SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY
2020 (LXI) 4 (223)

sciendo

DOI:10.2478/sjpna-2020-0013

POSSIBILITIES OF DETECTION OF THE JAMMING OF THE GNSS RECEIVER WITH THE HELICAL ANTENNA

Andrzej Felski[1] Piotr Stopienski[2*]

[*] *Polish Naval Academy, Faculty of Navigation and Naval Weapons, Śmidowicza 69 Str., 81-127 Gdynia, Poland; [1]e-mail: a.felski@amw.gdynia.pl; [1]ORCID ID: 0000-0002-0326-3397; [2]e-mail: p.stopienski@o2.pl*

ABSTRACT

Jamming of GNSS signals is lately treated as essential threat for GNSS users. It is especially dangerous in the face of common usage of GPS-like systems in everyday life, and the great belief of everyday users in the truth of devices indications. In spite of the legal prohibition of using them, jammers are commonly accessible, especially in the Internet. Last years showed however that such threat generated purposely also some governments, what is clearly visible in armed conflicts, and during military exercises. Of course this creates the great threat for civilian users if will be in the vicinity.

Applications and services based upon GNSS are becoming increasingly embedded in modern society, so community have now become critically dependent upon their correct operation. This refers positioning first of all, but telecommunications networks, power grids, financial transactions, whole world of logistics are dependant as well. The main users of GNSS, both professional and non-professional smartphones users are not prepared on such situation, and usually have no technical possibilities to detect of jamming. For operators of critical installations, for example seaports, or airfields, the detection of jamming cases is extremely important. It can be provided with special devices, which are usually based on specific antennas, and deep analysis of signal. In this paper experiments in detection of the jamming with helical antennas are discussed

Keywords:
GNSS Receiver, helical antenna.

Research article

INTRODUCTION

Global Navigation Satellite System (GNSS) is a common acronym for US Global Positioning System (GPS), and similar to them: Russian GLONASS, European Union Galileo, and BeiDou of China. There are accessible for free, and widely used in many fields, including navigation, positioning, surveillance, search and rescue, as well as in many field based on precise timing (electric power net, banking, communication etc.), and other public services (for example such applications as tracking of costly goods, pay-as-you-drive services, sport application, even wild animals behavior monitoring). However the weak side of all these systems is the low power of radio-transmitters installed on satellites, so signal received on the Earth is very week. Their vulnerability to radio frequency interference (RFI) is drawing significant attention, as it is especially problematic for GNSS-based safety-of-life services, such as aviation, or digital mobile communication. Complete list of possible sources of GNSS receiver malfunctioning consists[5] of:

- User's receiver and antenna noise,
- Multipath, which is especially important in urban area,
- Atmosphere status, in which solar activity, and its influence on the state of Ionosphere (its ionization) are the most important,
- Space segment errors, mainly orbit perturbation, but even erroneous data, and possible Space Vehicle (SV) faults,
- Cyber-attacks on Ground Segment, or on satellites,
- Unintentional interferences with other radio signals,
- Intentional disturbances in GNSS satellites signals.

Apart from the multipath, only natural disturbances for long time has been discussed as the serious threat for GPS. The special attention was directed on the activity of the Sun, and state of Ionosphere which especially determined the threat for such systems in polar, and magnetic equator areas. But now it is clear, that the main threat for GNSS systems are intentionally produced false signals in GNSS spectrum. In this threat of jamming (the process of generating a radio-waves of noise character in the GPS spectrum to block or interfere with satellite signals) is the most common, but nowadays spoofing is observed in many places also. Spoofing, is a more complicated activity, and puts on thatching itself under satellite of the system, and transmission of false signals whose the receiver will not recognise, and makes receiver believe it is at false location. Jamming is a kind of activity which form a powerful radio signal, intentionally generated to disturb GNSS service. The most popular jammer has power in miliwatt, but there are military jammers with power of dozen of Watt. Depending on power of the jammer, the size of an area where jamming may

appear is from few meters to hundreds kilometers. It is an illegal activity[1], however they appear in our everyday life everywhere. Probably the most known example is the case of Newark International Airport, where truck driver was using the jammer for a long time to counteract monitoring his activity by his boss [20], but his jammer was so powerful, that it was disrupting Ground-Based Augmentation System ground station. Later similar accidents was notified on many airfields.

Another commonly known example of jamming is the activity of North Korea's military forces against South Korea in region of Seoul and Inchon Airport. This events are examples of the problem [17]. Since the engagement of Russia into the conflict in Syria, similar events are every-day-reality in the eastern part of the Mediterranean Sea.

In spite of jamming, last four years accidents of spoofing are observed more often. This is activity in which some false signals similar to GNSS are generated with the aim to deceive user's receiver. As an result the false coordinates will be calculated.

