Method, algorithm and implementation of vehicles GNSS information protection with help of anti-jamming and anti-spoofing

Larisa Dobryakova[1], Łukasz Lemieszewski[2] and Evgeny Ochin[3]

[1] West Pomeranian University of Technology, Faculty of Computer Science and Information Technologies, Szczecin, Poland;
[2] The Jacob of Paradies University, Department of Technology, Gorzów Wielkopolski, Poland
[3] Maritime University of Szczecin, Faculty of Navigation, Szczecin, Poland
ldobryakova@wi.zut.edu.pl,llemieszewski@ajp.edu.pl,e.ochin@am.szczecin.pl

Abstract. Jamming and anti-jamming technologies have become an important research topic within the GNSS discipline. While many GNSS receivers leave large space for signal dynamics, enough power space is left for the GNSS signals to be jammed. The goal of jamming is adding a noise to the satellite signal and fooling the receiver not to use signals plus noise for positioning calculations. The goal of spoofing is a falsification of the satellite signal and fooling the receiver to generate a false position; thus, misleading the navigator. This article discusses the experimental approach to anti-jamming and anti-spoofing based on the shielding of the antennas from the jammers and spoofers signals to develop an algorithm for the built-in protection system. In experimental studies, we used two types of screens: the metal funnel and the system of metallic concentric rings on a metal substrate. We also briefly consider the commercial civilian and military jammers. The presented algorithm enables the development of an integrated vehicle safety system.

Keywords: algorithm, protection, vehicles, GNSS, attacks, jamming, anti-jamming, spoofing, anti-spoofing, shielding

1 Introduction

Satellite based positioning provides the world's most precise location information. It is possible to acquire positioning anywhere in the world where the GNSS satellite signals are available any time of day at data rates up to 100 Hz. Raging currents, rugged coastlines, narrow passageways, and high winds all contribute to making marine environments some of the most challenging navigation conditions in the world. Modern GNSS receivers, antennas, and post-processing software provide precise, accurate, and reliable positioning measurements for a wide range of marine applications.

Ability and quality of measuring and monitoring the GNSS signals are critical to assessing GNSS system usability and performance. The GNSS receiver technology relies on signals broadcast from satellites orbiting 20 000 km above the Earth at a frequency of approximately -163 dBW or about the strength of a single Christmas tree bulb. This makes GNSS signals susceptible to interference from many sources [6].

Jamming is a purposeful creation of active interference to reduce the signal/noise ratio of the GNSS satellite signals. Usually, it is a part of electronic warfare. Jamming may be targeted to all or some recipients of the signal. The device for silencing is called the jammer.

Generally, purpose of jamming is to prevent the useful information or a signal receiver or, at least, creating inconvenience to him. As the object of jamming can be any receiver insufficiently protected from external influences signals: radio, radar beacon, the wireless network, the mobile phone (or base station), etc. Jamming can be used in actual combat conditions and in the cases of the information war, or even competitive telecommunications companies or broadcast, to make completely disable the security system or to transfer it to the unservice mode.

Development Unmanned Vehicle (UV) caused developing the special-purpose technologies both for military and dual-use applications. And it is not only the traditional system of military intelligence, but, also, rapidly developing electronic warfare systems including mobile systems of noise suppression radar and radio navigation systems (jamming) [1] and mobile jamming and/or spoofing the GNSS signals [2, 9–16].

2 Interference for unmanned vehicles

For positioning unmanned vehicles (UV), the GNSS and Inertial Navigation System (INS) [3, 4] are used. Accuracy of positioning using INS is not sufficient. The GNSS corrected the work of INS. Creation a radio interference field for GNSS neutralizes UV. Information from navigational monitoring devices is not reflected in the observation area and is not up-to-dated. Furthermore, UV themselves without knowing its coordinates with a high probability can not return to the base and will be lost. In areas where there are woods or forest, you can not see under the trees any objects of interest, such as a human or animal, even in the winter when there are no leaves on the trees. Not by chance, all advertising UV are applied to the treeless terrain with a smooth relief, *i.e.*, in relation to the deserts and water surfaces.

