Scientific Journals
Maritime University of Szczecin

Zeszyty Naukowe
Akademia Morska w Szczecinie

2014, 40(112) pp. 47–52
ISSN 1733-8670

Design and analysis of spoofing detection algorithms for GNSS signals

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

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

Key words: GNSS, GPS, NAVSTAR, GLONASS, Spoofing, Dual-Receiver

Abstract

Many civil GNSS (Global Navigation Satellite System) applications need secure, assured information for asset tracking, fleet management and the like. But there is also a growing demand for geosecurity location-based services. Unfortunately, GNSS is vulnerable to malicious intrusion and spoofing. How can users be sure the information they receive is authentic? Spoofing is the transmission of matched-GNSS-signal-structure interference in an attempt to commandeer the tracking loops of a victim receiver and thereby manipulate the receiver's timing or navigation solution. A spoofer can transmit its counterfeit signals from a stand-off distance of several hundred meters or it can be co-located with its victim. Spoofing attacks can be classified as simple, intermediate, or sophisticated in terms of their effectiveness and subtlety. In an intermediate spoofing attack, a spoofer synchronizes its counterfeit signals with the authentic GNSS signals so they are code-phase-aligned at the target receiver. In this paper we consider the anti-spoofing algorithms based on spoofing detection via Dual-Receiver.

Introduction

The main requirement for a navigation system is the ability to continuously determine the coordinates of the object with the required of precision. However, during the exploitation GNSS (Global Navigation Satellite System) the situations of the refusal of communication satellites or ground-based control system may arise. The refusals may lead to the state in which coordinates of object will determine some errors, excess of desired coordinates, therefore to assess the GNSS situation the concept of GNSS **totality** and **continuity** should be used [1].

Many civilian GNSS applications require confidence that the information on asset tracking, fleet management, etc. **is not counterfeit**. Noteworthy is the growing demand for the safety of geo-location based services. Unfortunately, civilian GNSS signal is vulnerable to formulate and modify the data packets. The question arises: how users can be confident that the information they receive is authentic? Spoofer can transmit fake signal to hide within a few hundred meters or be co-located with the victim.

In this article, we consider the algorithm of spoofing detection based on the analysis of the satellite signal for civilian use of **Dual-Receiver**. During the operation, the algorithm compares the distance of received signals from two receivers.

A real-time method for detecting GNSS spoofing in a narrow-bandwidth civilian GNSS receiver is still being developed. The ability to detect a spoofing attack is important for reliability of systems ranging from cell-phone towers, the power grid, and commercial fishing monitors. A civilian GNSS spoofer is implemented on a digital signal processor. It is used to characterize spoofing effects and to develop ways of defense against civilian spoofing.

This work is intended to equip GNSS users and receiver manufacturers with authentication methods that are effective in dealing with unsophisticated

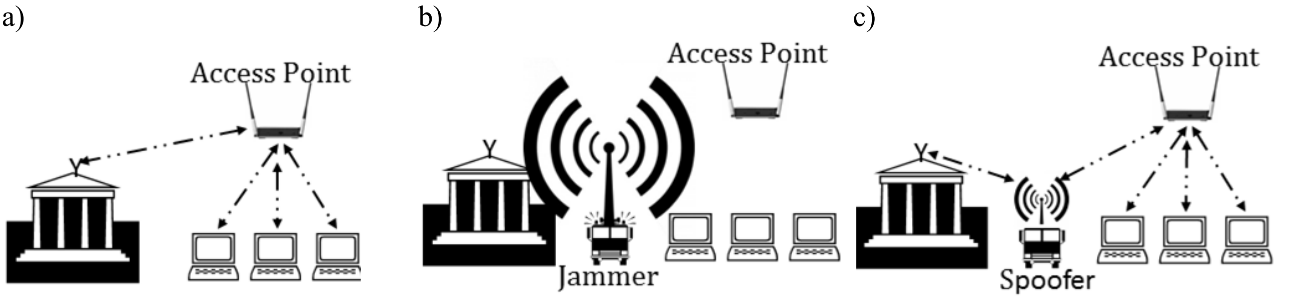

Fig. 1. Network before Spoofing (a), during Jamming (b), during Spoofing (c)

spoofing attacks. In this paper we consider the anti-spoofing algorithms based on spoofing detection via Dual-Receiver.

