Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2017, 50 (122), 77–83
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)
DOI: 10.17402/219

Received: 15.10.2016
Accepted: 24.04.2017
Published: 16.06.2017

Protecting vehicles vulnerable to terrorist attacks, such as GNSS jamming, by electromagnetic interference shielding of antenna

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

[1] West Pomeranian University of Technology
Faculty of Computer Science and Information Technologies
49 Żołnierska St., 71-210 Szczecin, Poland, e-mail: ldobryakova@wi.zut.edu.pl
[2] The Jacob of Paradies University, Department of Technology
25 Teatralna St., 66-400 Gorzów Wielkopolski, Poland, e-mail: llemieszewski@ajp.edu.pl
[3] Maritime University of Szczecin, Faculty of Navigation
1–2 Wały Chrobrego St., 70-500 Szczecin, Poland, e-mail: e.ochin@am.szczecin.pl
corresponding author

Key words: GNSS, navigation, jammer, jamming, anti-jamming, spoofer, spoofing, anti-spoofing, repeater

Abstract

Spoofing, anti-spoofing, jamming and anti-jamming technologies have become an important research topic within the GNSS discipline. While many GNSS receivers leave a large space for signal dynamics, enough power space is left for the GNSS signals to be spoofed and/or jammed. The goal of spoofing is to provide the receiver with a misleading signal, fooling the receiver into using fake signals in the extra space for positioning calculations. The receiver will then generate a false position, thus misleading the navigator. The goal of jamming is to add noise to the satellite signal which leads to fooling the receiver into using "signals plus noise" for positioning calculations. This article discusses the approach to anti-jamming based on the shielding of antennas from the signal jammer.

Introduction

Transport security is an important component of the national security interests of all countries. What is generally understood as transport security is the state of protection of the transport infrastructure and vehicles from acts of unlawful interference in their activities. The concept of transport safety includes:

- the identification of factors that threaten transportation security;
- the formation of a counteraction system for transportation security;
- the definition of measures set to improve transport safety;
- the transport safety being in line with international standards.

Reliable transport security has now become an urgent task for many countries. This is due to several factors:

- the penetration of terrorism into the sphere of transport and the implementation of sabotage;
- the intensification of organized crime (smuggling, illegal migration, and others);
- the interweaving of international drug trafficking and terrorism (the drug trade is a potential means of financing terrorism).

Among the main threats to transport, the following potential cases can be identified:

- the hijacking or seizure of aircraft, ships, river boats, railway rolling stock, vehicles;
- criminal acts against passengers;
- criminal acts against cargo.

The ability to navigate with a compass and map is an essential skill for many potential situations. Even with new technology, such as Global Navigation Satellite System (GNSS) receivers, map and compass skills are still needed. Confidence with navigation skills comes with practice and proficiency. This

level of confidence often impacts on how a person performs during a crisis, which can result in life or death outcomes of their decisions. It has to be noted that the use of Unmanned Vehicles (UV) shows an increasing trend today. The need for such equipment poses a lot of problems, the most significant of which are shown in Figure 1.

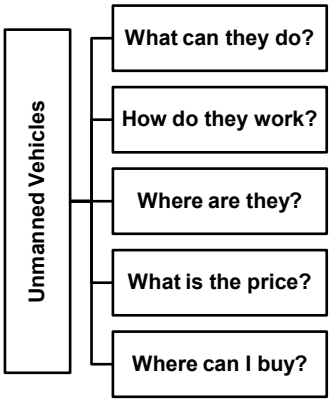


Figure 1. Unmanned Vehicles (UV) and related issues

To understand the problems of UV they should be classified according to methods of control (Figure 2) and the environment (Figure 3).

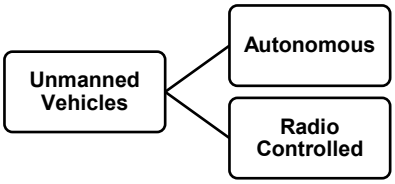


Figure 2. Classification of UV according to methods of control

The term "unmanned" implies the absence of a pilot on board the UV, but admits the presence of a remote human operator (remote control). If there is no pilot and no remote human operator, then such a UV is referred to as "autonomous".

