DE GRUYTER OPEN

DOI: 10.1515/aon-2016-0013

ANDRZEJ FELSKI
Polish Naval Academy, Gdynia, Poland

METHODS OF IMPROVING THE JAMMING RESISTANCE OF GNSS RECEIVER

ABSTRACT

Jamming of GNSS signals can be both a consequence of accidental activities and an intentional act. This issue is lately discussed as an essential threat for the use of satellite navigation systems. This 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. Until recently even specialists have shared the conviction that the broadband GPS signal is not a subject of disturbances in contrast to older wireless communication techniques because its power level is below natural level of noises and in addition it is randomly coded. But nowadays jammers are very often successfully applied, which is confirmed in many reports. The average user has not the suitable knowledge about the specificity of the jamming and has no technical possibilities of the detection of jammer signals. Receivers, which can indicate the presence of perturbative signals, became accessible a few months ago only. Presently accessible jamming monitors can also determine the direction of interferer signal transmission. There are also specially designed receivers with anti-jamming mechanism, which are, however, not commonly accessible. The possible way of countermeasure the jamming in the GNSS receiver are discussed in this paper.

Keywords:
jamming, jamming monitoring, GNSS vulnerability.

INTRODUCTION

GNSS signals received on the Earth surface are very weak, so are very vulnerable to many disturbances. Complete list of possible sources of GNSS receiver

malfunctioning is presented in [http://gpsworld.com/make-it-real-developing-a-test-framework-for-pnt-systems-and-devices] by Guy Buesnel, John Pottle, Mark Holbrow and Paul Crampton. On this list we will find Multipath, which is especially important in urban area and atmosphere influence, in which solar activity and scintillation are the most important. Authors of course mention about the space segment errors, e.g. erroneous data and possible SV faults. In this context possible cyber-attacks appears but unintentional an intentional interferences, including jamming, are the nowadays the most important. Additionally we should have in our mind spoofing and meaconing, which are possible and known as a threat since many years, still more as a theoretical than practical threat. This is the reason of introducing the SAASM technology.

Only natural disturbances have been discussed for a long time as the important threat for GPS, but now it is clear, that the main threat for GNSS systems are any interferences, especially intentionally produced false signals. Jamming — a kind of this activity — is a form of powerful radio signal, intentionally generated to disturb GNSS service. Depending on power of the jammer, the size of an area where jamming may appear is from some meters to hundreds kilometers. This is illegal activity, however the presence of jammers in our everyday life, especially on roads, is confirmed by authors of many reports. 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 [Federal Aviation, 2011], but his jammer was so powerful, that it was disrupting WAAS signal around the airport. Another commonly known example of jamming is activity of North Korea's military forces against South Korea in region of Seoul and Inchon Airport. This events are only examples of the problem.

For long time we were convinced that the randomly coded, broadband GPS signal was not subject of disturbances in contrast to older wireless communication techniques. Nowadays we know that GNSS signals, similarly to all radio signals, can be a subject of all kinds of disturbing. Natural disturbance to the RF signal can be the reason, but mainly it is man-made, sometimes non-intentional but more and more often also intentional. First reports about the possibility of the disturbance of the signal GPS originate from the half of '90s [Falen, 1994]. In the report of the American Department of the Trade published in 2001 potential possibilities of the interference of the signal GPS with broadband wireless communication systems has been widely described but only reports of the Royal Academy of Engineering [Global Navigation, 2011], [Space Weather, 2013] not only touches

the problem of the interference of signals from other systems, but also raises the problem of the advisable usage of perturbative devices. Today devices for producing the jamming are easily accessible and such incidents are very common.

Whether we like 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 results, especially in the information about the position. Only the damage of satellite as a reason of the lack of signal and the reflections and interferences in urbanized areas were taken into account some years ago. Today it is clear that our world urgently wants immune and resilient PNT systems. Many GNSS applications, not only localization of the ship or airplane, depends on GNSS. Nowadays such applications as tracking of costly goods, pay-as-you-drive services, sport application, but even animals behavior monitoring are based on GNSS. This is not a only question about position or navigation, but many other critical infrastructures of our society would literally collapse in case of a GNSS failure. GPS is also used to provide accuracy, synchronized time, around the world. Without it, data systems and energy systems cannot work. In this context, the information, that Raytheon has awarded by DARPA with contract for early warning system detecting spoofing and cyber--attacks against US power grid infrastructure[1] is very eloquent.