Spoofing is a technology to intercept network traffic between nodes, arranged in a single wide-domain transmission. The beginnings of anti-spoofing, can be seen in the patent 1942 [2], despite the fact that the main purpose of this patent was the fight of the American radio-controlled sea-based torpedoes with a radio jamming of German boats and submarines.

Network Spoofing

The Network Spoofing is an attack, in which the spoofer (hacker, attacker, offender, opponent, a bad Boy) is sending a false packages in order to persuade the victim's computer that the listening computer is the final recipient. Then the packets are sent to the actual recipient. MAC (Media Access Control) – address of the sender is replaced in such a way that the reply packets pass through the listening computer [3, 4].

An attacker can unleash large amounts of noise using these devices and jam the airwaves so that their signal is so low, that the wireless LAN ceases to function. The only solution to this is RF proofing the surrounding environment. The hacker can use a high power RF signal generator to interfere with the ongoing wireless connection, making it useless. It can be avoided only by physically finding the jamming source.

A hacker uses a Trojan Access Point (AP) to hijack mobile nodes by sending a stronger signal than the actual AP is sending to those nodes. The clients then associate with the Trojan AP, sending its data into the wrong hands.

Attack machine uses vulnerabilities to get information about AP and clients. Attack machine sends deauthentication frames to the victim using the AP's MAC address as the source. Victim's 802.11 card scans channels to search for the new AP. Attack machine's fake AP is duplicating MAC address and ESSID of real AP. Fake AP is on a different channel than the real one. Attack machine associates with real AP using MAC address of the victim's machine. Attack machine is now inserted and can pass frames through in a manner that is transparent to the upper level protocols. The listening computer becomes the "gateway" for traffic victims and the offender gets a hearing traffic, for example, e-mail offerings.

GNSS Spoofing

Civilian vehicles, such as unmanned aircraft or helicopter, the vessel, truck-type TIR etc., will be called the "navigator" or "GNSS receiver[1]". Navigator moves in space with the civil GNSS procedure (mode L1) and is subjected to an spoofing attack from other vehicles, which we will call "spoofer". GNSS spoofing is the GNSS signal conversion technology. Spoofer plans to organize an attack so that the navigator should not know that the signal received by GNSS receiver is false. As a result of an organized attack, the navigator determines wrong time and/or location. This means that the spoofer began to administer the GNSS position in time and space [5, 6, 7, 8].

The only GNSS systems which can't be deceived, are GNSS military systems, that utilize principles of cryptography. However, for GNSS civil use such protection doesn't exist. Therefore the research of spoofing property for anti-spoofers design must be conducted. The spoofing main idea is illustrated in figure 2. Spoofer is generally located in the immediate vicinity of the navigator and moves in space with civilian L1 or military GNSS mode L1/L2. Spoofer performs short-term disruption of the GNSS signal L1 using GNSS jammer, which is now very widespread. A fishing vessel is able to block the self-registration system for routing and trot fishing in foreign waters. As a result of jamming GNSS receiver "loses satellites" and starts looking for GNSS signals. At this time, spoofer

[1] In the literature, such a vehicle is often called a victim.

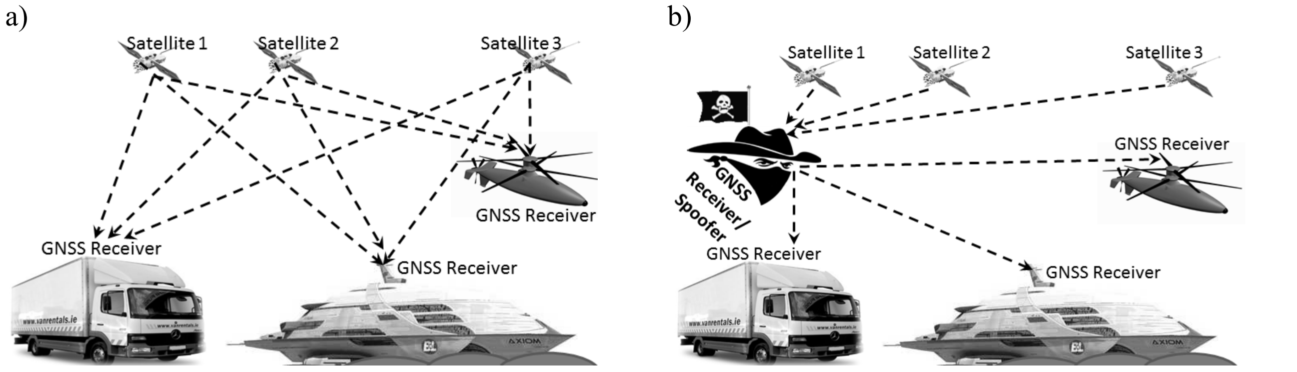

Fig. 2. GNSS before Spoofing (a) and during Spoofing (b)

