ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY

2016 (LVII) 4 (207)

DOI: 10.5604/0860889X.1229749

Andrzej Felski*, Marta Gortad**

THE SIGNIFICANCE OF AN ANTENNA FOR JAMMING RESISTANCE OF A GPS RECEIVER

ABSTRACT

At present jamming is considered one of the main threats to a GPS receiver's user, both in dynamic and stationary conditions, and especially regarding telecommunication synchronization. Threats stemming from the use of cheap jammers, more and more commonly referred to as Personal Protecting Devices, available on the Internet, are especially dangerous. Despite the formal ban on using them, there is evidence that they are in common use. Therefore the problem which has hitherto been considered marginal needs to be urgently investigated. Reports dealing with investigations on jamming focus mostly on analyses of effects of various jammers on receivers. This article presents part of the results of experiments focused on the effects and it shows that the effects of jamming when the same device is used depend on both the receiver and the antenna it employs.

Key words:
jamming, GPS, Personal Protecting Device.

INTRODUCTION

The common use of GPS in all sectors of everyday life entails the confidence of users in the reliability of the results. Most often position accuracy is taken into consideration but stability of time standard, which the GPS is more and more often considered to be, becomes equally important, which plays a special role in computer networks and cellular communication. Until recently there has been a conviction that as a GPS wide-beam signal is by its nature weaker than a natural noise level

* Polish Naval Academy, Institute of Navigation and Hydrography, Śmidowicza 69 Str., 81-127 Gdynia, Poland; e-mail: a.felski@amw.gdynia.pl

** Polish Navy, 3rd Flotilla of Ships, Rondo Bitwy pod Oliwą Str., 81-103 Gdynia, Poland; e-mail: marta.gortad@gmail.com

and in addition it being randomly coded, it is not affected by jamming as opposed to older radio-communication technologies. Absence of signals was considered possible only as a result of occultation of satellites or accidental interference or reverberations of signals. However such cases could have happened only in special situations, mostly in an urban area. At present, we know that these signals, just like all radio signals, can also be affected by other kinds of interference, both random and intentional.

For land users this is interpreted as a risk of absence of data relating to the position in services based on user localization (so called GNSS-based services) as a result of occurrence in close proximity of interference sources having low power, usually used by drivers to jam the monitoring system of a car fleet which is more and more often employed by many firms. These devices have already earned their own name (Personal Protecting Devices), as they would protect drivers against excessive supervision by superiors through generating a phenomenon of absence of information. It appears, however, that these devices, although they theoretically should have the capability to jam GPS signals inside the car, they usually have longer ranges and jam receivers within the range of a few, sometimes a few dozen meters [4, 7, 8, 13].

Reports on projects concerned with investigating the nature of jamming appear in several publications. For example [10] make attempts to define an indicator which can be used to assess the fact of jamming occurrence. Similarly [14] consider coefficients used to unequivocally detect interference occurrence. The issue is not new. It is [11] that have suggested establishing a network of inexpensive receivers in order to record jamming occurrences on motorways. A similar system has been proposed by [9] and [3]. Then [1] have presented employment of automatic strengthening of signals from particular satellites as one of the first solutions to limiting the effect of jamming, in contrast to the earlier offered solution based on a receiver employing multi-correlation [2].

This article presents the results of comparative studies on the effect of such devices on the same receiver working with C/A signal but using different antennas.

THREATS POSED BY JAMMING AND JAMMING DEVICES

First reports on the possibilities of jamming a GPS signal, date from the 1990s [6] but wider interest in this issue has appeared in the 21st century. An example is a report by the US Trade Department published in 2001, which described the potential possibilities of interference by a GPS signal with wideband radio-communication

systems, while a decade newer report by the Royal Academy of Engineering [7] raises not only the problem of intentional interference of signals with the signals from other systems, but it also raises the problem of intentional use of jamming devices. More and more news has appeared in media about the intentional jamming of a signal. In May, 2012 especially lively discussed was the information published by the government of South Korea concerned with electronic jamming signals transmitted from North Korea which affected radio communication and use of GPS by passenger planes in the area of Seoul.