Emphasize the importance of UV as a means of electronic warfare, *i.e.*, media jammers and/or spoofers of the GNSS. In this case, the radar will observe hundreds of decoys and the GNSS-receiver will be switched from real signals of the GNSS to false ones.

3 Generation of radio noise to suppress the GNSS signals

The availability and usage of low-cost GNSS jamming devices has resulted in the increased threat of intentional and unintentional disruption of commercial and industrial systems that rely on precise GNSS data. The basic scheme of jamming is shown in Fig. 1.

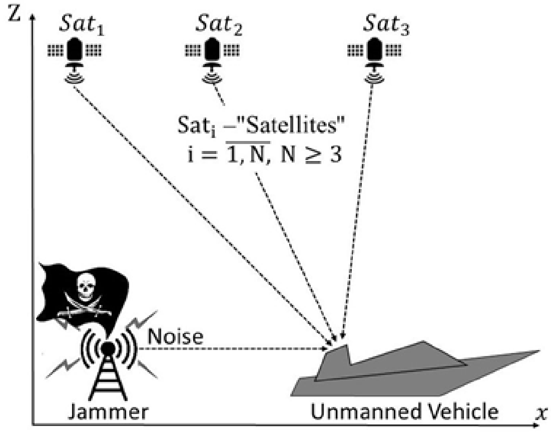
Z
Sat_1
Sat_2
Sat_3
$\mathrm{Sat_i}$ –"Satellites"
$\mathrm{i} = \overline{1, \mathrm{N}}$, N ≥ 3
Noise
Jammer
Unmanned Vehicle
x

Fig. 1. GNSS Jamming: the suppression of GNSS signals via radio noise generator.

4 Algorithm for the main scenario of GNSS jamming

It is well known that the use of directional antennas weaken the jammer signal, and, in some cases, it is blocked to 100%. You can use a metal funnel to change the directionality of antenna. The main scenario of the GNSS jamming using a funnel is shown in Fig. 2. A vehicle during normal operation carries traffic using the GNSS. The minimal elevation angle $\beta_{\min}$ is known for satellite above the horizon at which the antenna can "see" the satellites.

The terrorist located at a distance from vehicle broadcasts to the vehicle a high power radio noise or a fake signals from the spoofer and suppresses a mode of the normal operation using GNSS. The maximal elevation angle $\alpha_{\max}$ of the jammer above the horizon at which the antenna "does not see" the jammer (Fig. 2).

In most practical situations $\beta \gg \alpha$, so the main parameter of shielding type funnel (angle γ) you can select as $\gamma = (\alpha + \beta)/2$.

5 Experimental study of EMI shielding type funnel

To test the effectiveness of shielding type funnel, we performed experimental studies. The funnel was made from an aluminum sheet of diameter 300 mm and height 86.6 mm (Fig. 3). The elevation of jammer changed from 0 to a value at which jammer "drowned" normal browser operation. The experiment showed that this angle is almost coincided with the main parameter of funnel-shieldede one (angle γ) equal 30°.

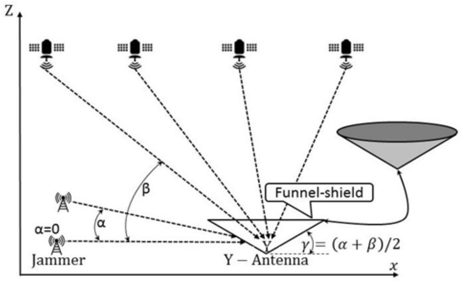

Fig. 2. The main scenario of GNSS jamming; the EMI shielding type funnel of antenna Y.

