DOI: 10.36163/aon-2024-0002

THREATS FOR GNSS – PRESENT STATUS & COUNTERACTIONS

Andrzej Felski
Navigation and Marine Hydrography Chair
Polish Naval Academy
Gdynia, Poland
a.felski@amw.gdynia.pl

ABSTRACT

Nowadays, most of the society, especially young people, treat GPS as an obvious source of information, just like television, radio or the Internet. In fact, we are dealing not only with the American system, but also several others that make up Global Navigation Satellite Systems. This is the primary source of situational awareness for many activities: professional, military and business as for everyday use. From crisis actions, by timing and synchronization in critical infrastructures such as financial, communications, power grid and industrial systems, and more. In fact, we can talk about the critically reliant of human life upon GNSS. Like any radio system, GNSS is also susceptible to interference and changes in the ionosphere, however on the turn of the centuries appeared the new, not expected threat in the form of more and more frequent cases of interferences, especially intendent one. If so, appears the question how to recognize this threat and how to proceed in such case? In the paper, some current information about the question, as well as some suggestions how to act on board in such cases will be presented.

Keywords— GNSS, Jamming, Spoofing, Countermeasures to GNSS threats

1. INDRUCTION

For mane mariners GPS is a synonym of navigation, but in fact, this is a technology, which is used for much more than just navigation. And not only American version of such systems is in the use. So, since many years we can talk about Global Navigation Satellite Systems (GNSS). These are different systems, but from the user's point of view, the principle of their operation is identical, and from the point of view of this article, the issue applies to all of them equally. It is important that commonly used variants of the system operate on identical frequencies, so possible interference affects all of them: American GPS, European GALILEO, China BEIDOU, as well as Russian GLONASS.

All GNSS services are critical for real-time information on positioning, navigation and time (PNT). Because of the highly accurate and continuous PNT solution provided in all weather conditions and all over the world, this multi-use technology, originally designed for the armed forces, has been adopted for civil applications including some for transportation, agriculture, aviation, emergency services, location dependent services and many others. The increasing societal dependence on PNT services delivered by GNSS has also created a set of security vulnerabilities for the applications, which base on them. The fundamental problem is the accuracy and accessibility of them, as well as resistance of these systems to interference. In this article we will deal with the issue of intentional jamming, which has been widely discussed recently. We will consider the nature of jamming impacts, the level of commonness of these phenomena and the capabilities of the GNSS user on the ship to minimize the impact of these activities on the receiver. The presented considerations are based on the analysis of literature, on logical analysis of the described phenomena and on many years of experience in operating such equipment.

Systems of GNSS group, since they are based on the electromagnetic waves, are sensitive to the status of ionosphere, and environment in general. But in addition, are vulnerable on signal interference, which can be accidental, but also - intentional. The threat of GPS in the form of electromagnetic interference was already known at the turn of the 1980s and 1990s (see [4] for example) but was ignored for long time. Research on this issue began only at the end of the 20th century [2, 3, 5]. Important is, that GNSS service may be intentionally degraded or disrupted during military operations, in form of jamming or spoofing. However, if talking about intentional threats for GNSS we should mention such as cyber threats or physical destruction of the space segment, as well as ground elements, also. But this paper only discusses jamming and spoofing as it is very common and can lead to inaccurate PNT service and poor navigation performance.

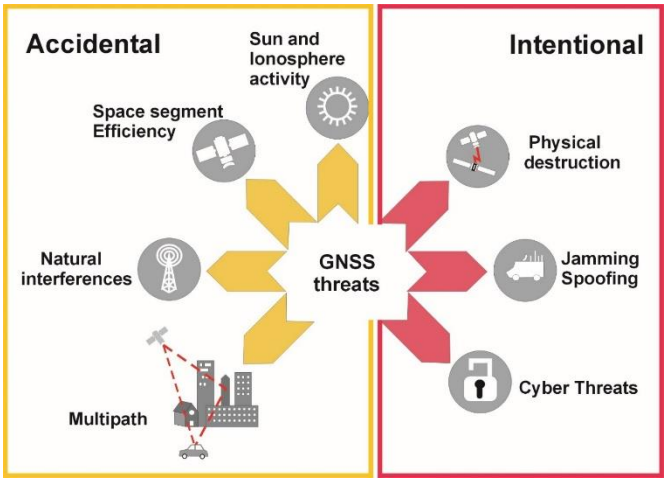

Fig. 1. Possible GNSS threats.