In the years 2011–2012 the government of Great Britain financed project SENTINEL. In this project 20 sensors were installed to detect incidents of jamming GPS signals on public roads [7, 15]. At this time only one of the sensors recorded more than 60 of such events. These investigations proved the hypothesis made by the researchers involved in the project that interference caused by small and cheap, generally-available jamming devices is omnipresent and poses an obvious hazard. There have been press reports of cases of punishing users of such devices in Great Britain, USA and Germany, especially car thieves who more and more often use these devices in order to prevent finding the location of stolen cars equipped with appliances for monitoring, based on satellite technologies. A special aspect of jamming is raised by authors of the report [13] pointing out the possibility of using these devices as a way of showing 'civil disobedience' against electronic toll collection systems which employ a GPS-based vehicle tracking system.

It is also worth bearing in mind that a common user of a GPS system usually does not have any idea of how the system works. Therefore it is even more doubtful if he/she can notice the effects of interference. These, among others, result from the fact that many receivers in common use do not signal the presence of jamming or interference. However, it is also worth noting that there are currently available receivers signaling unfavorable signal to noise ratio, which is one of the features suggesting the presence of jamming.

Jamming any radio device means, in fact, generating a signal in the same frequency band, but having such a strength that in the place of the receiving device the noise strength exceeds the effective signal strength. As a result the reception of the effective signal, i.e. separating it from the noise background becomes impossible. Such solutions have been known and used since WWII, e.g. in political or military activities for jamming radio-stations or radar. As for the GPS an average effective signal level is approximately 30 dB weaker than noises, and the acceptable effective signal level can be even up to 64dBw. This means that a GPS receiver works when the signal is weaker than the ambient noises and for the receiver it is a natural condition. However,

it also means that if the noise level is raised, the acceptable border will be crossed, which means that the receiver will lose its capability to track satellites, i.e. the capability to fix positions (fig. 1).

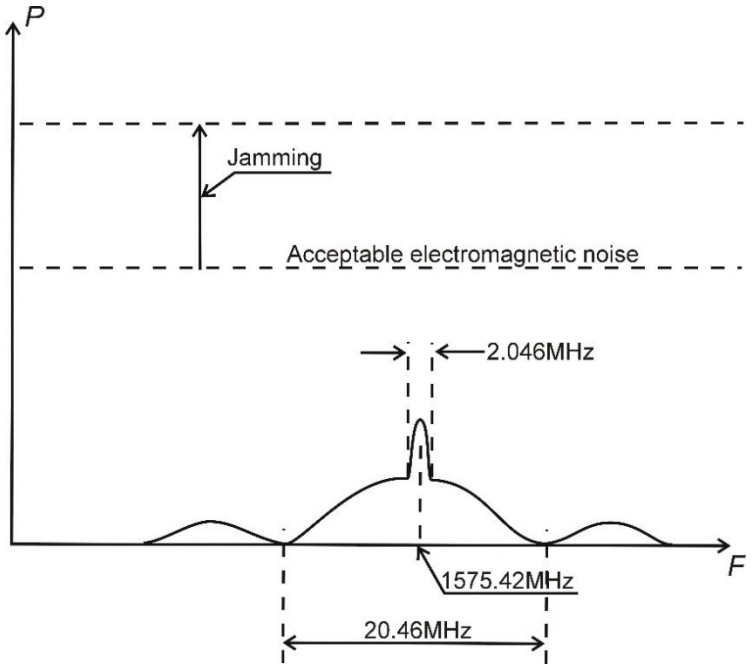

Fig. 1. The effect of jamming on the GPS system [own work]

In the literature there can be found reports that jamming devices having the power of a few dozen milliwatts [mW] feature the range even up to 50 m, and a device having power of 1 W can jam a GPS device within the radius of several kilometers [5, 10, 12]. It must also be underscored that the general perception is that a GPS receiver in the presence of jamming indicates that it has stopped working or is not jammed if these signals do not have sufficient power. In reality it is not a black and white situation. Very often some satellites are eliminated (the receiver discontinues tracking a signal) and some continue to be tracked. It, first of all, depends on such factors as the altitude of a satellite over the horizon and signal strength, as well as many others. As a result, very often the accuracy of fixes decreases although the device does not necessarily lose its capability to work.