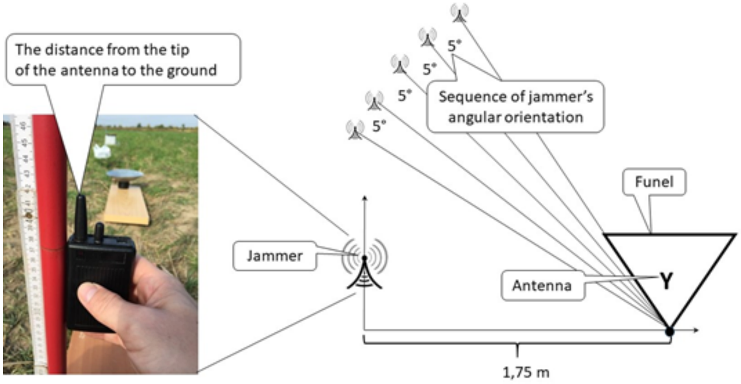
The distance from the tip of the antenna to the ground
5°
5°
5°
5°
Sequence of jammer's angular orientation
Funel
Jammer
Antenna
Y
1,75 m

Fig. 3. The elevation of jammers to a value, at which the jammer is "drowned" the normal browser operation.

6 The main scenario of GNSS jamming and EMI shielding

As described in point 4, that the use of directional antennas weaken the jammer signal, and, in some cases, it is blocked to 100%. You can use a system of metallic concentric rings on a metal substrate to change the directionality of the antenna. A vehicle during normal operation carries traffic using the GNSS. The antenna

Y can “see” all satellites. Terrorist located at a distance from vehicle broadcasts to the vehicle a high power radio noise or a fake signals from the spoofer and suppresses a mode of the normal operation using GNSS (Fig. 4). Details related to diffraction of electromagnetic wave from a jammer was described in detail in [5, 9].

7 Experimental study of EMI shielding with help of metallic concentric rings

In real experiments, we used five metallic concentric rings (Fig. 5). To test the effectiveness of shielding with help of metallic concentric rings, we performed experimental studies. A jammer was used as a source of electromagnetic radiation.

Experiment #1. Wave front propagates parallel to the X axis.

The purpose of this experiment was to find out the minimum distance along the X axis, from which it would be possible to receive the GNSS signal using a jammer and a screen shield. The distance was systematically increased every 10 cm between the GNSS receiver and the jammer until the satellite signal was received by the GNSS antenna Y, as shown in Fig. 6.

When the jammer was as close to the screen as possible, the antenna received the noise from the jammer. Then, the jammer was moved in the direction $-x$ until the receiver captured genuine GNSS signals with the help of the antenna Y. The result of the experiment is $R = 3.6$ m.

Experiment #2. Wave front propagates at the angle γ to the axis X, $\gamma \in \{15°, 10°, 5°, 0°, 5°, 10°, 15°\}$

The purpose of the next experiment was to determine how the relative height of the jammer affected the receivers reception despite the use of the screen. As in the previous experiment, the distance was systematically increased by 10 cm each time, but at different height levels between the GNSS receiver and the jammer until the satellite signal was received by GNSS antenna Y, as shown in Fig. 7.

When the jammer was as close to the screen as possible, the antenna received the noise from the jammer. The jammer was then moved in the direction (x) at the angle γ to the axis X, $\gamma \in \{15°, 10°, 5°, 0°, 5°, 10°, 15°\}$ until the receiver captured the GNSS signals again with the help of the antenna Y. The results of the experiment are shown in Table 1.

Table 1. The results of the angular dependency experiment

γ	$-15°$	$-10°$	$-5°$	$0°$	$5°$	$10°$	$15°$
R, m	1.0	1.2	1.3	3.6	3.6	3.6	3.6

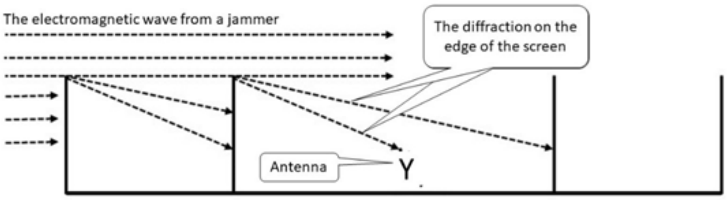
The electromagnetic wave from a jammer
The diffraction on the edge of the screen
Antenna

Fig. 4. The diffraction of electromagnetic wave from a jammer on the edge of the two metallic concentric rings.