includes imitator GNSS signals, which is set up to imitate the new coordinates of the GNSS receiver. Generally GNSS signal strength exceeds the strength of imitator real GNSS signals and GNSS receiver can't determine from what time of its movement in space it is controlled by a spoofer.

GNSS Simulators

A GNSS simulator device is more complex compared to GNSS Jammer, it costs about € 1000 [9, 10]. A GNSS simulator provides an effective and efficient means to test GNSS receivers and the systems that rely on them. A GNSS simulator provides control over the signals generated by the GNSS constellations and the global test environments are all in a box, so that testing can be conducted in controlled laboratory conditions. GNSS simulators generate the same kinds of signals that are transmitted by the GNSS satellites, thus GNSS receivers can process the simulated signals in exactly the same way as those from actual GNSS satellites.

A GNSS simulator provides a superior alternative for testing, compared to using actual GNSS signals in a live environment. Unlike live testing, testing with simulators provides full control of the simulated satellite signals and the simulated environmental conditions. With a GNSS simulator, testers can easily generate and run many different test scenarios for different kinds of tests, with complete control over:

Date, time, and location. Simulators generate GNSS constellation signals for any location and time. Scenarios for any locations around the world or in space, with different times in the past, present, or future, can all be tested without leaving the laboratory.

Vehicle motion. Simulators model the motion of the vehicles containing GNSS receivers, such as aircrafts, ships, or automobiles. Scenarios with vehicle dynamics, for different routes and trajectories anywhere in the world, can all be tested without actually moving the equipment being tested.

Environmental conditions. Simulators model effects that impact GNSS receiver performance, such as atmospheric conditions, obscurations, multipath reflections, antenna characteristics, and interference signals. Various combinations and levels of these effects can all be tested in the same controlled laboratory environment.

Signal errors and inaccuracies. Simulators provide control over the content and characteristics of the GNSS constellation signals. Tests can be run to determine how the equipment would perform if various GNSS constellation signal errors occur.

GNSS Spoofing (1D)

A GNSS Spoofing is performed in 3D $\{X, Y, Z\}$ space. **To illustrate the principles of spoofing, we consider a virtual experiment in 1D $\{X\}$ space navigation.** There are two transmitters S_1 and S_2, which move in unknown directions. Each of the transmitters S_1 and S_2 know their position x'_1, x'_2 in space. Between them is a receiver R, which also moves in an unknown direction and it does not know its position x''.

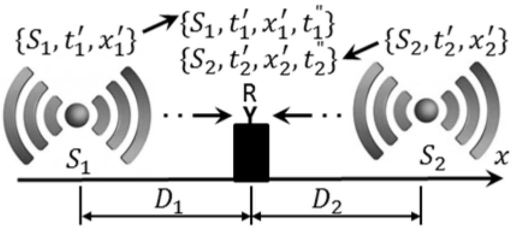

Fig. 3. Virtual navigation 1D experiment with one antenna R and two transmitters $\{S_1, S_2\}$: $D_1 = C\,(t''_1 + \Delta t - t'_1)$, $D_2 = C\,(t''_2 + \Delta t - t'_2)$, C – speed of light

On transmitters S_1 and S_2 are installed accurate clocks, such as atomic, and on the receiver R clock is inaccurate, such as quartz. Transmitters S_1 and S_2 in times t'_1, t'_2 send messages, which contain three numbers: transmitter number (1 or 2), time of message (t'_1 or t'_2), and its coordinates in space (x'_1 or x'_2). Receiver will receive this messages at the times (t''_1 or t''_2) with unknown error of Δt.