In the investigations referred to in this article two devices capable of jamming the whole band of the GPS system (L1, L2, L3) were used. The appliance made by Spy Electronics LTD is a transmitter with an antenna and a battery as well as

a charger that can be plugged into a car cigarette lighter socket. Time of performance specified by the manufacturer is 3 hours, nominal jamming range is up to 15 m, and dimensions: 100 x 45 x 18 mm.

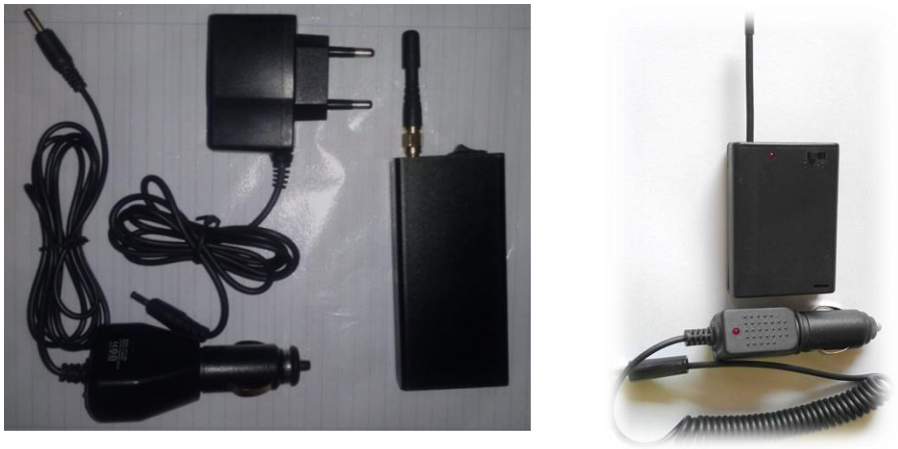

Fig. 2. The jamming device made by Spy Electronics LTD (left) and GX-40B made by TTS (right) [authors' photos]

The other device — GX-40B made by TTS is an appliance of a medium range although it looks similar. Its parameters are: 1 hour of work between charges, declared jamming range — 40 m, and dimensions — 67 x 47 x 16 mm.

THE RESULTS OF THE EXPERIMENTS

The experiments referred to were aimed at acquiring a picture of the effect of an antenna on jamming and were carried out in the closed car park of the Naval Academy using a Hemisphere R110 receiver and two versions of active antennas: A30 (Hemisphere) and MGL-3 (CSI WIRELESS). In the course of the experiment other receivers were also used but those experiments are not the subject of this article.

The MGL-3 antenna is an antenna developed to receive the L1 band (1.575 GHz) having a narrow frequency range of 3MHz and GPS LNA Gain of approx. 27dB. The A-30 antenna belongs to the range of products from the Hemisphere Company, is immune to multipath signaling. It provides reception of both GPS and SBAS signals and, in addition, it has a toroidal antenna providing reception of signals from a reference DGPS station in the band of 300 kHz. The received frequency band width is 20 MHz and GPS LNA Gain is 34 dB.

Fig. 3a. Antenna A-30
[http://www.canalgeomatics.com (access 10.04.2016)]

Fig. 3b. Antenna MGL-3
[http://csi-wireless.com (access 10.04.2016)]

The aim of the investigations was to draw conclusions concerning the performance of various configurations of receiving sets in the area of operation of the same jamming systems. Both antennas are active antennas but they differ substantially in frequency ranges. It appears that this had a significant effect on the different performance of the same receiver.

Fig. 4. The way the antennas were fitted [authors' photo]

The receivers were installed on the roof of a car which provided almost identical conditions for all the receivers, and at the same time made it possible to move.

In the course of the investigations the car moved about the car park getting close to the device and moving away from it. In this time two messages were recorded: $GPGGA and $GPGSV. These two messages contain, apart from the position and time, such data as state of the system, number of visible satellites or value of the DOP ratio. The same measurement sessions were carried out for both jamming devices.