Whether one likes it, or not, our society has become strongly dependent on the Positioning, Navigation, and Timing infrastructure. The widespread of the GNSS use in all aspects of everyday life entails the average user's belief in the truth of data presented by receiver. Today it is clear that our world urgently wants immune and resilient PNT systems [1]. It is not only question about position, or navigation, but many other critical infrastructures of our society would literally collapse in case of a GNSS failure. The transfer of time data is equally essential for GPS service. Without it, data systems, and energy systems cannot work. In this context, the opportunity to detect such events are critical.

JAMMERS

GNSS jamming is a form of intentional radio-interferences generated by devices, which deliberately transmit signals at the specified frequencies with the power sufficient for disrupting GNSS-based services. In this way GNSS-based services can be disrupted on distances up to of several kilometers from jammer, it depends mainly on the power of the jammer. However, the impact of jamming depends also on receiver circuit, antenna characteristics, and a spectrum of signal generated by jammer. Jamming is not the zero-one process: on some distances jamming is ineffective, on shorter distances it degrades signals of some part of visible satellites, and when even closer, it is completely blocking receiver [12]. The reaction of different

[1] For example in Poland this is the order of Ministry of Transport of 3 July 2007.

types of receivers is dissimilar. Besides, in some part it depends on the height of satellites above the horizon, as satellite elevation is correlated in some part with the signal strength. It causes jamming variety of different space vessels. One can also observe correlation between jamming process, and of the antenna parameters [7]. Briefly the reactions of the same receivers with different antennas vary.

In this context one should dedicate the special attention to jamming devices. Several papers have addressed the problem of characterizing the jamming signal. Probably most jammers used in a civil context can broadcast frequency modulated signals, which covers all GNSS band, or can be periodically moved over the band, mostly in tooth-mode [18]. There are jammers which cover not only the L1 band, but sometimes mobile phones frequency too. Depending on the properties of generated radio, waves jammers can be classified in different ways. Rash [16] suggest to divide jammers into three categories:

1. Continuous wave, occupying less than 100 KHz bandwidth;
2. Narrowband jamming occupying more than 1 MHz of bandwidth, but less than, or equal to, the entire 1.023MHz bandwidth of C/A code;
3. Wideband jamming occupying the entire 10.23 MHz bandwidth about L1, or L2.

Different classification with four classes of jammers was proposed by [14], or [11]:

- Class I: CW signals;
- Class II: single saw-tooth chirp signals;
- Class III, multi saw-tooth chirp signals (the device transmits a frequency modulated signal, but its RF evolution is determined by the combination of several saw-tooth functions);
- Class IV, chirp with signal frequency bursts (the device transmits a frequency modulated signal, and frequency bursts are used to enlarge the frequency band affected by the disturbing signal).

It cannot be in doubt, that professionals have at their disposal devices, which possess completely different properties. There is no information about technics which are implemented for generating jamming signal, but it is clear that power of this group of devices is much higher than "personal" one. So called "electronic countermeasure devices" are offered by Allen Vanguard, CAST, Chronos Technology, Novatel, Forsberg etc. This is not only the domain of the activity of the west forces, as Russia announced its electronic warfare systems too, for example the Borisoglebsk-2, Krasukha, Parodist etc. electronic warfare (EW) complexes which compromises of several stations based on a multi-purpose armoured all-terrain vehicle [13]. There are suggestions in the media, that Turkey, Israel, China, and other countries do the same.

As far as "personal devices" usually possess little power measured in milliwatts, then professional devices generate power even to 500 W.

POSSIBILITIES OF JAMMING COUNERMEASURE

Designers of GPS found that the use of the spread spectrum of the signal would assure the resistance on interferences. In that case nobody anticipated needs of the uses in the receiver of the mechanism verifying the occurrence of disturbances. At the moment the standard GNSS receiver is not equipped with any tool for detecting the jamming, and for ordinary users it is difficult to discover such accident. Most often it ascertains disturbances when the receiver freezes indications, while the carrier changes its own position, or coordinates on the display are completely different than on the other navigation devices. However, today some new receivers can inform its user about jamming incidents by changing the status on dedicated pin. There are also accessible products equipped with a mechanism of transmitting NMEA warning, or function of informing the user about detected abnormal values of S/N ratio, which can suggests jamming. Solution in jamming resistant devices is integration GNSS receiver with Inertial Systems, when mechanism of comparing the coordinates can be implemented. Other way is the usage of very sophisticated receiver with complicated segment-antenna, and Beam-Forming Mechanism, which can create null sections in antenna beam, that signals from some directions will not be received [4]. [2], [3], [6]. By using multiple antenna elements spaced a known distance apart, signal-processing techniques can be employed to discern the direction, from which an interfering signal is arriving, and then adaptively change the apparent receiving strength of the antenna array, creating null gain in source of interference's direction. This idea is implemented into Novatel's (Veripos) GAJT receiver for example.

