mode. Schweizerischen Geodätischen Kommission, Zweiundfünfzigster Band, Vol. 52, 1995.
10. OCHIN E., DOBRYAKOVA L., LEMIESZEWSKI Ł.: Antiterrorism – design and analysis of GNSS antispoofing algorithms. Scientific Journals Maritime University of Szczecin 30(102), 2012, 93–101.
11. http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer (December 15, 2011).
12. Countermeasures for GPS signal spoofing. University of Oklahoma (2004). http://www.blockyourid.com/~gbpprorg /mil/gps4/Wen Spoof.pdf
13. Countermeasures for GPS signal spoofing Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. ION GNSS, 2008, http://web.mae.cornell.edu/psiaki/humphreys etal iongnss2008.pdf
14. Countermeasures for GPS signal spoofing Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer // ION GNSS, 2008, http://web.mae.cornell.edu/psiaki/humphreys etal iongnss2008.pdf
15. http://radionavlab.ae.utexas.edu/videos