Cases where GNSS service is unavailable or significantly degraded require alternative solutions to PNT, but the unprecedented success of GPS led to the abandonment of almost all alternative systems that were in operation by the end of the 20th century. Only remnants of the Loran C system still exist in Russia and Asia's Pacific coast and still we wait for eLoran. In this situation, several countermeasures are implemented by providers, to mitigate the security vulnerabilities. These include frequency excision to negate narrow band interference and blanking to negate pulsed interference, but also smart ranging code design and smart antenna design [15]. For example, GPS transmitting systems is in the process of modernization including higher transmitter powers on Block III satellites, new, more resistant codes (M, L2C) and a new frequency (L5). On the receiving side, producers propose more advanced signal filters and adaptive antennas. However, this requires the purchase of new receivers, which not every user is satisfied with, and process of modernization GNSS is still in progress. So, the question arises: how important is the problem and what should a user of older receivers do?

2. THE ESSENCE OF THE PROBLEM

Jamming involves intentional radio frequency interference that prevents GNSS receivers from receiving satellite signals, rendering the system degraded or fully ineffective. It creates a kind of barrier that limits the ratio of the power of the incoming signal to noise, which leads to a reduction in the number of received satellites, sometimes even to a drop below four, thus completely blocking the receiver. Of course, it depends on the power of the jammer and the distance to it. Meanwhile, spoofing involves feeding false satellite signals to fool GNSS receivers, resulting in incorrect position, navigation and time (PNT) data.

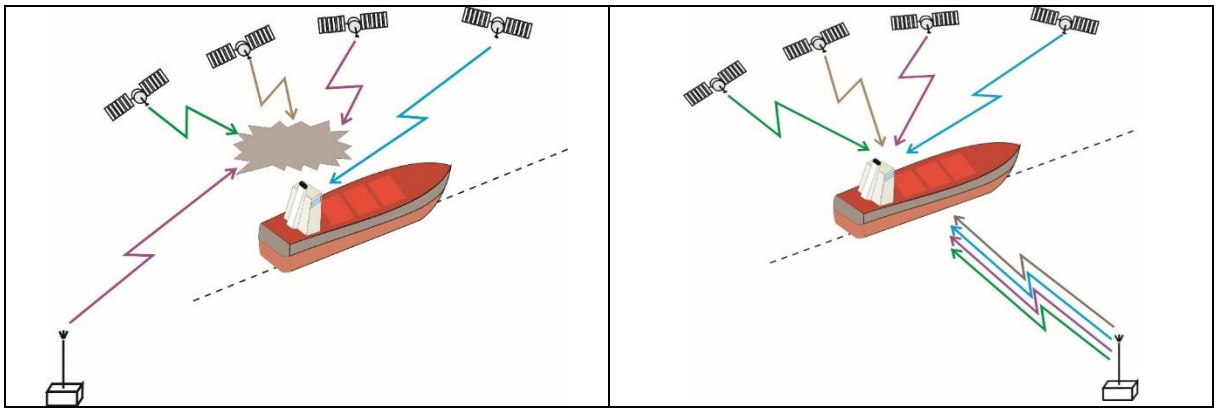

Fig. 2. The essence of jamming and spoofing.

Jamming typically results in immediate and noticeable effects, whereas spoofing is more difficult to detect and poses a higher safety risk. As a rule, jamming may be noticed by operator if notice such symptoms like lower number of tracked satellites or lower carrier-to-noise ratio (C/No). This is the carrier power divided by noise power density (expressed in dB/Hz) and means the ratio of the received signal power, to the spectral density power of the noise in the receiver circuits though it isn't an information about the power of the satellite signal. When the GPS signal is received on the Earth surface, its power is very week. As the satellite's altitude is approximately 20200 kilometres, the corresponding path loss is around -157 dBW. Following the GPS standard documentation, the minimum level of the GPS L1 C/A signal that reaches the earth's surface must not fall below -160dBW (-130dBm). To maintain this, the transmitter power of the GPS L1 C/A is approximately 25W. C/No coefficient depends on the specificity of receiver's circuits, correlator etc. but usually this is around 40dB/Hz. This information is usually accessible for the user on the receiver's screen, however, this requires special attention, and it is difficult to expect, for example, an officer of the watch to devote all his attention only to these issues. In this context, it should be mentioned that the IMO resolution[1] of 2017 requires the receiver should raise an alarm in case any errors are detected. This is done by internal mechanism for analysis of standard structure of the received signal, analysis of the C/No ratio, by different filters etc. However, information about incorrect operation of the receiver still means that it cannot be used. Since such a receiver on a modern ship is part of a certain information network, it involves additional complications: it limits the operation of other systems, e.g. ECDIS, AIS, Satellite Communication, etc.