The main goal using the jammer is to exclude GNSS services in a particular area, and it seems easy to detect by comparison the signal to noise ratio. But the detection of the appearance of disturbances is not enough for locating jammer. In addition, the direction from which an interfering signal is arriving, must become fixed. It is impossible with the standard receiver, as the standard receiving antenna of GNSS receiver's has hemispherical beam pattern, and receive all signals from sources distributed over horizon. Dedicated anti-jamming service should be able, as a minimum to alert users, and it would be desirable, to show direction (or position) in which jammer is situated. Such solution creates the chance of neutralizing the intruder. Nowadays some models of jamming detectors are accessible, however it is not a big market. In the open sources CTL3520, and CTL3510 GPS Jammer Detectors

and Locators of CHRONOS are suggested, however some other are offered too. In this paper one refer to the results of experiments in use ordinary receiver equipped with directional antenna. Detecting the azimuth, or sector in which jammer is located gives the opportunity to determine its location by intersection of two directions determined from two points. An example of such solution can be the Signal Sentry GPS system offered by Harris [10]. The net of two, or more sensors (more sensors gives more accurate results) placed strategically around the port, will instantaneously sense and locate the jamming sources. The data is analysed in real time, the threat type is verified, geolocated, and presented on a web-based visual map. If there are multiple jamming sources present, the system locates each individually.

Authors of this paper found, that the protection of the critical infrastructure from disturbances demanded establish at least two stationary posts with opportunity to determine at least two directions on the source of disturbances, so it gives localization of the area in which jammer is situated. It is possible by using directional antenna with GNSS receiver. We assume that each post will consists of number of receivers equipped with directional antennas [15]. For example, receiving system equipped with three antennas with 180deg sector of beam pattern in the horizontal direction (fig. 1) gives the opportunity to detect the direction in sector of 60 deg. by comparing the signals peer-to-peer.

Let's assume, that in the reception area a signal is available from nine navigation satellites. It seems rational to found that in the region one jammer is located, so signal is transmitted from one direction. Antenna 1, along with a supporting receiving device (signal processor 1) decodes, and processes navigation information from satellites Sv2, Sv3, Sv4, and Sv5. Antenna 2, with a signal processor 2 from: Sv5, Sv6, Sv7, and Sv8, respectively. Antenna 3, with a signal processor 3 from: Sv8, Sv9, Sv1, Sv2, respectively plus a jamming signal. A control and processing device – a navigation processor - continuously analyses, and processes navigation information from all signal processors, and when signals from one of the receiving channels is clearly different from that obtained from the other (as it consists of satellite signals and jammer noise), the channel can be blocked. In this example signals from Sv2 in track 1 (antenna 1 and signal processor 1), and track 3 (antenna 3 and signal processor 3) should differ because of jammer signal presence in track 3. Finally Sv 1 and Sv7 can be skipped in calculations of the position (Sv2 will be received by track 1), but based on the current knowledge about satellites' accessibility the remaining number of satellites is more than 4. The more important is, that this way we know that jammer is located in direction ±30deg from North. For example, if signal will be detected by signal processor 1 and 2 this can be interpreted as jammer is located in the sector between azimuth 300 degrees and 330 degrees.

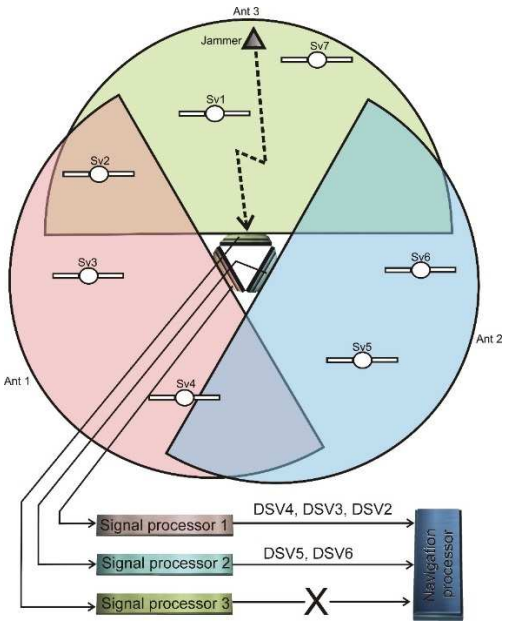

Figure 1. Scheme of device with three antennas, and three parallel receivers.
Source: Felski, 2016

MATERIALS AND METHOD OF EXPERIMENT

In this research we used GPS receivers series R100 of Hemisphere working with helical antennas [21] M1575HCT-22P-SMA of Maxtena Inc. It is a rugged high performance passive antenna designed for the GPS L1 band (fig. 2). An ultra-light (10 grams) screw-on design, featuring an integrated SMA connector. As both, the receiver, and the cabling which we had at our disposal in the laboratory, did not foresee the use of the SMA standard, additionally the transit connectors and the antenna amplifier were used.