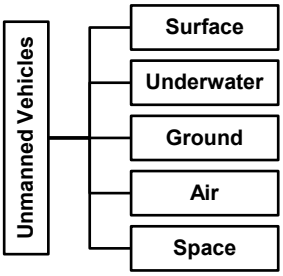


Figure 3. Classification of UV according to the environment

The development of modern and advanced technologies allows UV to successfully perform these functions, which they were unable to perform in the past and which were accomplished by other forces and means. In particular, UV have been shown to be highly effective in carrying out the tasks of monitoring roads, pipelines, farmland, forest fires, rivers, lakes, seas, and coastal oceans, searching for fish and other items of interest. An unmanned vehicle prevails in those industries that operate in environments which are remote from humans, such as warehouse logistics, mining and others. UV enable tracking and monitoring the development of a situation in a given area or for a given route in real time.

It should be noted that the driving force of UV development has been, and continues to be, special-purpose technology and above all the military (Dual-Use System). It is not only a traditional system of military intelligence, but also electronic warfare systems are rapidly being developed for UV, including mobile systems noise suppression radar and radio navigation systems (jamming) (Pullen & Gao, 2012), and mobile jamming and/or spoofing of GNSS signals (Retscher, 2002; BDBS, 2011; Jafarnia-Jahromi *et al.*, 2012; Ochin, Dobryakova & Lemieszewski, 2012, 2013; Ochin *et al.*, 2013; Cameron, 2014; Dobryakova & Ochin, 2014; Dobryakova, Lemieszewski & Ochin, 2014a, 2014b, 2014c; MX Marine, 2017).

Interference for unmanned vehicles

UV use GNSS and INS for positioning (NWCG, 2016; AUVSI, 2017). The accuracy of positioning using INS is not sufficient, and so GNSS is employed to correct INS. Creating a field of radio interference for GNSS neutralizes a UV's ability to calculate its own position. The information calculated as a result of this interference is not in agreement with the UV's real location and so has no significant value. Furthermore, without knowing its own coordinates there is a high probability that the UV will not be able to return to base, and therefore will be lost. In areas where there are woods or forest, a UV cannot see objects of interest under trees, such as humans or animals, even in the winter when there are no leaves on the trees. It is not coincidence that in all UV advertising the technology is shown operating in treeless terrain with smooth surface relief, *e.g.* over deserts and bodies of water.

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

Generation of radio noise to suppress GNSS signals (GNSS-jamming)

The availability and usage of low-cost GNSS jamming devices has resulted in the increased threat of intentional and unintentional disruption to commercial and industrial systems that rely on precise GNSS data. The basic scheme of jamming is shown in Figure 4.

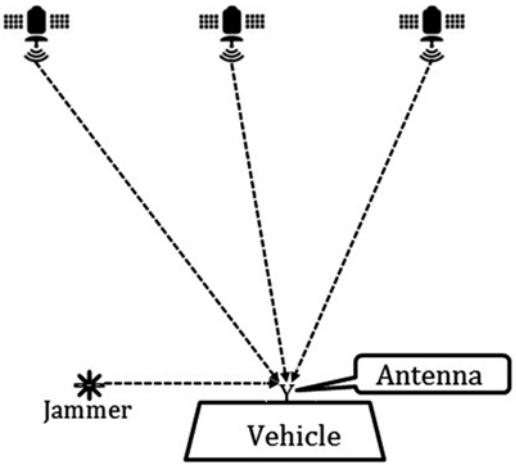


Figure 4. GNSS jamming: the suppression of GNSS signals *via* a radio noise generator

The main scenario of GNSS jamming

The main scenario of GNSS jamming is shown in Figure 5. During normal operation, a vehicle receives positioning information *via* GNSS. A terrorist, located at a distance from the vehicle, broadcasts high power radio noise and suppresses the normal mode of operation using GNSS. The jammer may be in one of three positions relative to the antenna of the vehicle:

- at the same height as the antenna ($\alpha = 0$);
- above the antenna ($\alpha > 0$);
- lower than the antenna ($\alpha < 0$).