Detecting the spoofing with the receiver is much more complex. This is easy when such interference causes a radical change in the data at the receiver output: a sudden and important changes in the ship's position or heading or speed. There is a famous example when, approaching the port of Novorossiysk, 20 ships reported that, according to GPS data, they were at the distant Galendzhik airport [3, 9]. If such falsifications are minor, all that remains is to compare permanently the results of GNSS and another system. However, let us remember that in fact there are no exists such systems. Only special ships are equipped with inertial systems, and this solution is used on warships or surveying vessels, not on standard merchant ships. Anyway, some symptoms of suspected GNSS spoofing include incoherence in navigation position, abnormal differences between speed over the ground and speed through the water, time differences etc. may be recognized.

3. COMMONNESS OF THE THREAT

According to many publications [2, 6, 10, 14, 16], if talking about jamming and spoofing two different groups of transmitters should be considered. There are non-professional devices (so called Personal Protection

[1] MSC.1/Circ.1575, Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing to the Performance standards for multi-system shipborne radio navigation receivers (IMO, 2017).

Devices - PPD) and professional (military) devices. The first one is very common, cheap and usually low power and mostly occur on the land, on roads and in the cities. However, it can be used by personal on the board! In contrary, professional is usually very powerful, often are installed on trucks, but can be installed on board of moving warships or helicopters or at the buildings.

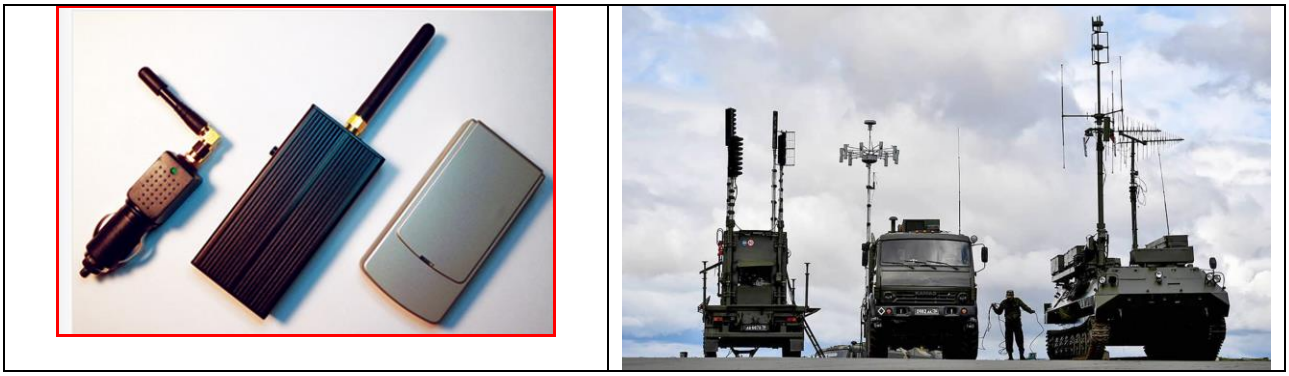

Fig. 3. Examples of jammers/spoofers (left – not professional [16], right – militaries [3, 17]).

PPD's ranges are small, but these cases most often concern highly urbanized areas, including highways, and their large number sometimes causes great complications. Fortunately, this very rarely concerns ships. In this context specific is the case of so called "white van" in USA. In 2013, the Federal Communications Commission, after two years' investigation, punished a person with thousands of dollars for using a device intended to block the fleet management tracking system on his company vehicle. With simple $30 device, he unconsciously but periodically blocked Newark airport, one of the biggest in USA [9].

An important thing to note is that the range of jammers is strongly correlated with its power. A small jammer power is usually not more than 1W (mainly some mW) and range should be measured in meters. The huge jammers used by Russian in Ukraine, for example, are usually around 1kW and about the size of a truck, so its range is in hundreds of kilometers. This can be assessed based on the diagram shown in Fig. 4.