For the determination of accurate values of their coordinates x'' receiver can determine the approximate distance of coordinates from transmitters by inaccurate determining the time distribution of radio signal from transmitter to receiver. The evaluation of the receiver's position with help of transmitter S_1 is determined as:

$$x''_1 = x'_1 + C\left(t''_1 + \Delta t - t'_1\right) \tag{3}$$

and the estimation of the receiver's position with help of transmitter S_2 is determined as:

$$x''_2 = x'_2 - C\left(t''_2 + \Delta t - t'_2\right) \tag{4}$$

Distance error between the receiver and the transmitter is determined by the inaccuracy of a quartz clock receiver, which is equal to ΔD and leads to indeterminacy of the receiver position in space as if the receiver was in to points in space in the same time $x'' + \Delta D$ and $x'' - \Delta D$, and the distance between these points is equal to $2\Delta D$. An accurate determination of receiver position in space is determined as follows:

$$x'' = \frac{x''_1 + x''_2}{2} = \frac{x'_1 + x'_2 + C\left(\left(t''_1 - t'_1\right) - \left(t''_2 - t'_2\right)\right)}{2} \tag{5}$$

where: t'_1, t'_2 – messages return time S_1 and S_2 transmitters; x'_1, x'_2 – coordinates of the S_1 and S_2 transmitters; t''_1, t''_2 – exact time of a message is received by the receiver R from S_1 and S_2 transmitters; x''_1, x''_2 – approximate location of the receiver R, x'' – exact position of the receiver R.

Let as represent our virtual experiment in space navigation, but in spoofing terms (Fig. 4). Spoofer at the same time interferes with GNSS signals by jammer and transmits to the receiver R amplified signals containing $\{S_1, t_1^S, x_1^S\}$ and $\{S_2, t_2^S, x_2^S\}$ information.

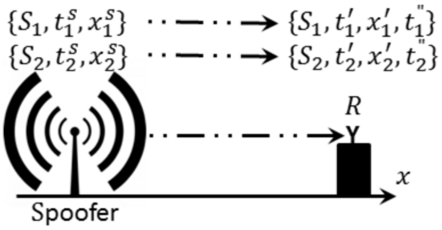

Fig. 4. Virtual 1D experiment in spoofing space navigation

The receiver begins to receive imitative GNSS signals from spoofer: $\{S_1, t_1^S, x_1^S\}$, $\{S_2, t_2^S, x_2^S\}$ and determines its position in space as follows:

$$x'' = \frac{x_1^S + x_2^S + C\left(\left(t''_1 - t_1^S\right) - \left(t''_2 - t_2^S\right)\right)}{2} \tag{6}$$

GNSS Spoofing Detection (1D)

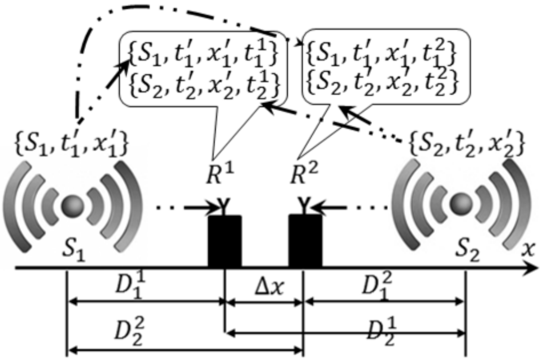

Fig. 5. Virtual navigation 1D experiment with two antennas $\{R^1, R^2\}$ and two transmitters $\{S_1, S_2\}$: $D_1^1 = C\,(t_1^1 + \Delta t - t'_1)$, $D_2^1 = C\,(t_2^1 + \Delta t - t'_2)$, $D_1^2 = C\,(t_2^2 + \Delta t - t'_2)$, $D_2^2 = C\,(t_1^2 + \Delta t - t'_1)$

Since we know the estimation of the antennas location, it is possible to determine the distance evaluation between the antennas:

$$\Delta\hat{x} =$$

$$= \left| \frac{\left(x'_1 + D_1^1\right) + \left(x'_2 - D_2^1\right)}{2} - \frac{\left(x'_1 + D_2^2\right) + \left(x'_2 - D_1^2\right)}{2} \right| =$$

$$= \frac{\left|\left(D_1^1 - D_2^1\right) + \left(D_2^2 - D_1^2\right)\right|}{2} \tag{7}$$