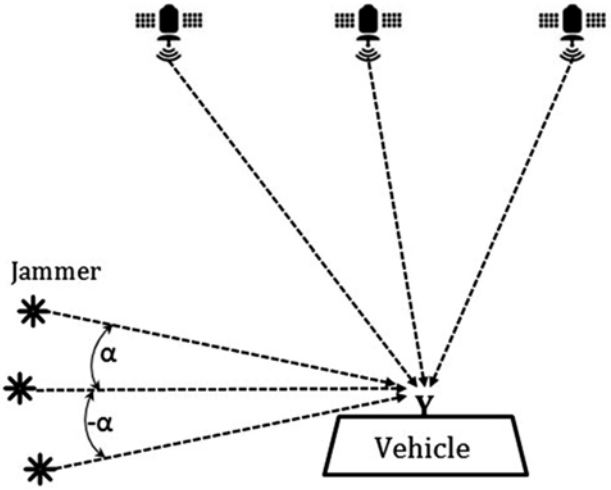


Figure 5. The main scenario of GNSS jamming

With a relatively small angle α, the efficiency of a jamming signal has little dependence on the value of α.

The shielding of UV antenna to protect against GNSS-spoofing and/or jamming

Assume that the transmitting antenna of S and the receiving antenna of V are at the same height, *i.e.* $z_s = z_v$. In this case V may be protected against jamming by a screening metal ring (Figure 6).

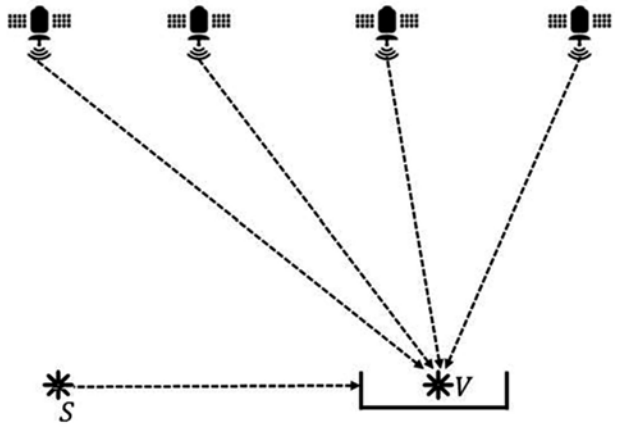


Figure 6. UV protection from jamming using a screening metal ring

Assume that the distance from S to the metallic screen is sufficiently large to consider that an electromagnetic wave falling on the screen is a flat wave (Figure 7).

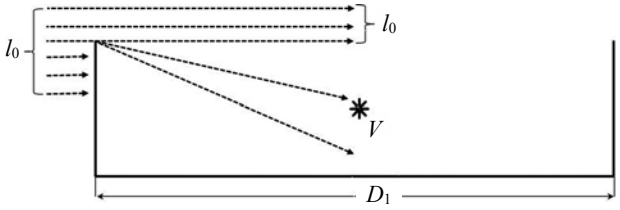


Figure 7. Diffraction of electromagnetic waves from a jammer on the edge of the ring

The reception antenna is located in the shadow of the incident wave. However, due to diffraction at half-plane, a part of the signal energy from the spoofer still reaches the receiving antenna. A rigorous solution of diffraction problems can in principle be found on the basis of the wave equation and the boundary conditions. However, due to the complexity of these problems, a rigorous formulation solution can only be obtained in just a few simple cases.