The area of investigations can be classified as an open area. There was a one--storey residential building and a few trees in the vicinity, but they were at least a several meters from the receiver. The jammers were placed on the building at a height of approx. 15 m in such a way that the elevation angle in relation to the antennas was approx. 20–40°.

Fig. 5. The place of experiments [Google Earth]

The signal to noise ratio (SNR), geometric DOP ratio, and the system state (0–1) which is transmitted in $GPGGA message were used as measures for the GPS receivers' immunity to jamming.

THE RESULTS OF THE EXPERIMENTS

The fundamental information in the context of jamming is the state of the system. This is one of the pieces of information contained in the message $GPGGA and

means: 1 — works, 0 — does not work. The results of one of the records (GX-40B) are presented in figures 6 and 7, in which the measurements are referred to the time expressed in seconds. It is surprising that the identical receivers installed, in fact, at the same place showed different responses to the same interference due to the fact that two different antennas were employed. The continuous lines mark the work status of the device and the dashed line marks the geometric ratio.

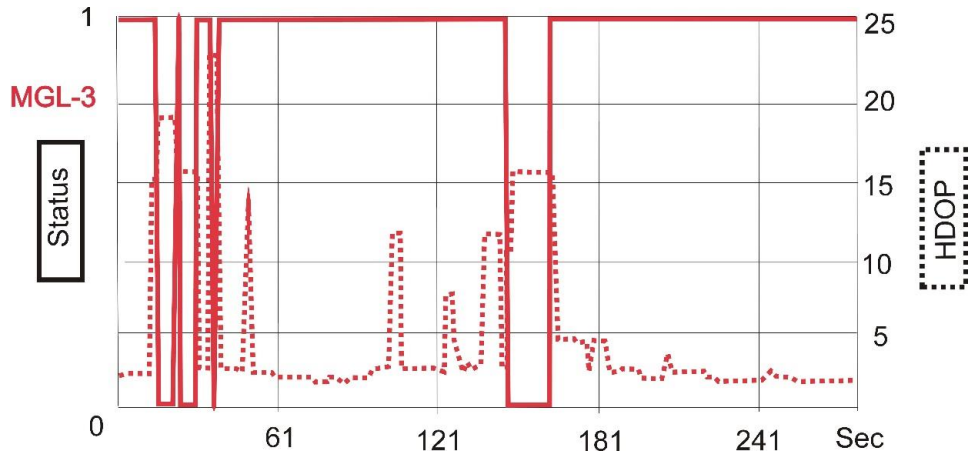

Fig. 6. The state of the system during the measurement for configuration R110/MGL-3 (jammer GX-40B) [own work]

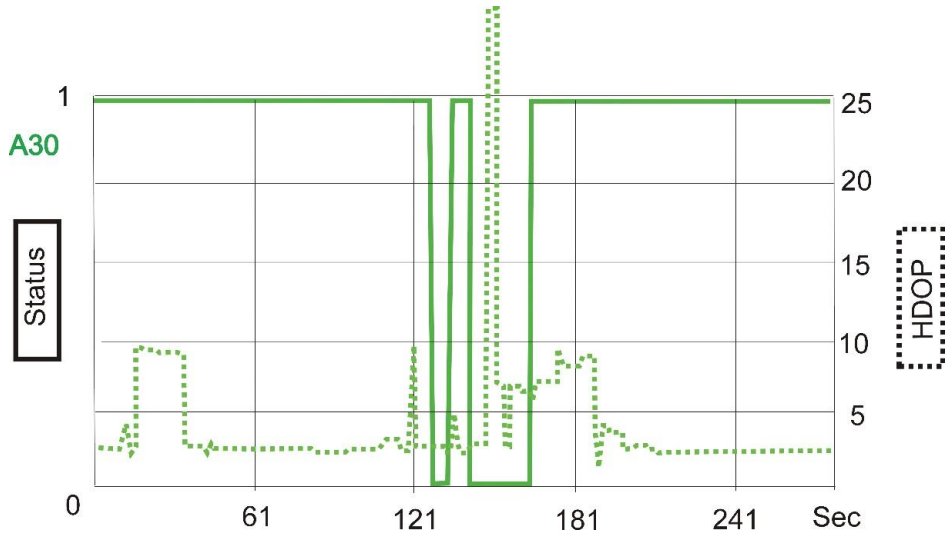

Fig. 7. The state of the system during the measurement for configuration R110/A-30 (jammer GX-40B) [own work]

The work of the R110 receiver with the investigated antennas is at the same time a spectacular example of how different are the results of jamming the same receiver with the same jamming set. Figure 8 shows completely different moment of absence of receiver work depending on the antenna it employs.