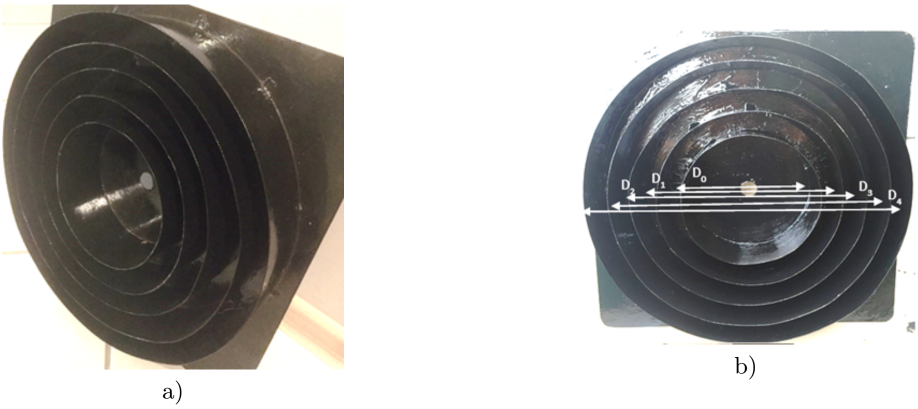

Fig. 5. The system of the five metallic concentric rings (diameters of rings D_0=155 mm, D_1=205 mm, D_2=260 mm, D_3=305 mm, and D_4=355 mm; height H=65 mm; thickness T=1 mm).

8 Commercial civilian GNSS jammers

8.1 GNSS jammer for a car

There are a few civilians that use jamming GNSS signals, mostly privacy related, including the ability to conceal oneself or one's vehicle, in the case, when it is being tracked by a GNSS receiver. A practical application would be a salesperson or delivery driver that may wish to lunch outside their territory or return home for a forgotten item without having to do a lot of explaining due to the GNSS tracking on their vehicle. The range of the most civilian GNSS jammers is sufficient to cover even the largest of vehicles giving the user a cloak of privacy [7].

For car, truck, bus, van, or even boat security, stopping the GNSS tracking signals is provided by simply plugging the jammer into any cigarette lighter or vehicle power outlet of 12V. With up to 10 meter coverage, it will protect you from being detected. It will automatically protect you by blocking any GNSS signals that are being sent to track you inside and outside your vehicle. This

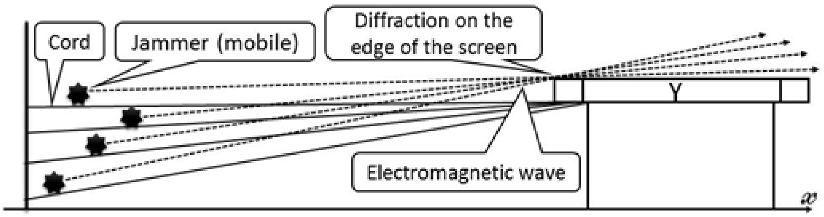

Fig. 6. Experimental study of EMI shielding: Y shielded antenna of the receiver.

tracking jammer is a popular item with sales personnel, truckers, and delivery drivers, who wish to take lunch or make a personal stop outside of their territory or route “off the radar” [7].

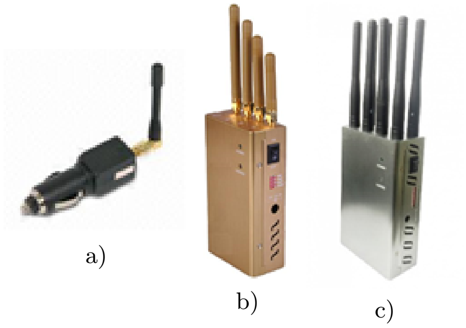

Fig. 7. a) the GNSS jammer for a car, b) the Cell GNSS PRO, c) the High Power Combination Unit.