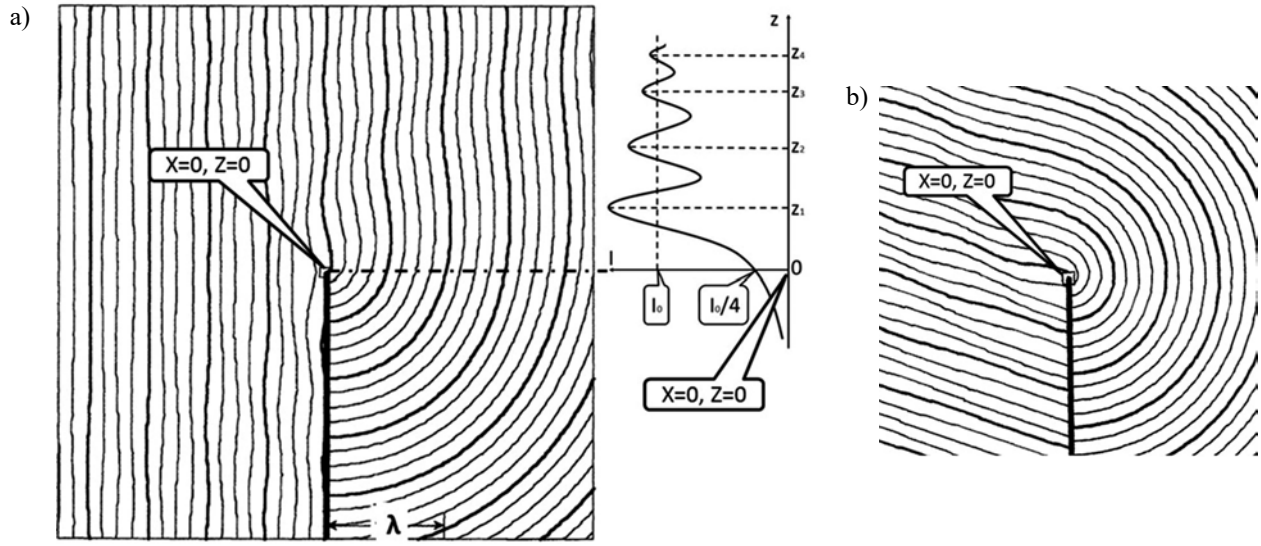


Figure 8. The diffraction of electromagnetic waves on the edge of the ring (Nye, Hannay & Liang, 1995): a) wave front propagates parallel to the *X* axis; b) wave front propagates at an angle to the axis *X*

The Fresnel diffraction at the edge of a shielding ring

The distribution of wave amplitude for the half-plane metal screen in general is a complex mathematical problem. When the screen is at a short distance from the receiving antenna the intensity distribution of the diffracted wave in the near field is described by the Fresnel integral. A rigorous solution of the Fresnel diffraction at the edge of the half-plane shows that near the area of the geometrical shadow is a series of alternating light and dark bands, which are parallel to the edge of the half-plane and located in the illuminated region (Figure 8).

In the shadow, the intensity decreases monotonically to zero, and at the boundary of geometric shadow intensity is 4 times lower than the intensity of the incident wave. In fact, the wave front is spherical and analytical calculation of the diffraction field becomes more complicated (Nye, Hannay & Liang, 1995).

The reduction of diffraction at the edge of a shielding ring

To reduce diffraction, a second ring, which has the same height *H*, can be installed (Figure 9).

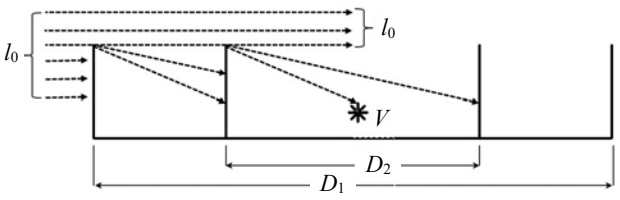


Figure 9. The reduction of diffraction by the introduction of a second ring

To further reduce the effects of diffraction, third, fourth, *etc.* rings can be installed. Thus, for example, Figure 10 shows a system of screening, which consists of four concentric rings of height *H*.

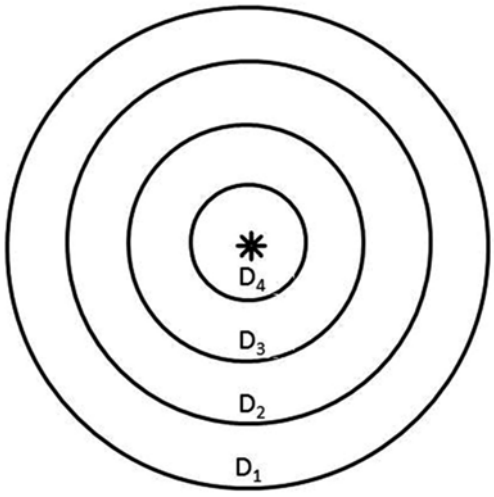


Figure 10. The shielding of an antenna with four concentric rings

The task of designing a shielded antenna

The task of designing a shielded antenna for a given number of shielding rings *N* reduces to finding the diameters *D* and heights *H* of the shielding rings:

$$\{D_1; D_2; \ldots; D_N; H_1, H_2, \ldots, H_N\} \quad (1)$$

In the particular case where $H_1 = H_2 = \ldots = H_N$, the task of designing a shield is reduced to finding the diameters *D* of the shielding rings:

$$\{ D_1; D_2; \ldots; D_N \} \quad (2)$$

If it can be assumed that:

$$\{(D_1 - D_2) = (D_2 - D_3) = ... = (D_{N-1} - D_N) = \Delta D\} \quad (3)$$

then the task of screening a GNSS antenna is reduced to defining the diameter of the outer ring and the determination of such values ΔD, where the energy E of the diffracted wave incident on the receiving antenna of UV would be minimal.

$$E(\Delta D) = E_{\min} \quad (4)$$

Because in the shadow of the screen the intensity of the diffracted wave decreases monotonically to zero, and on the border of a geometric shadow the intensity is 4 times smaller than the intensity of the incident wave, we can assume that screening a system through the use of N rings reduces the energy E of the diffracted wave incident on the receiving antenna of the UV by K times:

$$K = 4^N \quad (5)$$

For example, for N = 4 (Figure 10) you can expect a decrease of the diffracted wave energy of $4^4 = 256$ times.

Simulation of UV antenna shielding

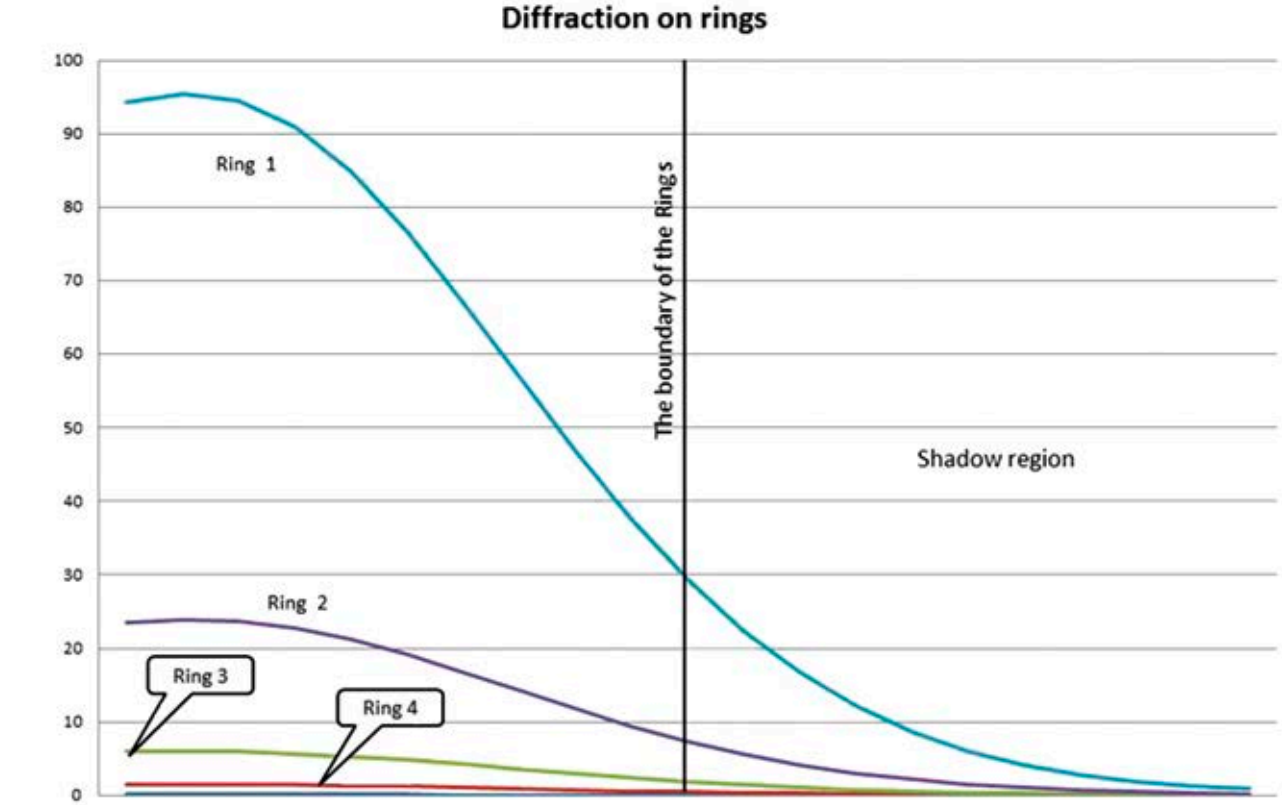
In accordance with the principle of Huygens-Fresnel we can calculate the energy of the diffracted wave by the first ring reaching the second ring as a screen. It is known that the distribution of the operating frequency of GNSS as in the case of NAVSTAR GPS and GLONASS is in the range of 1559–1610 MHz, which corresponds to wavelengths in the centimeter range 18.6–19.2 cm.