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 in radii of several kms from jammer, it depending on the power of the jammer and type of antenna used. 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 as it was presented by author on ENC 2015 in Bordeaux[2]. Depending on the particular situation jammer can

[1] See: http://gpsworld.com/raytheon-darpa-developing-tech-to-protect-power-grid-against-cyber-attack/ [access 05.12.2016].

[2] A. Felski, A. Nowak, M. Gortad, Investigation over jamming in the aspect of the construction of the GNSS receiver, European Navigation Conference, Bordeaux 2015, [online], https://www.researchgate.net/profile/Andrzej_Felski/contributions [access 12.05.2015].

eliminate only part of potentially visible satellites, so receiver can present the position, however usually it will be degraded in accuracy. The reaction of different types of receivers is dissimilar, for example it depends on the height of satellites above the horizon. It causes that jamming of different space vessels is not the same. We can also observe correlation between jamming process and the construction of the antenna. Briefly the reactions of the same receivers with different antennas are different.

In this context we 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) [Scott, 2012]. There are jammers which cover not only the L1 band, but sometimes also mobile phones. Depending on the properties generated radio waves jammers can be classified in different ways. Rash [Rash, 1997] suggest to divide jammers into three categories:

- continuous wave, occupying less than 100 KHz bandwidth;
- narrowband jamming occupying more than 1 MHz of bandwidth but less than or equal to the entire 1.023 MHz bandwidth of C/A code;
- wideband jamming occupying the entire 10.23 MHz bandwidth about L1 or L2.

Different classification with four classes of jammers was proposed by [Mitch et al., 2011] or [Kraus, Bauernfeind and Eissfelle, 2011]:

- 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 TF 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).

In addition, Mitch and coauthors points three principal types of 'personal' jammers [Mitch et al., 2011]:

- the device with declared range of some meters connected to the car (the lighter socket) power supply;
- the next group has range more than ten meters equipped with the internal battery and external antenna;
- the third group consists of hidden instruments, for example in the casing of the cellular phone, with own power supply, but usually without the external antenna.

We cannot be in doubt that professionals have at their disposal devices which possess completely different properties. SCORPION™ and EQUINOX of Allen Vanguard can be presented as an example. SCORPION is a flexible and powerful jamming solution to support soldiers pedestrian patrol [http://www.allenvanguard.com/product/scorpion/]. A range of vehicle options can be supported with the EQUINOX jamming system [http://www.allenvanguard.com/product/equinox/]. 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. Similar products can be delivered by CAST, Chronos Technology, Novatel, Forsberg etc. As far as 'personal devices' usually possess little power measured in milliwatts, then professional devices generate powers even to 500 W.

SCORPION EQUINOX

Fig. 1. Examples of military jammers offered by Allen Vanguard [http://www.allenvanguard.com (access 02.08.2016)]

POSSIBILITIES OF JAMMING COUNERMEASURE

At the moment the standard GNSS receiver is not equipped with any tool for detecting the jamming, however some counter examples can be indicated. GMM-U5J receiver with build-up an Anti-Jamming Assessment Command Feedback mechanism can inform the 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 changes between

background noise and a jamming signal. Some producers offer very sophisticated receivers with very complicated segment-antenna and Beam-Forming Mechanism which can create null sections in antenna beam, so signals from some directions are not received.

The impact of jamming depends also on receiver design, antenna characteristics and spectrum of signal generated by jammer. In most cases the goal of use the jammer is to exclude GNSS services in a particular area and it seems be easy detectable. If so, dedicated service should be able to alert users and switch-on alternative service or system. Unfortunately at present suchlike counter jamming service does not work, as well the back-up PNT service does not exist. Even if it is possible, it can work only on small area. For such a reason it seems to be very essential to design a receiver which is resistant on jamming.

Accordingly the disturbance should be earlier detected. Nowadays some models of jamming detectors are accessible, however this is not a big market. Two examples of CHRONOS products are presented in the Figure 2. CTL3520 GPS Jammer Detector and Locator is a handheld, battery operated device designed to detect and quickly locate the presence of jamming signals from commercially available jammers, when CTL3510 GPS Jammer Detector is a low cost, handheld, battery operated device designed to detect the presence of GPS jamming. Both work in the L1 band.

Fig. 2. The Chronos CTL3510 GPS Jammer Detector (left) and CTL3520 GPS Jammer Detector and Locator (right) [http://www.gps-world.biz/index.php/products/gps-jamming-detection/products-solutions; http://www.gps-world.biz/index.php/products/gps-jamming-detection/products-solutions (access 02.08.2016)]

The answer on the question how to design GPS receiver with the option to be immune on jamming should be formulated with respect to the different receiver designs, because different solution can be implemented on different stages of the receiver[3].