Spoofer uses only one antenna, with which imitates the signals from the two antennas (Fig. 6):

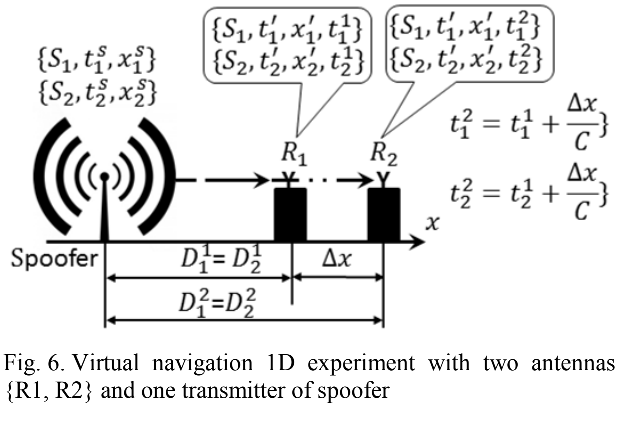

Fig. 6. Virtual navigation 1D experiment with two antennas {R1, R2} and one transmitter of spoofer

Substituting $D_1^1 = D_2^1$ and $D_1^2 = D_2^2$ into (7), we have $\Delta\hat{x} \sim 0$. The degree of approximation $\Delta\hat{x}$ to zero is determined mainly by the instrumental error of the navigator's calculation.

The main errors of positioning and their influence on accuracy of the distance evaluation between the antennas

Selective Availability

Selective availability is an artificial falsification of the time in the L1 signal transmitted by the satellite. For civil GPS receivers (which leads to a less accurate position determination) fluctuation of about 50 m during a few minutes. Additionally the ephemeris data is transmitted with lower accuracy, meaning that the transmitted satellite positions do not comply with the actual positions. Selective availability make the same mistake in the coordinates of the two antennas R1 and R2 and has a negligible impact on the accuracy of the distance between the antennas, since the measurements are performed at the same time at close range of the antennas.

Satellite geometry

Another factor influencing the accuracy of the position determination is the "satellite geometry". Simplified, satellite geometry describes the position of the satellites to each other from the view of the receiver. Satellite geometry make the same mistake in the coordinates of the two antennas R1 and R2 and has a negligible impact on the accuracy of the distance between the antennas, since the measurements are performed at the same time at close range of the antennas.

Atmospheric effects

Another source of inaccuracy is the reduced speed of propagation in the troposphere and ionosphere. Atmospheric effects make the same mistake in the coordinates of the two antennas R1 and R2 and has a negligible impact on the accuracy of the distance between the antennas, since the measurements are performed at the same time at close range of the antennas.

Satellite Orbits

Although the satellites are positioned in very precise orbits, slight shifts of the orbits are possible due to gravitation forces. Sun and moon have a weak influence on the orbits. The orbit data are controlled and corrected regularly and sent to the receivers in the package of ephemeris data. The errors of the satellite orbits make the same mistake in the coordinates of the two antennas R1 and R2 and has a negligible impact on the accuracy of the distance between the antennas, since the measurements are performed at the same time at close range of the antennas.

Multipath effect

The multipath effect is caused by reflection of satellite signals (radio waves) on objects. It was the same effect that caused ghost images on television when antennas on the roof were still more common instead of todays satellite dishes. The multipath effect make the same mistake in the coordinates of the two antennas R1 and R2 and has a negligible impact on the accuracy of the distance between the antennas, since the measurements are performed at the same time at close range of the antennas.

The decision rule for spoofing detection (1D)

If $\Delta\hat{x} \sim 0$ then {We are under the Spoofing Attack}

The decision rule for spoofing detection (2D)

In the horizontal plane (x, y) the estimate of the distance between the antennas can be written as

$$\Delta\hat{S} = \sqrt{\Delta\hat{x}^2 + \Delta\hat{y}^2} \qquad (8)$$

The corresponding decision rule becomes:

If $\Delta\hat{S} \sim 0$ then {We are under the Spoofing Attack}

The figure 7 shows the equipment for experimental studies, including two antenna GNSS Holux GR-213u.