For approximate calculations we can assume that the length of the main working wave of GNSS is $\lambda = 18$ cm. For $\{-10 \le z \le 10\}$ cm in steps of 1 cm the calculated intensity of the diffracted wave is:

$$I(z) = \sum_{k=0}^{99} \exp\left(i\frac{2\pi}{\lambda} \cdot \mathrm{abs}(z - 0.01k + i\Delta D)\right)$$
$$-10 \le z \le 10 \text{ cm} \quad (6)$$

where: $i = \sqrt{-1}$, $\lambda = 18$ cm, $\Delta D = 15$ cm.

The diffracted wave is diffracted a second time on the second ring, and again on rings 3 and 4. As a result, the energy of the diffracted wave



Z=	0,10	0,09	0,08	0,07	0,06	0,05	0,04	0,03	0,02	0,01	0,00	-0,01	-0,02	-0,03	-0,04	-0,05	-0,06	-0,07	-0,08	-0,09	-0,10
Ring 4	1,47	1,49	1,48	1,42	1,33	1,20	1,05	0,89	0,73	0,59	0,46	0,35	0,26	0,19	0,13	0,09	0,06	0,04	0,03	0,02	0,01
Ring 3	5,89	5,96	5,91	5,68	5,30	4,79	4,19	3,55	2,93	2,35	1,84	1,40	1,04	0,76	0,54	0,37	0,25	0,17	0,11	0,08	0,05
Ring 2	23,55	23,85	23,62	22,74	21,21	19,15	16,75	14,22	11,72	9,40	7,35	5,60	4,17	3,04	2,16	1,50	1,02	0,68	0,45	0,30	0,22
Ring 1	94,20	95,40	94,49	90,95	84,82	76,60	67,01	56,86	46,87	37,60	29,39	22,41	16,69	12,14	8,63	5,99	4,06	2,71	1,79	1,21	0,88

Figure 11. Modeling of jammer wave diffraction at four shielding rings covering an antenna in Matlab 6

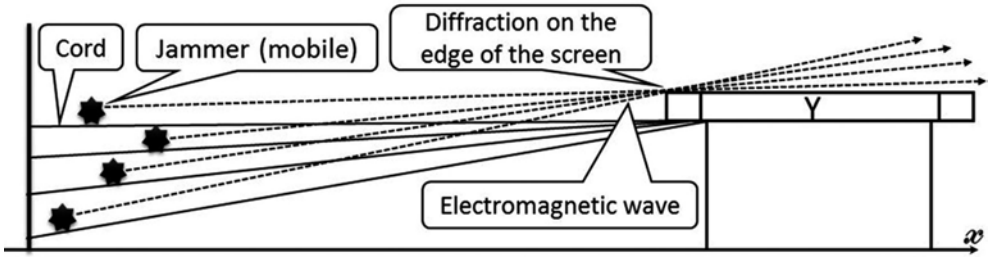


Figure 12. Experimental study of UV shielding: Y – shielded antenna of the receiver

reaching the GNSS antenna is reduced hundreds of times.

Experimental study of UV shielding

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 Figure 12.

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*) until the receiver captured genuine GNSS signals with the help of the antenna *Y*. The result of the experiment: $R = 3.6$ 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 receiver's 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 Figure 12.