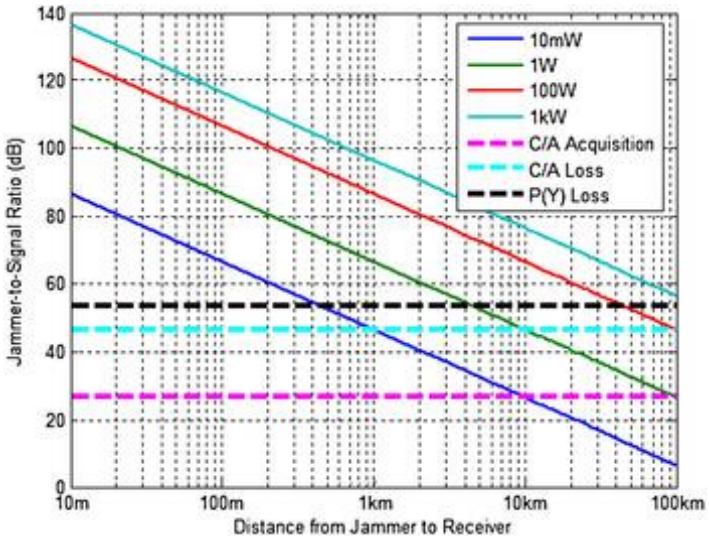

Figure 4. Average jammer range as a function of emitted power [14].

Impact of different sources of electromagnetic waves on different receivers is different and depends not only on emitted power. The receiver's resistance to interference signals depends on its synchronization status, but there is always a threshold beyond which the jamming signal will be successful in causing the receiver to lose the satellite signal. To achieve this, the jammer must emit a signal that reaches the receiver's antenna with

greater power than the receiver's threshold. However, it also depends on the bandwidth of the interfering signal and its encoding method. There are known jammers that emit only a sine wave covering the entire L1 band. But also, those that emit a narrowband signal sweeping the GNSS band. More advanced jammers additionally emit coded signals like GNSS. In paper of [Bhuiyan et al.] authors discuss some recorded interference signatures, and their use in standardized test procedures of two main group of receivers: mass-market and professional grade. The result analysis in terms of well-defined receiver key performance indicators showed that performance of both receiver categories was degraded by the selected interference threats, although there was considerable difference in degree and nature of their impact.

As already said, jammer users can be divided into two groups. The first are PPD users who want to avoid supervision. This especially applies to company car drivers and usually occurs in densely populated areas and on busy roads. On the other hand, strong jammers are used by various government services and armed forces to protect people, especially large numbers of people, mass events, military units or regions. This is a form of electronic warfare against weapons controlled via GNSS, and sometimes they are used by terrorists. The areas where these disruptions occur are very specific and usually appear in areas where there are military or terrorist threats. Current information on this subject is available on the Internet. Examples of jamming recorded on commercial aircraft over the Baltic Sea are given in Fig. 5a, and numbers of spoofing cases - in Fig. 5b. When analyzing these charts, it should be borne in mind that they are created based on data from commercial aircraft, so they do not provide data from areas over which such aircraft do not fly. The red color on the left figure present intensive jamming, when green - lack of this. Such observations are very dynamic and constantly changing, but it is possible to indicate areas where they occur more often. There is a belief that long-range disruptions are generated from land, but there are speculations that some Russian ships also generate them, especially at night.