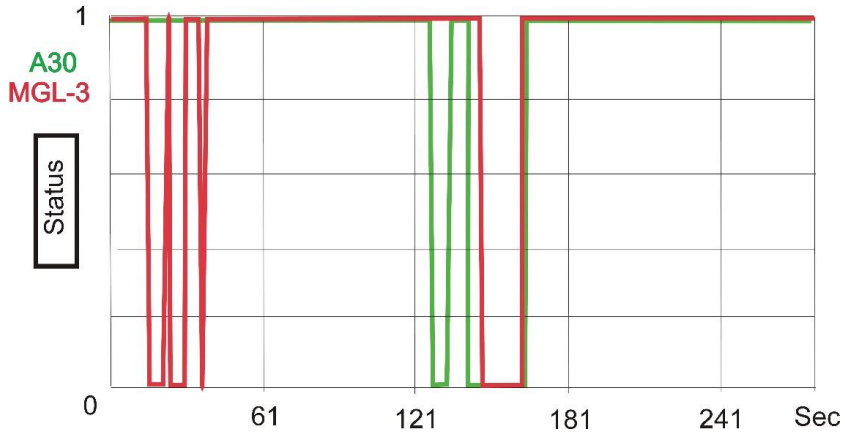

Fig. 8. The state of the system in relation to time, depending on the employed antenna (jammer GX-40B) [own work]

When investigating the signal spectrum for both jammers it was found out that for the GX-40B it is wider and embraces the whole band from 1.5 to 1.8 GHz, but the signal strength is lower and does not exceed approx. 68 dBm. For the Spy Electronics the spectrum is more concentrated (1.45–1.65 GHz), and the maximum noise value is approx. 68 dBm. The noticeable differences in the performance of the two receivers probably as a result of their construction being immune to the A-30 antenna multipath, which despite the wider frequency range performed better than the MGL-3 antenna characterized by the narrower frequency range. In the case of jamming with the latter devices such spectacular differences were not recorded, however, despite the type identity of the receivers differences can be noticed. This can result from the radically lower operating range of the jammer.

The state of the receiver work, i.e. fixing or not fixing a position does not result from the number of satellites tracked. It appears that the distance of a receiver from a source of jamming is not the only measure of this process as the same jamming signal level causes various effects in relation to different satellites. At the same time the signal to noise ratio for different satellites can be different. It is directly connected with the altitude of a satellite over the horizon. An example of the SNA value (Signal-to-Noise Ratio) for some satellites is presented in figure 10.