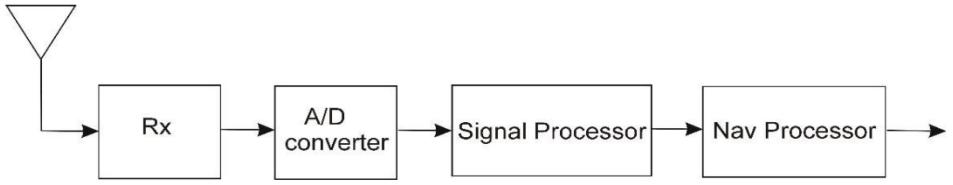

Fig. 3. The general configuration of the standard GPS receiver

The standard GNSS receiver consists of antenna, radio receiver, some digital processing chain and navigation processor. Signal processor is becoming more and more important part of these devices, sometime this is converted even into Software Design Receiver [Akos et al., 2001], [Chen et al., 2010]. However usually some kind of classic radio-receiver exists in this chain and after that signal is converted into digital form. So GNSS Receivers' Anti-Jamming Techniques can be divided into five actions:

- analogue filtering and automatic gain control at RF;
- increased resolution of Analogue-to-Digital Converter;
- Digital Signal Processing with the mechanism to reduce out-of-band interferences and suppress interfering signals before de-spreading;
- antenna/receiver in Software Defined Radio (SDR) technology.

Besides, we should notice that in many works special attention is given for manipulation in antenna beamwidth (Controlled Reception Pattern Antenna — CRPA or the possibility of Analogue Beam-Forming), which was mentioned earlier.

The first receiver stage which can be affected by jamming is receiver. The most popular front-end-receiver has the goal to filter an incoming signal in the system bandwidth and down-converting it before performing the Analog to Digital (A/D) conversion. On this stage exact filtration and adequate control of the gain is possible and important, especially when Doppler shift information is used. Probably all modern GNSS receivers use this solutions. On the other hand it must be clear that these activities are not sufficient for the counteraction to the jamming.

[3] For the ordinary user the understanding if the vessel systems are being affected is also important. In this context plausibility checks can be important (for this see [Swaszek, 2015]).

Based on accessible publications, we can define that the main element of jamming control is signal processing stage, which is executed in digital domain. It consist of the acquisition block and tracking block. The acquisition element has to determine the signal presence and provide a rough estimate of the signal code delay and Doppler frequency. The main task of this block is to correlate input signal with local replicas of the signal code as well as carrier. According to the idea of spread spectrum technology, when the GNSS signal is present and in the absence of interference, a single dominant peak should be detected by correlator. Presence of jamming signals can make the lack of correlation, but also can take effect of few peaks and finally the acquisition block may provide erroneous Doppler and erroneous delay estimates. This influences also signal tracking errors, and consequently the accuracy of the pseudoranges is degraded. This is executed by correlators which should correlate the input signal with its local replica. Under normal conditions the loop of tracking the signal should correlate them with zero tolerance, but in the presence of interference it can be shifted or oscillate. It meant permanent or not stable error. On the other hand jamming can influence the data decoding so even if the pseudoranges will be measured (more or less accurate) the receiver cannot calculate the position.

THE MANIPULATION WITH THE ANTENNA BEAM

Receiving antennas of modern satellite navigation devices are, in principle, non-directional in the horizontal plane and covering almost of the entire upper hemisphere. This way the receiver can receive signals having no knowledge about the position of satellites.

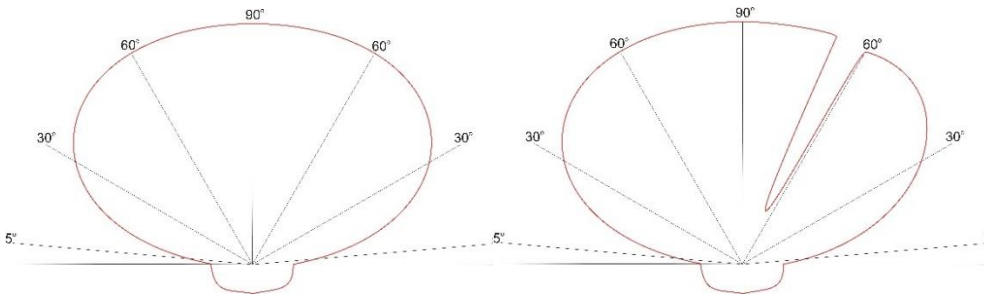

Fig. 4. The beamwidth of GNSS antenna in the vertical plane: ideal (left) and corrected — nulled on some direction (right)