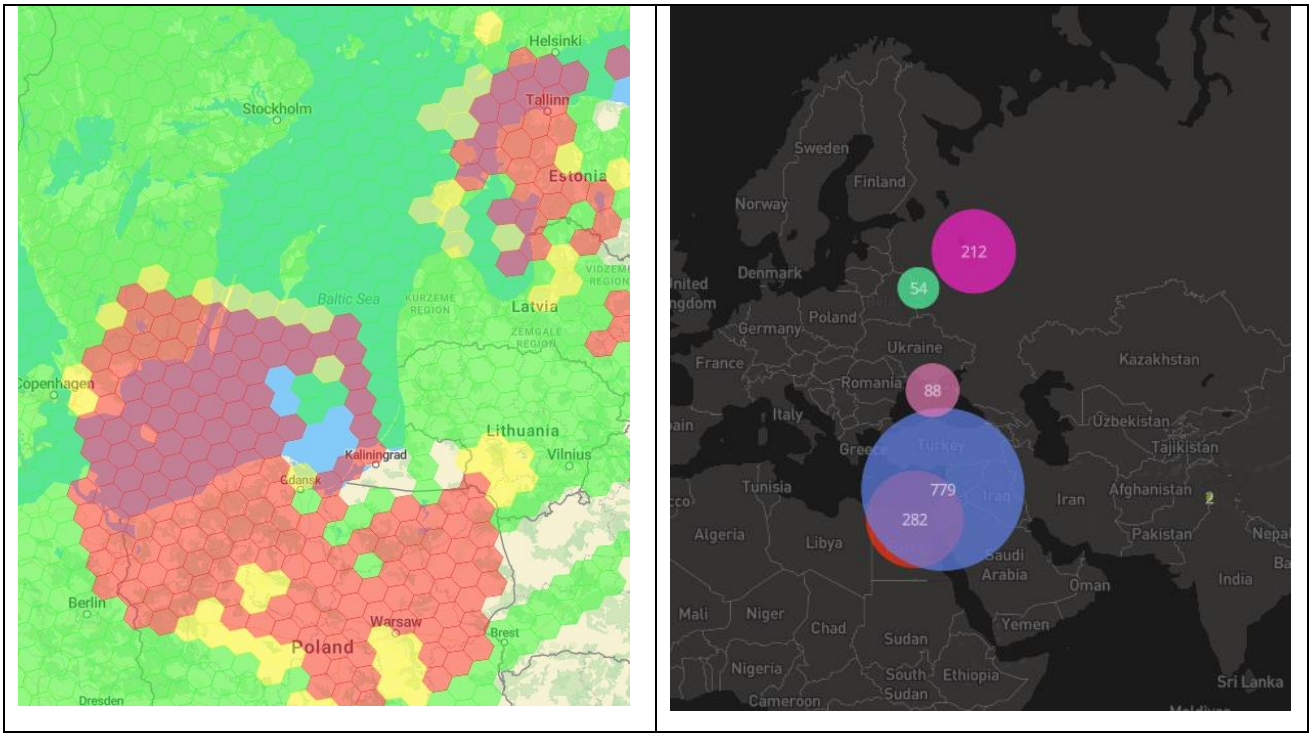

Figure 5. Occurrence of jamming over the Baltic Sea on 23 March 2024 (left, from [12]) and the number of registered spoofing cases on 16 April 2024 (right, from [13]).

4. JAMMING MITIGATION ON THE SURFACE SHIP

When discussing measures to reduce the impact of jamming, the following facts should be considered:

- The 1.5GHz radio wave propagates in straight lines,
- We assume that there is only one jamming source nearby,
- Jammer is located on land.

If so, the curvature of the Earth must be considered, and this means, that regardless of the power of such a transmitter, its range depends on the hight of the transmitting and receiving antennas. The great ranges shown in Fig. 5a result from the great power of the jamming device, which is most likely located in the Królewiec (Königsberg) region, but also from the fact that planes fly at altitudes of several kilometers. The GNSS antenna on the ship is placed at a height of several, maybe a dozen or so meters, and even if the transmitting antenna is placed at a height of about 60 m above the sea, such a jammer should not be an obstacle at 25 Nm.

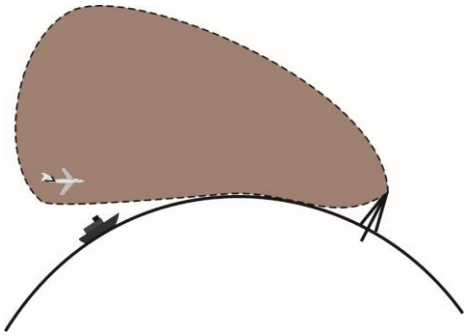

Figure 6. The influence of the earth's curvature on the jammer's range.

In this context, it should be emphasized that it is preferable to place the antenna lower, if possible. This is contrary to the common practice of installing receiving antennas on masts. In some situations, a low-installed antenna may be obscured by the ship's infrastructure but considering the number of available satellites (usually over 10), this does not pose a significant threat. The experience of operating GNSS in difficult conditions, e.g. in cities, shows that even blocking several satellites does not significantly reduce the accuracy. Paradoxically, there are known cases where a low-placed antenna was covered towards the jammer, thus preventing interference.