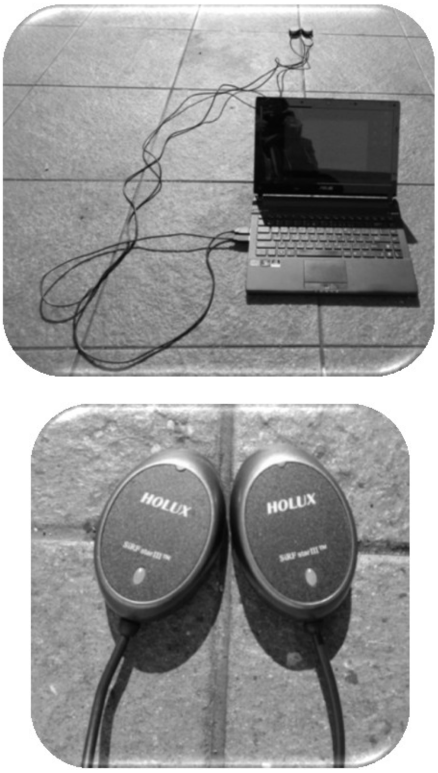

Fig. 1. The equipment for experimental studies

Typical measurements of $\Delta\hat{S}$ are shown in figure 8 (t in sec.).

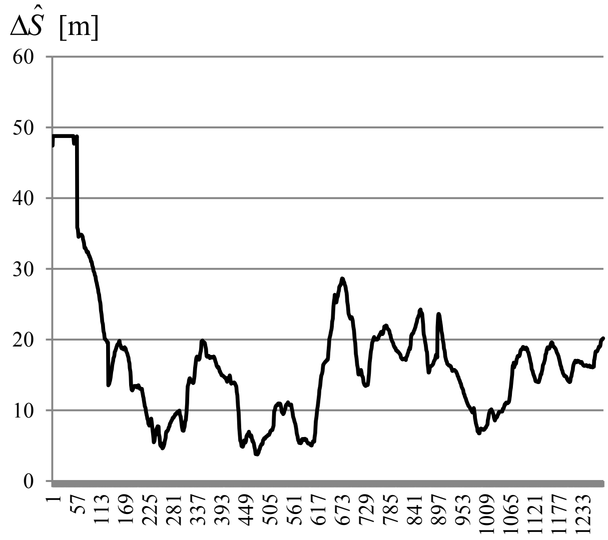

Fig. 8. $\Delta\hat{S} = f(t)$

Conclusions

This article describes a general approach to anti--spoofer design. The results of the design are markedly different depending on the means of communication (ships, aircraft or surface transportation), the presence of the crew on board, means of communication (drone anti-spoofing is more complicated), the limit price and other parameters [11].

References

1. Specht C.: System GPS. Biblioteka Nawigacji nr 1. Wydawnictwo Bernardinum, Pelplin 2007.
2. Markey H.K. at al.: Secret Communication System. US Patent 2,292,387 11.08.1942.
3. Flickenger R.: Wireless Hacks: 100 Industrial-Strength Tips & Tool. O'Reilly & Associates, September 2003.
4. 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.
5. Ochin E., Gucma L., Petlin S., Vidmar P., Gucma M., Puszcz A., Perkovic M., Harsh R., Lemieszewski Ł.: Problems of telecommunication networks for the safety of maritime transport. Proceedings of World Maritime Technology Conference 2012, Saint-Petersburg, ISBN 978-5-88303-503-5.
6. 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 Volume 2012, Article ID127072, doi: 10.1155/2012/127072.
7. Humphreys T.E., Ledvina B.M., Psiaki M.L., O'Hanlon B.W., Kintner P.M. Jr.: Assessing the Spoofng Threat: Development of a Portable GPS Civilian Spoofer. Preprint of the 2008 ION GNSS Conference Savanna, GA, September 16–19, 2008.
8. Badea V., Eriksson R.: Pseudolite INDOOR real time precise positioning. Norrkopping, 2005.
9. GNSS Simulators, http://www.spirent.com/positioning-and-navigation.aspx
10. Psiaki M.L., O'Hanlon B.W., Bhatti J.A., Shepard D.P., Todd E.: Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals. Humphreys, Preprint from ION GNSS, 2011.
11. Ochin E., Lemieszewski Ł., Lusznikov E., Dobryakova L.: The study of the spoofer's some properties with help of GNSS signal repeater. Scientific Journals Maritime University of Szczecin 36(108) z. 2, 2013, 159–165.