Figure 2. Antenna M1575HCT-22P and transition connector.
Source: authors' photo.

Its antenna pattern shape is typical for GNSS antennas (see fig. 3), however its dimension and weight gives opportunity to use its as directional one, if its main axis is oriented horizontally. If so, in horizon it forms almost 180 deg sector, as well in vertical plane – only 90 deg from the horizon plane. We assume, that in such configuration all signals from satellites seated in direction opposite to the orientation of the antenna will not be received, as the radiation generated by jammer. In addition the signals from satellites located in direction of antenna pattern will be received without jammer noise.

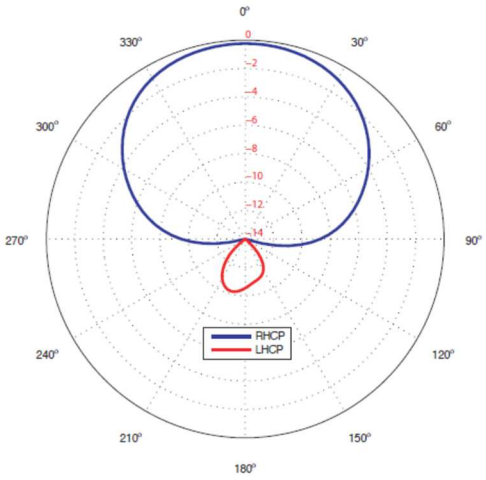

Figure 3. MS575HCT-22 antenna gain plot in vertical intersection.
Source: GPS Helix Antennas

During experiments small, battery powered GPS jammer of Spy Electronics LTD, has been used. It is a device purchased by Internet with (theoretically) 15 meters of radius of activity. [Stopienski, 2020]

Figure 4. Devices applied to experiments: R110 receiver and Spy Electronic jammer.
Source: authors' photo

Receivers were steered with the use of PocketMax4 software, for analysing the local satellite configuration and satellites received by device, we used freely accessible Trimble GNSS Planning software. Example of visualisation of SkyPlot, and received signals with the information about S/N Ratio, is presented on the figure 5. All results and observations were exported to text files with the use of the NMEA 0183 standard, first – the GPGSV message. The message gives the information on the number of visible satellites, their azimuth, the elevation, and the signal strength (see fig. 6).

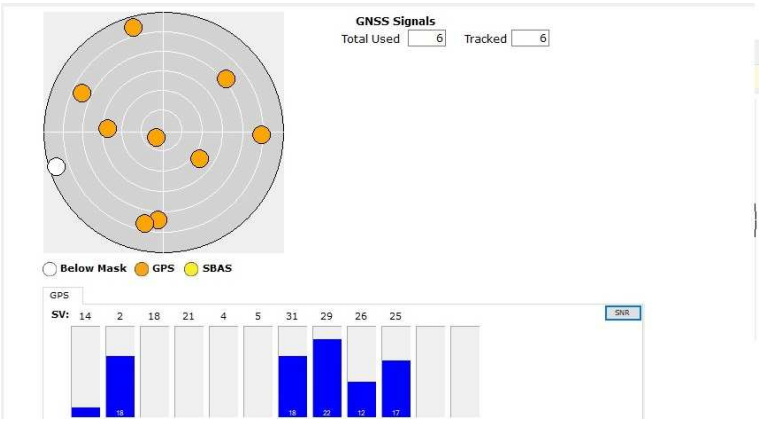

Figure 5. Visualisation of tracked satellites with the standard antenna.
Source: Pocked Max4, authors.

```
$GPGSV,3,1,10,02,42,069,51,06,22,040,,12,47,104,,14,21,268,,*54
$GPGSV,3,2,10,24,04,,,25,81,117,52,26,01,288,33,29,57,24,44,*7D
$GPGSV,3,3,10,31,37,302,47,32,10,246,,,,,,,,*7C
```

Figure 6. Content of GPGSV message adequate to configuration presented on fig. 5.
Source: authors' research.