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

Conclusions

This paper focusses on the issue of transport security for vehicles relying on GNSS. The subject of this analysis is GNNS-jamming. The shielding of 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. The outcomes were presented through both the use of modeling and experiments to test UV shielding, and they confirmed the assumptions of the authors. Physical experiments have shown that the distance between the GNSS receiver and the jammer, 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 to suppress the original satellite signal. In the future, experiments will be carried out with a precise shield which will be printed using a 3D printer.

References

1. AUVSI (2017) *Association for Unmanned Vehicles Systems International*. [Online] Available from: http://www.auvsi.org [Accessed 15 February 2017]
2. BDBS (2011) *Beacon DGPS Base Station*. [Online] Available from: http://www.mx-marine.com/downloads/BrochureBeacon2011.pdf [Accessed: February 15, 2017]
3. Cameron, A. (2014) *Spoofing, Detection, and Navigation Vulnerability*. [Online] Available from: https://www.youtube.com/watch?v=qlX-MsYZvoM [Accessed: February 15, 2017]
4. Dobryakova, L. & Ochin, E. (2014) *On the application of GNSS signal repeater as a spoofer*. *Scientific Journals of the Maritime University of Szczecin* 40(112), pp. 53–57.
5. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014a) *Design and analysis of spoofing detection algorithms for GNSS signals*. *Scientific Journals of the Maritime University of Szczecin* 40(112), pp. 47–52.

6. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014b) Transport safety: the GNSS spoofing detecting using two navigators. *Logistyka* 3, pp. 1328–1331.
7. Dobryakova, L., Lemieszewski, Ł. & Ochin, E. (2014c) The main scenarios of GNSS spoofing and corresponding spoofing detection algorithms. *Logistyka* 4, pp. 2751–2761.
8. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. & Lachapelle, G. (2012) GPS Vulnerability to Spoofing Threats and a Review of Anti-spoofing Techniques. *International Journal of Navigation and Observation* 2012, Article ID 127072. [Online] Available from: http://dx.doi.org/10.1155/2012/127072 [Accessed: February 15, 2017]
9. MX Marine (2017) *Beacon DGPS Broadcasting Stations network*. [Online] Available from: http://www.mx-marine.com/beacon-dgps-base-stations.html [Accessed: February 15, 2017]
10. NWCG (2016) National Wildfire Coordinating Group. *Basic Land Navigation*. Chapter 5 – Global Positioning System. May 2016, PMS 475, NFES 002865 [Online] Available from: https://www.nwcg.gov/sites/default/files/publications/pms475.pdf [Accessed: February 15, 2017]
11. Nye, J.F., Hannay, J. & Liang, W. (1995) *Diffraction by a Black Half-Plane: Theory and Observation*. Proceedings of The Royal Society A Mathematical Physical and Engineering Sciences 449(1937), pp. 515–535, June 1995. [Online] Available from: https://www.researchgate.net/publication/259054854_Diffraction_by_a_Black_Half-Plane_Theory_and_Observation [Accessed: February 15, 2017]
12. Ochin, E., Dobryakova, L. & Lemieszewski, Ł. (2012) Antiterrorism – design and analysis of GNSS anti-spoofing algorithm. *Scientific Journals of the Maritime University of Szczecin* 30(102), pp. 93–101.
13. Ochin, E., Dobryakova, L. & Lemieszewski, Ł. (2013) The analysis of the detecting algorithms of GNSS-spoofing. *Scientific Journals of the Maritime University of Szczecin* 36 (108) z. 2, pp. 30–36.
14. Ochin, E., Lemieszewski, Ł., Lusznikov, E. & Dobryakova, L. (2013) The study of the spoofer's some properties with help of GNSS signal repeater. *Scientific Journals of the Maritime University of Szczecin* 36 (108) z. 2 pp. 159–165.
15. Pullen, S. & Gao, G. (2012) *GNSS Jamming in the Name of Privacy. Potential Threat to GPS Aviation*, INSIDE GNSS: applications of the Global Navigation Satellite Systems: GPS, Galileo, GLONASS, BeiDou, and related technologies, U.S.A. 2012. [Online] Available from: http://www.insidegnss.com/auto/marapr12-Pullen.pdf [Accessed: February 15, 2017]
16. Retscher, G. (2002) Accuracy Performance of Virtual Reference Station (VRS) Networks. *Journal of GPS* 1, 1, pp. 40–47.