However, only a special antenna can be a solid way to reduce jamming. Two types of antennas with appropriately shaped receiving beams are suitable for this purpose. A typical GNSS receiving antenna has a beam that allows it to receive signals from any direction in the upper hemisphere. However, this does not mean that the antenna pattern is hemispherical. If this were the case, the receiver in the plane would not receive interference from the Earth's surface. This shape is in fact more complicated, it allows reception even at a negative angle to the horizon and has the so-called side wing. The latest anti-jamming antennas have characteristics that significantly reduce low sectors. An example of a typical and modernized beam is shown in Fig. 7. The main difference is a significant limitation in the reception of signals from low elevation angles.

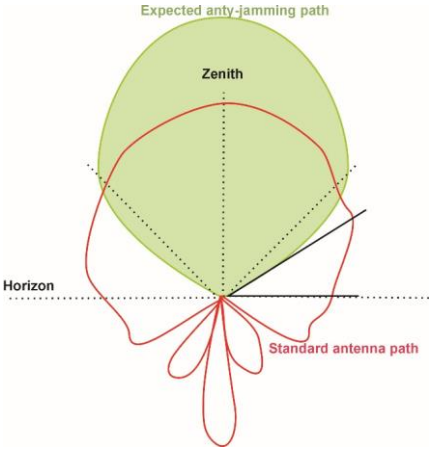

Figure 7. Scheme of standard GNSS antenna path and anti-jamming path.

Shaped beam antennas (Controlled Reception Beam Antenna – CRPA) are considered more perfect. These are antenna arrays that, by supplementing them with appropriate electronic systems, allow for determining the existence of interference, assessing the direction from which it is coming and zeroing a specific section around this azimuth. CRPA antennas are available in many models, that use from 2 to 9 elementary antennas, with the rule that the number of zeroed sectors is one less, than numbers of antennas elements.

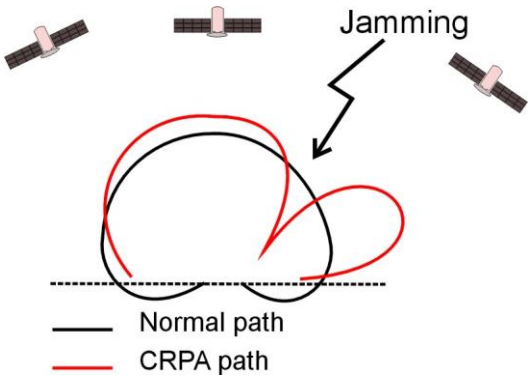

Figure 8. Comparison of the normal antenna path and CRPA's.

These solutions confirm their effectiveness. Indeed, CRPA antennas ensure that the receiver operates in code mode under interference conditions, but sometimes the HDOP coefficient deteriorates slightly, which should not be surprising since the number of received satellites may be reduced. The presence of jamming often leads to a reduction in the C/No ratio, even to around 20, but in principle the coordinate values C/No do not change. Importantly, such antennas work well even when the source of interference is relatively close. Of course, only if the power of the generated interference does not exceed a certain level. If the jammer is located at long distances, the CRPA antenna also works well, because the essence is the relationship between the power level of signals coming from space and the level of signals coming from the jammer.

An antenna with anti-jamming characteristics, as in Fig. 7, generally works well on a ship in the presence of interference coming from low elevation angles, i.e. from distant jammers. The rule is that if the interference comes from a visible object, i.e. at no more than a dozen or so nautical miles, such an antenna cannot be a remedy for jamming. This is a conclusion like the one mentioned earlier - a lower antenna limits the

possibility of receiving signals from low transmitters since the "range of visibility" decreases as the receiving antenna is lowered.

It should be emphasized that the presented experiments, both with respect to CRPA antennas and those with a specially shaped receiving beam, concern code methods at the L1 frequency. The author has not yet been able to use CRPA antennas for phased measurement techniques. More specifically, CRPA antennas work with phased receivers, for example in RTK mode, but only in the absence of jamming. In the case of jamming, measurements were not possible, so the use of such antennas in the RTK mode does not work.