From the fig. 5 we concluded, that receiver should track 10 satellites with numbers: 02, 06, 12, 14, 24, 25, 26, 29, 31, and 32, however in this example only six (branded in red on the fig. 6) are tracked (02, 14, 25, 26, 29, and 31). Particularly in this example four satellites were shadowed by neighbouring building, and because of that during the next experiments antenna was moved into new place. This example is useful to show how the satellite is presented, which is found within the antenna pattern, however its signal is not taken – after the valuation of the azimuth the value of the signal to the noise ratio should appear. If the signal is not taken, no symbol appears among following commas separating every value (in the fig. 6. for example sat. 06). Figure 6 shows, that over the receiver ten satellites are accessible, all information is divided into three parts and, for example elevation of satellite no 02 is 42 degree, its azimuth is 069 degree and S/N ratio is 51.

On figure 7 the similar information (recorded few minutes later) is presented, but jammer is switched on at the north direction of antenna, at the distance of 10 meters from antenna, and 3 meters over antenna horizon (elevation of about 17 degree over the antenna plane). It must be noticed, that number of tracked satellites dropped from 6 to 3, and S/N ratio dropped down, for example for sat. no 29 from 44 to 35. Important conclusion from similar tests is that low elevation satellite are eliminated by jamming. In this example all satellites below the elevation of 48 degree are eliminated. When active jammer was switched on at the distance closer than 10 meters all signals were blocked in our experiments.

```
$GPGSV,3,1,11,02,22,047,,04,09,336,,05,20,084,,09,01,008*56
$GPGSV,3,2,11,12,17,120,,18,32,182,21,28,192,,25,48,129,35*55
$GPGSV,3,3,11,26,29,296,,29,87,090,35,31,48,262,34,,,,*4F
```

Figure 7. Content of GPGSV message adequate to configuration presented on fig. 5 after the jammer switched on.
Source: authors' research.

The following step of experiments was connection of the helical antenna (situated with main axis almost horizontally, and in azimuth 278 deg.) to the same receiver, and the check of the visibility of satellites. Example of such data is presented on fig. 8. According to the expectations only the part of satellites were tracked, it means only these which were located within the range of the antenna pattern (showed as red sector) oriented in the azimuth of 278 deg.

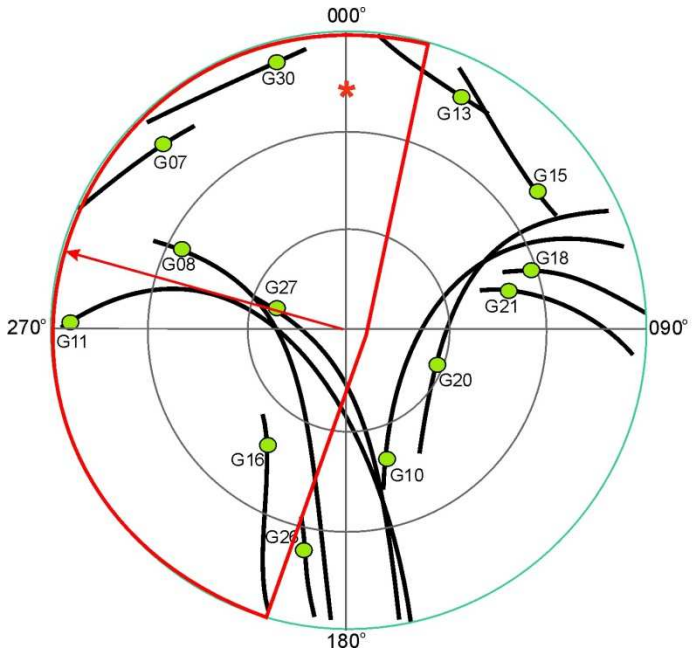

Figure 7. Example of the SkyPlot.
Source: on the basis of Trimble GPS Planner. Red sector present the antenna pattern, red star – jammer.

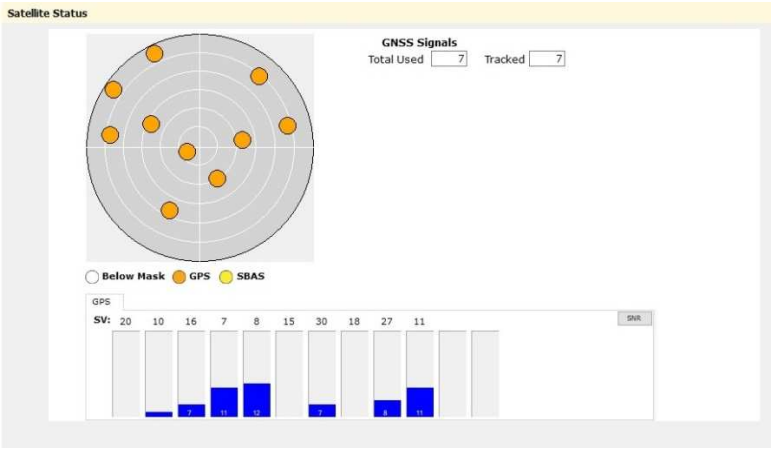

Figure 8. Visualisation of tracked satellites with the helical antenna situated in the horizon plane and in azimuth 278 deg.