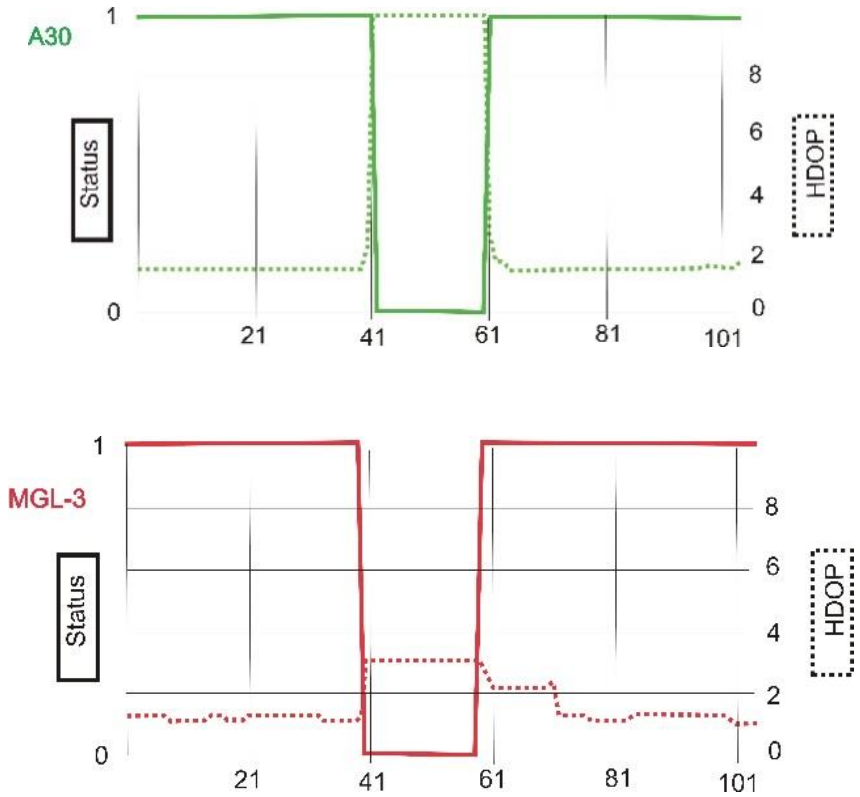

Fig. 9. The state of the system and the value of the HDOP ratio during the measurement for configuration R110/A-30 and R110/MGL-3 (jammer Spy Electronic) [own work]

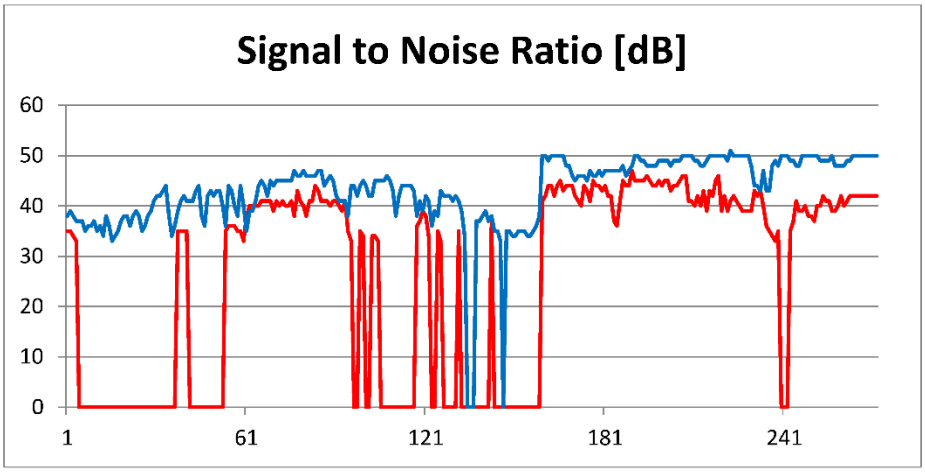

Fig. 10. Relation of SNR for two satellites in configuration R110/MGL-3 [own work]

CONCLUSIONS

In the course of the experiments with the GX-40B jammer (weaker) referred to here all the receivers were used for tracking the same, all available satellites. During the work of the stronger Spy Electronics LTD jammer they partly made use, of tracking other satellites (e.g. during one of the experiments they tracked the same 7 satellites, but in addition one of them tracked satellites PRN 5 and PRN 7 while the other tracked satellites numbered PRN 3 and 5.

Both jammers caused blocking the receivers into a state, however, this occurred in different ranges from a jammer and usually these moments did not overlap. This means that the effect of jamming was different depending on the antenna type. This follows from making use of different satellites for tracking. It should be noted that jamming is not a black and white process, and therefore the action of the same jamming system is different for different receiving sets, and this means a varied range of the same jamming system as well as varied capability to eliminate particular satellites. This results in a different geometric ratio for different receiving sets, and in consequence in different position fixing accuracies.

REFERENCES

[1] Bastide F., Akos D., Macabiau C., Roturier B., *Automatic Gain Control (AGC) as an Interference Assesment Tool*, 'ION GPS/GNSS', 2003, pp. 2042–2053.