Such a shape of the antenna beam makes the detection of the direction on the jammer impossible, even if we are in a position to detect this event. For this the antenna with narrow beam (directional antenna) can be useful, but this is opposite to idea of receiving satellite signals from any directions. Solution is given by the multi-segment antenna. The simplest example of this solution is an adaptive multi-element antenna which uses the power minimization technique to place nulls at the jammer direction [Rama Rao et al., 2013]. This can be reached by different time or phase delays of the signals approaching from each elements. The gain pattern of a GPS antenna can be steered on different directions and actually number of narrow beams can be formulated. In this way the resistance to jamming can be significantly increased because the signal from the jammer can be excluded. Mitigation of disturbances like jamming or interferences for GPS applications using adaptive antenna arrays has been previously studied in many publications, for example [O'Brien and Gupta, 2011], [Soloviev and van Graas, 2010], [de Lorenzo, Lo, Enge, Rife, 2011], [Rama Rao et al., 2013].

The solution is not easy to implement, because adaptive array processing requires a special hardware and intensive computational power. It needs such elements as digital beamforming processor and beam controller. Some general concept of such receiver is presented in Figure 5 (based on [US Patent 2008/0291079]).

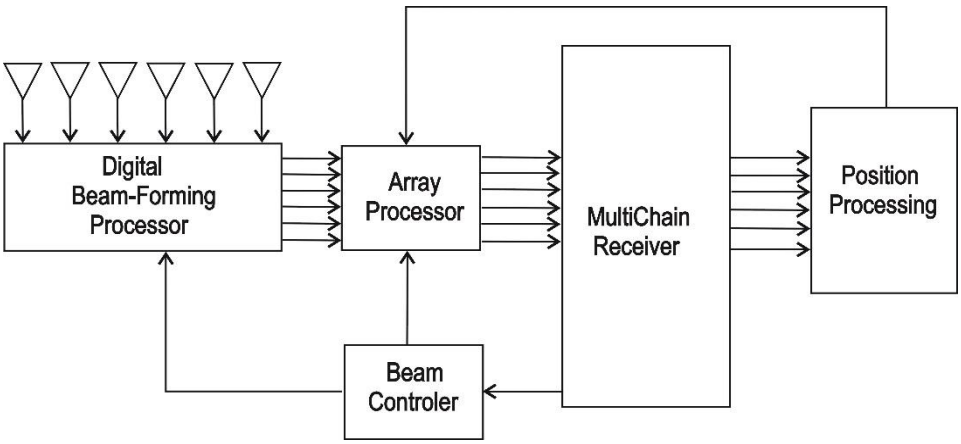

Fig. 5. General scheme of receiver with option of digital beamforming
[based on US patent 2008/0291079]

An antenna array system consists of a number of closely spaced antennas and the received signals from each antenna element are then processed coherently. As a result the fixed receive beamwidth can be formulated or the beamwidth which can be adaptively modified. The second one is more difficult to introduce so this solution is usually employed in safety critical applications. There are also examples when detached beamwidth for each visible satellite is formulated. Manipulation with the antenna beamwidth now is applied in practice and some receivers are offered. NavAtel's GAJT with active antenna based on 7-element controlled reception pattern antenna and QinetiQ's null-forming algorithm is an example. This is recognized as resistant solution on jamming. On the other side, according to some reports, the measurements in receiver equipped with antenna array and beamforming equipment can be distorted due to time processing. These may affect the carrier phase measurements and can be not desirable for high accuracy applications. A separate matter is the cost of such antenna as they can be quite expensive.

A new method of removing jamming is proposed in the paper. It involves the determination of navigation parameters by at least three independent receiving devices grouped locally, covering by its antennas beamwidth sectors with such a calculation that they altogether covers the entire upper hemisphere. The concurrent and simultaneous analysis of indications of these parallel receivers, in the presence of jammer, shows that one of the devices gives parameters different from the others. This information is then ignored in the navigation calculations.