8.2 Cell GNSS PRO

The PRO model secures the area and prevents both cell phone and GNSS application with the most popular combination of the cell phone and GNSS units. This high powered handheld PRO model features a built-in fan to keep the unit cool during extended periods of use, as well as switch selectable settings; so, you can choose which channels to block. The PRO creates a protected zone around you, your vehicle, or your meeting by blocking cellular and/or GNSS signals at a distance of up to 25 meters (under best conditions). The indicator lights on top of the unit confirm which bands are actively being inhibited, and the durable rubber coated antennas will not be brken with rugged use.

8.3 High power combination unit

This model provides secure area coverage and prevents both cell phone and GNSS application with our highest powered handheld. This model features a built-in fan to keep the unit cool during extended periods of use, as well as switch selectable settings; so, one can choose, which channels to block.

Jamming:

700–800 MHz (4G)
850–965 MHz (GSM)
2400–2500 MHz
2500–2700 MHz
2100–2170 MHz (3G)
1800–1990 MHz (PCS)
GNSS L1
GNSS L2

9 Military GNSS jammers

In the world, there are many different versions of Military GNSS jammers. Here, we give as an example the station Autobase-M 1L222M (Fig. 8), which may operate in a mode jammer. The 1L222M "Autobase-M" complex is the executive radio-technical reconnaissance (EW) mobile complex component with the jamming stations SPN-2/SPN-4 [8].

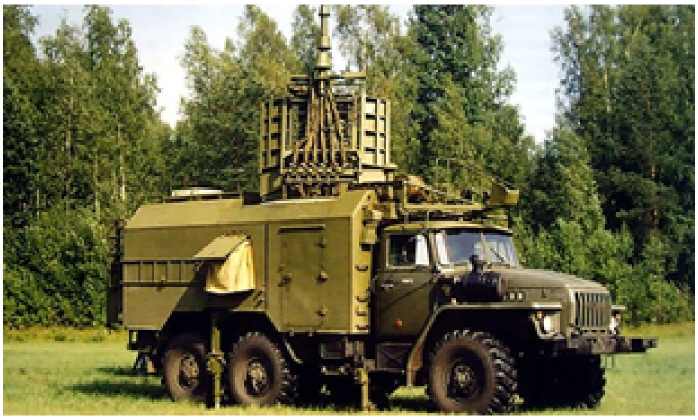

Fig. 8. The station RTR 1L222M "Autobase-M", maximum range radar reconnaissance — 150 km.

10 Conclusions

In this study of GNSS anti-jam and anti-spoof techniques, we have contributed by summarizing various approaches and discussed open research issues in the field [9–16]. Different GNSS jammers attack in various ways and their attacks are significantly different. For instance, a constant jammer consumes all resources available and continuously jams the GNSS, but it is easily detected. On the other hand, a smart jammer senses the medium and only attacks when a certain condition is satisfied. So, it is a good choice for resource-constrained hardware.

Shielding of the UV antenna in order to protect against GNSS-spoofing, and the reduction of diffraction at the edge of the shielding rings are presented in detail. Physical experiments have shown that the distance between the GNSS receiver and the jammer or spoofer, as well as the difference in altitude between the two devices, has a significant effect on the resulting disturbance of the receiver. The higher the setting of the receiver is, the easier it is for the jammer or spoofer to suppress the original satellite signal. Moreover, if a jammer or spoofer has a periodic low power, it is hard to detect it; a powerful jammer or spoofer will certainly jam (spoof) most of the networks but will be easily detected. The presented physical experiments and algorithm created on their basis will allow to develop a program for the built-in vehicles safety system.