[2] Bastide F., Chartre E., Macabiau C., *GPS Interference Detection and Identification Using Multicorrelator Receivers*, 'ION GPS', 2001, pp. 872–881.

[3] Calcagno R., Fazio S., Savasta S., Dovis F., *An interference detection algorithm for COTS GNSS receivers*, 'NAVITEC', 2010, Workshop, Noordvijk.

[4] Dixon Ch., Hill S., Ucar A., Ameer G., Greaves M., Cruddace P., *GNSS threat quantification in the United Kingdom in 2015*, 'Coordinates', 2016, Vol. XII, Issue 01.

[5] *Extreme space weather: impacts on engineered systems and infrastructure*, Royal Acad. of Engineering, London 2013, [online], http://www.raeng.org.uk [access 12.09.2014].

[6] 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.

[7] *Global Navigation Space Systems: reliance and vulnerabilities*, The Royal Academy of Engineering, London 2011, [online], http://www.raeng.org.uk/gnss [access 12.03.2016].

[8] *Good Timing. Fighting GPS Interference on the London Skyline*, 'Velocity — Novatel's Annual Journal of GNSS Technology Solutions and Innovation', 2015.

[9] Isoz O., Akos D., *Development of a deployable low cost interference detection and localization system for the GNSS L1/E1 band*, 'NAVITEC', 2010, Workshop, Noordvijk.

[10] Kuusniemi H., Bhuiyan M. Z. H., Kroger T., *Signal Quality Indicators and Reliability Testing for Spoof-Resistant GNSS Receiver*, 'European Journal of Navigation', 2013, Vol. 11, No. 2.

[11] Lindstrom J., Akos D., Isoz O., Junered M., GNSS *Interference Detection and Localization using a Network of Low Cost Front-End Modules*, 'ION GNSS', Sep. 2007, pp. 1165–1172.

[12] Scott L., *Spoofs, Proofs & Jamming*, 'Inside GNSS', September/October 2012, pp. 42–53.

[13] Sheridan K., Whotworth T., Gabelli G., Casile R., Guidotti A., Corazza G. E., Hoelper C., Fremont G., *DETECTOR: Applications and Threats Analysis, 2012*, [online], http://www.aic-aachen.org/detector/downloads/DETECTOR_D21.pdf [access 20.03.2016].

[14] Sheridan K., Yeqiu Ying Y., Whitworth T., *Radio Frequency Interference Detection to Support the Use of GNSS in ITS*, 9th ITS European Congress, Dublin 2013.

[15] *Space Weather Full Report*, Royal Academy of Engineering, London 2013, [online], http://www.raeng.org.uk/publications [access 15.07.2014].

[16] http://csi-wireless.com [access 10.04.2016].

[17] http://www.canalgeomatics.com [access 10.04.2016].

ZNACZENIE ANTENY DLA ODPORNOŚCI ODBIORNIKA GPS NA ZAGŁUSZANIE

STRESZCZENIE

Zagłuszanie (jamming) jest obecnie uważane za jedno z podstawowych zagrożeń dla użytkowania systemu GPS, zarówno w warunkach dynamicznych, jak i stacjonarnych, zwłaszcza synchronizacji czasu dla celów telekomunikacyjnych. Szczególnie istotne stają się zagrożenia wynikające ze stosowania tanich zagłuszaczy dostępnych za pośrednictwem Internetu, nazywanych coraz powszechniej Personal Protecting Devices. Pomimo formalnego zakazu ich użytkowania dowiedzione jest powszechne stosowanie tego typu urządzeń. W tej sytuacji zgłębianie problemu, do niedawna traktowanego jako nieistotny, staje się pilne. W doniesieniach odnoszących się do badania wpływu jammingu dominują opisy nakierowane na analizę wpływu różnych jammerów na odbiorniki. W niniejszym artykule przedstawiono część wyników eksperymentów w zakresie wpływu zagłuszania na odbiornik pracujący z różnymi antenami i wykazano, iż efekty zagłuszania tym samym urządzeniem zależą zarówno od odbiornika, jak i współpracującej z nim anteny.

Słowa kluczowe:

zagłuszanie, GPS, Personal Protecting Device.