CONCLUSIONS

The phenomenon of jamming and spoofing is common not only on land, but also at sea. The specificity of wave propagation that is used in GNSS systems means that there is a real threat in coastal waters, rather within a range of several nautical miles from the shore. However, it is in these waters that inaccurate positioning or lack thereof poses a major safety hazard. These statements do not prove that this threat exists continuously or that it cannot occur in open waters. Therefore, the officer of the watch must be prepared for difficulties of this nature and the need to use more traditional methods of navigation. It should be noted that most often it will be possible to use radar and well-known radar navigation techniques. This possibility should also be the basis for verifying whether the GNSS receiver is not subject to spoofing. Compass and speed meter readings should also be compared with the GNSS receiver's readings, as significant differences in readings may be a symptom of incorrect operation of the satellite system.

However, these are not methods of mitigating the impact of disruptions, especially intentional disruptions, on the operation of these systems. Today, large teams are working on this threat, both on the part of service providers and among producers of receiving devices and this is certainly a perspective of several years. Currently, there are possibilities to improve the situation by replacing the receiving antennas with CRPA or other anti-jamming antennas. It is also a wise move to install the antenna currently in use lower down, which may limit the range of land-based jammers.

It should be noted, however, that these proposals refer to GNSS code variants and do not work or work poorly in relation to phase techniques.

REFERENCES

1. Bhuiyan M. Z. H., Ferrara N. G., Hashemi A., Thombre S., Pattinson M., Dumville M. Impact Analysis of Standardized GNSS Receiver Testing Against Real-World Interferences Detected at Live Monitoring Sites. Sensors **2019**, 19, 1276; doi:10.3390/s19061276.
2. Cameron A. Spoofer and Detector: Battle of the Titans at Sea. GPS World August 5, 2014.
3. C4ADS Above Us Only Stars. Exposing GPS Spoofing in Russia and Syria. Austin 2019. Available at www.c4ads.org (14.03.2023)
4. Falen, G. L. Analysis and Simulation of Narrowband GPS Jamming Using Digital Excision Temporal Filtering. (Master′s thesis) Air University, Air Force Institute of Technology, Ohio, 1994.
5. Felski A. Methods of Improving the Jamming Resistance of GNSS Receiver. Annual of Navigation 23/2016.
6. Felski A., Gortad M. The Significance of an Antenna for Jamming Resistance of a GPS Receiver. Scientific Journal of Polish Naval Academy no. 4 (207) 2016. Doi: 10.5604/0860889X.1229749.

7. *Global Navigation Space Systems: reliance and vulnerabilities*. The Royal Academy of Engineering, London 2011. Available at: http://www.raeng.org.uk/gnss (12.09.2014)
8. Goward D. Expert Opinion: Spoofing attack reveals GPS vulnerability. GPS World, 2017. Accessible at: http://gpsworld.com/expert-opinion-spoofing-attackreveals-gps-vulnerability/ (10.01.2018).
9. Goward D. GPS disrupted for maritime in Mediterranean, Red Sea. GPS World, 2018. Accessible at: https://www.gpsworld.com/gps-disrupted-for-maritimein-mediterranean-red-sea/ (24.01.2019).
10. Grant A. Wiliams P., Basker S. GPS Jamming and its impact on the maritime safety. Port Technology International (2010, 46, 39-41).
11. https://gpsjam.org (access: 23.03.2024)
12. https://spoofing.skai-data-services.com (accesses at 24.05.2024)
13. Jones M. The Civilian Battlefield. Protecting GNSS Receiver from Interference and Jamming. Inside GNSS March/April 2011. Accessible at: https://www.insidegnss/auto/marapr11-Jones.pdf (accessed at 12.08.2024).
14. Kaplan E., Hegarty C. Understanding GPS/GNSS: Principles and Applications. 3rd Edition, Artech House Publisher, London 2017.
15. Mitch R. H., Dougherty R. C., Psiaki M. L., Powell S. P., O'Hanlon B. W., Bhatti J. A., Humphreys T. E. Signal Characteristics of Civil GPS Jammmers. Accessible at: Innovation: Know Your Enemy - GPS World : GPS World (access 13.06.2014).
16. Operacja informacyjna sił tzw. "DRL" – tuszowanie obecności rosyjskich systemów WRE na Donbasie. Accessible at: Operacja informacyjna sił tzw. „DRL" – tuszowanie obecności rosyjskich systemów WRE na Donbasie (informnapalm.org) (access 20.12.2019).
17. Psiaki M. L., Humphreys T. H., Stauffer B. Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies. IEEE Spectrum, vol. 53, Issue 8, 2016.
18. Scott L., Spoofs, Proofs & Jamming. Inside GNSS, September/October 2012, pp. 42–53.