In this orientation of the antenna, according to the shape of beam pattern, only six satellite should be tracked. As it is shown on fig. 8 high satellite #10 seems to be

tracked additionally with the use of Pocked Max4, but this is not shown in NMEA 0183 messages (see fig. 9). It is proper to notice that low elevation satellite, for example 7, or 11, possess the very good S/N ratio, while at the use of the traditional antenna, usually such of the satellite show low S/N ratio. Of course this gets out of characteristics of the antenna, when its main axis is not placed vertically.

After the jammer was switched on, only satellite #08 was tracked by the receiver, the other signals were blocked (see fig. 10).

```
$GPGSV,3,1,12,07,09,310,39,08,39,296,41,10,54,157,,11,12,274,41*70
$GPGSV,3,2,12,13,09,020,,15,18,47,,16,41,209,38,18,24,073,,*69
$GPGSV,3,3,12,20,59,091,,21,33,078,,27,74,278,39,30,07,339,36*79
```

Figure 9. Content of GPGSV message adequate to configuration presented on fig. 7, and fig. 8 with helical antenna.
Source: authors' research

```
$GPGSV,3,1,12,07,09,310,,08,39,296,34,10,54,157,,11,12,274,,*51
$GPGSV,3,2,12,13,09,020,,15,18,047,,16,41,209,,18,24,073,,*52
$GPGSV,3,3,12,20,59,091,,21,33,078,,27,74,278,,30,07,339,,*5A
```

Figure 10. Content of GPGSV message adequate to configuration presented on fig. 7, and fig. 8 with helical antenna, and jammer switched on.
Source: authors' research.

In the following example we will talk about the situation when two helical antennas were placed in azimuths 230 and 327 degrees, and was connected to the separate receiver. Jammer, if switched on, was situated in the same place.

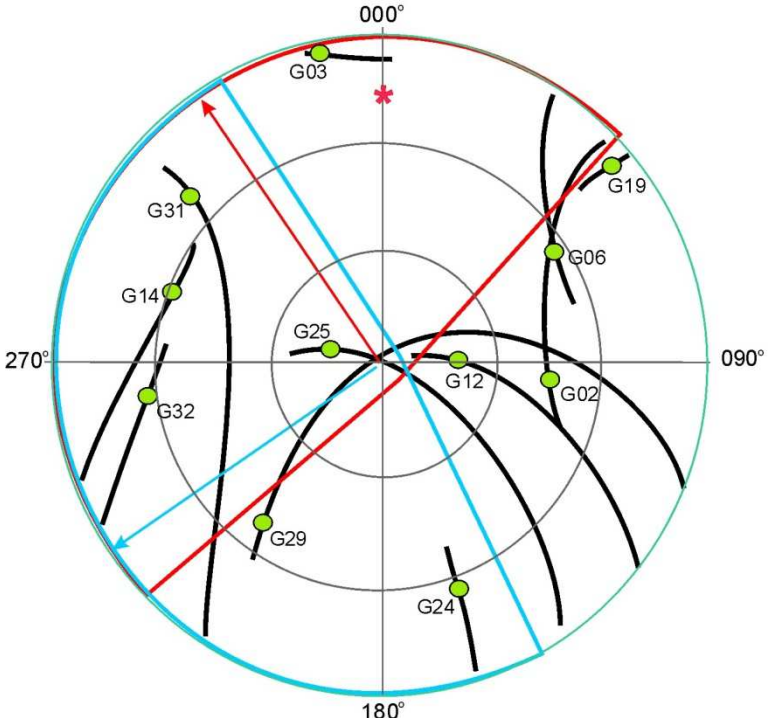

Figure 11. Example of the SkyPlot when two helical antennas are in use.
Source: on the basis of Trimble GPS Planner. Blue sector presents first antenna pattern, and red one – the second.

```
$GPGSV,3,1,11,02,43,094,,03,03,347,,06,32,055,,12,67,091,,*52
$GPGSV,3,2,11,14,28,287,41,19,05,049,,24,22,161,36,25,77,281,36*73
$GPGSV,3,3,11,29,37,217,42,31,21,310,41,32,24,260,36,,,,*44
```

Figure 12. Content of GPGSV message adequate to configuration presented on fig. 10 with helical antenna in azimuth 230deg.
Source: authors' research.

```
$GPGSV,3,1,11,02,43,094,,03,03,347,37,06,32,055,,12,67,091,,*56
$GPGSV,3,2,11,14,28,287,41,19,05,049,20,24,22,161,,25,77,281,36*74
$GPGSV,3,3,11,29,37,217,,31,21,310,41,32,24,260,36,,,,*42
```

Figure 13. Content of GPGSV message adequate to configuration presented on fig. 11 with helical antenna in azimuth 327deg.
Source: authors' research.