References

1. Pullen S., Gao G. GNSS Jamming in the Name of Privacy. INSIDE GNSS: applications of the Global Navigation Satellite Systems: GPS, Galileo, GLONASS, BeiDou, and related technologies, U.S.A. 2012. https://www.insidegnss.com/auto/marapr12-Pullen.pdf (date of the application 15.10.2017)
2. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J, and Lachapelle, G. GNSS Vulnerability to Spoofing Threats and a Review of Anti-spoofing Techniques. International Journal of Navigation and Observation, Volume 2012 (2012), Article ID 127072, http://dx.doi.org/10.1155/2012/127072 (date of the application 15.10.2017)
3. Association for Unmanned Vehicles Systems International (AUVSI). http://www.auvsi.org (date of the application 15.10.2017)
4. Basic Land Navigation, Global Positioning System, page 97, National Interagency Incident Management System,2017. https://www.nwcg.gov/sites/default/files/publications/pms475.pdf (date of the application 15.10.2017)
5. Nye, J. F., Hannay, J. H., Liang W. Diffraction by a Black Half-Plane: Theory and Observation, https://www.researchgate.net/publication/259054854_Diffraction_by_a_Black_Half-Plane_Theory_and_Observation (date of the application 15.10.2017)
6. GNSS Signal Monitoring. http://www.novatel.com/industries/signal-monitoring/ (date of the application 15.10.2017)
7. GPS Jammers. http://www.thesignaljammer.com/categories/GPS-Jammers/ (date of the application 15.10.2017)
8. 1L222M "Autobaza". http://militaryrussia.ru/blog/topic-598.html (date of the application 15.10.2017)
9. Dobryakova, L., Lemieszewski Ł., Ochin, E. Protecting vehicles vulnerable to terrorist attacks, such as GNSS jamming, by electromagnetic interference shielding of antenna, Scientific Journals of the Maritime University of Szczecin, 2017-07-06 http://repository.am.szczecin.pl/handle/123456789/2399 (date of the application 15.10.2017)
10. Dobryakova, L., Lemieszewski Ł., Ochin, E. The vulnerability of unmanned vehicles to terrorist attacks such as Global Navigation Satellite System spoofing, Scientific Journals of the Maritime University of Szczecin, 2016-06-27

11. Ochin, E., Dobryakova L., Lemieszewski, Ł. Antiterrorism design and analysis of GNSS anti-spoofing algorithm, Scientific Journals of the Maritime University of Szczecin, 2012. http://repository.scientific-journals.eu/handle/123456789/358 (date of the application 15.10.2017)
12. Ochin, E., Dobryakova, L., Lemieszewski, Ł., Lusznikov, E. The study of the spoofers some properties with help of GNSS signal repeater, Scientific Journals of the Maritime University of Szczecin, 2013. http://repository.scientific-journals.eu/handle/123456789/581 (date of the application 15.10.2017)
13. Dobryakova, L., Lemieszewski, Ł., Ochin, E. Design and analysis of spoofing detection algorithms for GNSS signals, Scientific Journals of the Maritime University of Szczecin, 2014. http://repository.scientific-journals.eu/handle/123456789/668# (date of the application 15.10.2017)
14. Dobryakova, L., Ochin, E. On the application of GNSS signal repeater as a spoofer, Scientific Journals of the Maritime University of Szczecin, 2014. http://repository.scientific-journals.eu/handle/123456789/669# (date of the application 15.10.2017)
15. Ochin, E. Detekcja GNSS spoofingu i bezpieczeństwo transportu, część I / Akademickie Aktualności Morskie, ISSN 1508-7786, nr 2(82)/ 2014, str. 8-10. http://am.szczecin.pl/userfiles/File/aam/AAM%202_82_2014.pdf (date of the application 15.10.2017)
16. Ochin, E. Detekcja GNSS spoofingu i bezpieczeństwo transportu, część II / Akademickie Aktualności Morskie, ISSN 1508-7786, nr 3(82)/ 2014, str. 12-13. http://am.szczecin.pl/userfiles/File/aam/AAM%203_83_2014.pdf (date of the application 15.10.2017)