Than jammer situated northerly of antennas (red star in the red sector on the fig. 11) was switched on. It caused the disturbance of signals taken by this antenna, and the

blocking of the receiver. However this had no influence on the work of the second receiver, which was connected to second antenna (See figures 14 and 15).

```
$GPGSV,3,1,11,02,43,090,,03,03,349,,06,32,053,,12,65,093,,*5E
$GPGSV,3,2,11,14,28,285,41,19,08,049,,24,20,161,36,25,80,281,33*73
$GPGSV,3,3,11,29,38,220,42,31,24,308,41,32,22,268,36,,,,*4D
```

Figure 14. Content of GPGSV message adequate to configuration presented on fig. 11 with helical antenna in azimuth 230deg., and jammer switched on.
Source: authors' research.

```
$GPGSV,3,1,11,02,43,090,,03,03,349,,06,32,053,,12,65,093,,*5E
$GPGSV,3,2,11,14,28,285,,19,08,049,,24,20,161,,25,80,281,,*5F
$GPGSV,3,3,11,29,38,220,,31,24,308,,32,22,258,,,,*48
```

Figure 14. Content of GPGSV message adequate to configuration presented on fig. 10 8 with helical antenna in azimuth 327deg., and jammer switched on.
Source: authors' research.

When signals were taken through the "blue" antenna, and did not take through the "red" one, jammer is located in the section among 320 and 057 degrees. This confirms the hypothesis that the system designed with sectorial antennas, and separate receivers serving each sections, and also the element comparing signals taken in each tracks assures the detection of jamming events, and settlements of the section, whence this disturbance originate

CONCLUSIONS

Today the threat a jamming of GNSS systems is indisputable. In this article results of experiments with sectorial, and helical antennas were described. These are different from commonly used in the GNSS technique non-directional antennas. Authors hypothesized, that the sectorial pattern of helical antennas allow to limit the jamming, if such antennas will act as the group.

Experiments confirmed the hypothesis that jammer being found outside the section of the activity of the helical antenna did not cause disturbances to the adequate receiver. Our research was passed only with the GPS receiver, however, there cannot be doubts that these rules bear upon all GNSS systems. Of course this is a truth for the certain distance among the jammer, and a receiver, what is mainly determined by the jammer's power.

Similar solution takes place if it is be based on the same number of directional antennas working with separate receivers, or to apply the mechanism of comparing of the relation of the signal to the noise, and the analysis of name of tracked satellites

gives the simple mechanism of the detection of the jamming, and besides this permits to estimate the direction whence comes the disturbance. Examples presented in the paper confirm above.

It became proved, that two antennas situated at the same place, however, directed differently had taken signals from different satellites, and were subject to jamming, or not, depending on the direction wherein the perturbative device was placed. Such solutions would be able to find the use of the installation whose functionality in the critical degree depend on the correct work of GNSS.

REFERENCES

1. Carroll J.V. *Vulnerability Assessment of the U.S. Transportation Infrastructure that Relies on the Global Positioning System*. Journal of Navigation vol.56 issue 2, 2003, pp. 185-193.
2. De Lorenzo D.S., Rife J., Enge P. and Akos D.M. *Navigation Accuracy and Interference Rejection for an Adaptive GPS Antenna Array*. ION GNSS 2006, pages 763-773.
3. De Lorenzo, D.S. *Navigation Accuracy and Interference Rejection for an Adaptive GPS Antenna Array*. PhD Thesis. Department of Aeronautics and Astronautics, Stanford University, US, 2007 (Available at http://waas.stanford.edu/pubs/phd_pubs.html)
4. Digital Beam-Forming Apparatus and Technique for a Multi-beam Global Positioning System (GPS) Receiver Patent US 2008/0291079 A1 2008.
5. *Extreme space weather: impacts on engineered systems and infrastructure*, Royal Academy of Engineering, London, 2013. Available at: https://www.raeng.org.uk/publications/reports/space-weather-full-report (12.09.2014).
6. Fante, RL; Vaccaro, JJ. *Wideband cancellation of interference in a GPS receive array*. IEEE Trans. Aerosp. Electron. Syst 2000, 36, 549–564. [Google Scholar].
7. Felski A., Gortad M. *The significance of an antenna for jamming resistance of a GPS receiver.* Scientific Journal of Polish Naval Academy vol. LVII, no. 4/2016, pp. 5-16.
8. Felski A. *Methods of improving the jamming resistance of GNSS receiver*. Annual of Navigation no. 23/2016 pp. 185-198.
9. GPS Helix Antennas. https://www.maxtena.com/products/helix-antennas/gps-helix-antennas/ (04.08.2020).
10. GPS Interference Detection and Geolocation System. Harris Corporation, 2015. Available at: https://www.ion.org/gnss/upload/files/1525_Harris_PNT_signalsentry_infographic.pdf (04.08.2020).

11. Kraus T., Bauernfeind R. and Eissfeller B., *Survey of in-car jammers – analysis and modeling of the RF signals and IF samples*. In: Proceedings of the 24th International Meeting of the Satellite Division of the Institute of Navigation Portland, 2011.
12. Kuusniemi H., Bhuiyan M. Z. H., Kroger T. *Signal Quality Indicators and Reliability Testing for Spoof-Resistant GNSS Receiver*. European Journal of Navigation vol. 11 no. 2, 2013.
13. McDermott R.N. *Russia's electronic warfare capabilities to 2025*. Republic of Estonia MoD, 2017.
14. Mitch R.H., Dougherty R.C., Psiaki L.M., Powell S.P., O'Hanlon B.W., Bhatti J.A., Humpreys T.E., *"Signal Characteristics of Civil GPS Jammers,"* Proc. Of the 24th Int. Techn. Meeting of the Satellite Division of ION, Portland 2011 Available at: http://gpsworld.com/gnss-systeminnovation-know-your-enemy-12475/ (04.08.2020).
15. Rama Rao B., Kunysz W., Fante R., McDonald K. *GPS/GNSS Antennas*. Artech House Boston, London 2013.
16. Rash. G. D. *GPS jamming in a laboratory environment* Proc. Of the 53rd Annual Meeting of the ION, Albuquerque, 1997.
17. Reports: *North Korea jamming South's air traffic navigation*. Available at: https://news.blogs.cnn.com/2012/05/03/reports-north-korea-jamming-souths-air-traffic-navigation/ (04.08.2020).
18. Scott L.: *Spoofs*, Proofs & Jamming, Inside GNSS, September/October 2012, s. 42-53.
19. Stopienski P. *Opportunity to elimination Jamming by the adequate formation of the antenna beam of the GNSS receiver* (in Polish: Możliwości eliminacji Jammingu poprzez adekwatne kształtowanie wiązki antenowej odbiornika GNSS). Master Thesis. PNA, Gdynia 2020.
20. Truck Driver with GPS Jammer Accidentally Jams Newark Airport. Available at: https://www.scientificamerican.com/article/truck-driver-has-gps-jammer-accident-2013-08/ (04.08.2020).
21. Wang Y-S., Chung S-J. *A miniature Quadrifilar Helix Antenna for Global Positioning Satellite Reception*. IEEE Transactions on Antennas and Propagation. Vol. 57, no. 12, 2009, pp. 3746- 3751

MOŻLIWOŚCI WYKRYCIA ZAGŁUSZANIA ODBIORNIKA GNSS PRZY POMOCY ANTENY ŚRUBOWEJ

STRESZCZENIE

Zagłuszanie sygnałów GNSS traktuje się ostatnio jako istotne zagrożenie dla użytkowników GNSS. Jest to szczególnie niebezpieczne w obliczu powszechnego stosowania systemów typu GPS w życiu codziennym oraz wiary użytkowników w prawdziwość wskazań urządzeń. Mimo prawnego zakazu ich używania jammery są powszechnie dostępne, zwłaszcza w Internecie. Ostatnie lata pokazały jednak, że takie zagrożenie celowo generowały również niektóre organy rządzące, co widać wyraźnie w konfliktach zbrojnych i podczas ćwiczeń wojskowych. Oczywiście stwarza to wielkie zagrożenie dla użytkowników cywilnych, jeśli znajdą się w zasięgu.

Aplikacje i usługi oparte na GNSS są coraz częściej osadzone we współczesnym społeczeństwie, więc społeczność stała się obecnie w decydującym stopniu zależna od ich prawidłowego działania. Dotyczy to przede wszystkim pozycjonowania, ale zależne są też sieci telekomunikacyjne, sieci energetyczne, transakcje finansowe, cały świat logistyki. Główni użytkownicy GNSS, zarówno profesjonalni, jak i nieprofesjonalni użytkownicy smartfonów, nie są przygotowani na taką sytuację i zwykle nie mają technicznych możliwości wykrycia zagłuszania. Dla operatorów instalacji krytycznych, na przykład portów morskich lub lotnisk, wykrywanie przypadków zagłuszania jest niezwykle ważne. Jest to możliwe za pomocą specjalnych urządzeń, które zwykle opierają się na określonych antenach i głębokiej analizie sygnału. W artykule omówiono badania dotyczące wykrywania zagłuszania za pomocą anten śrubowych.

Słowa kluczowe:

Odbiornik GNSS, antena śrubowa.