Let's assume that in the reception area a signal is available from seven navigation satellites and from one jamming source (see Fig. 6). An antenna 1 along with a supporting receiving device (signal processor 1) decodes and processes navigation information from satellites Sv2, Sv3 and Sv4. An antenna 2 with a signal processor 2 from: Sv5 and Sv6, respectively. An antenna 3 with a signal processor 3 from: Sv1, Sv2, Sv7, respectively plus a jamming signal. A control and processing device — a navigation processor — continuously analyses and processes navigation information from all the signal processors, and when navigation information from one of the receiving channels is clearly different from that obtained from the other, the channel is removed until the data received from it is consistent with that obtained from the other two. 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 will be skipped in calculations of the position (Sv2 will be received by track 1), but statistically the remaining number of satellites is more than 4.

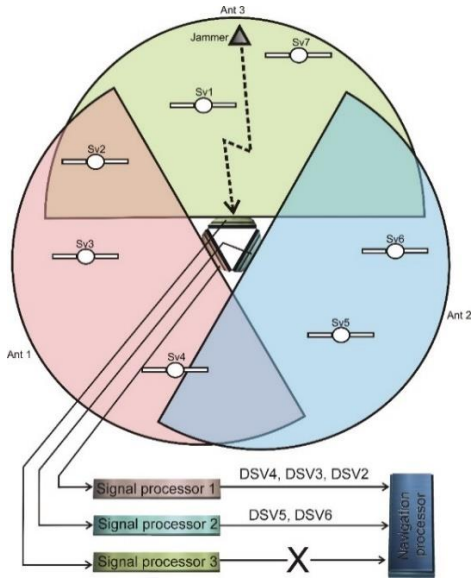

Fig. 6. Scheme of three antennas with three parallel receivers

As a result the position and velocity will be calculated on the basis of the part of satellites only, so DOP will be worst and finally the accuracy of results will be worst. But nowadays the number of satellites is so big, especially when multi-constellation signals are used, so it should work in the similar way as when some sector is shadowed. The number of antenna & processing elements can be increased, it depends on the possibility to build antenna with narrow beam. It is clear that any increase would reduce the 'lost' part of the sky should a jammer be identified.

CONCLUSIONS

In this paper, the characteristics of popular methods of improving the jamming resistance of GNSS receiver have been reviewed and partially illustrated with products offered on the market. It is shown that detection of jammer is important, but not sufficient. Nowadays receiver need some build-in mechanism to avoid the influence of jammers signals. This can be implemented at different receiver stages. The popular solution is based on multi-element antenna array steered by special digital hardware and very sophisticated software. Author propose simpler and cheaper solution which can be implemented in receivers dedicated for civilian and not-high-end applications.

REFERENCES

[1] Akos D. M., Normark P. L., Enge P., Hansson A., Rosenlind A., Real-Time GPS Software Radio Receiver, Proceedings of the 2001 National Technical Meeting of the Institute of Navigation, Long Beach, CA, USA, 2001, pp. 809–816.

[2] Balaei A. T., Motella B., Dempster A., A preventative approach to mitigating CW interference in GPS receivers, 'GPS Solution', 2008, Vol. 12, Issue 3, pp. 199–209.

[3] Borio D., Dovis F., Kuusniemi H., Lo Presti L., Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers, Proceedings of the IEEE, May 2016, [online], https://www.researchgate.net/publication/ 30179145 [access 30.08.2016].

[4] Buesnel G., Pottle J., Holbrow M., Crompton P., Make it real: Developing a test framework for PNT systems and devices, [online], http://gpsworld.com/make-it- real-developing-a-test-framework-for-pnt-systems-and-devices [acccess 10.08.2016].

[5] Chen Y. H., Juang J. C., De Lorenzo D. S., Seo J., Lo S., Enge P., Akos D. M., Real-Time Software Receiver for GPS Controlled Reception Pattern Antenna Array Processing, Proceedings of the 23rd International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland, OR, USA, 2010, pp. 1932–1941.

[6] De Lorenzo D. S., Rife J., Enge P., Akos D. M., Navigation Accuracy and Interference Rejection for an Adaptive GPS Antenna Array, ION GNSS, 2006, p. 763–773.

[7] De Lorenzo D. S., Navigation Accuracy and Interference Rejection for an Adaptive GPS Antenna Array, PhD Thesis, Department of Aeronautics and Astronautics, Stanford University, USA, 2007, [online], http://waas.stanford.edu/pubs/phd_pubs.html [access 10.08.2016].

[8] De Lorenzo D. S., Lo S. C., Enge P. K., Rife J., Calibrating adaptive antenna arrays for high-integrity GPS, GPS Solution, 2011.

[9] Digital Beam-Forming Apparatus and Technique for a Multi-beam Global Positioning System (GPS) Receiver Patent US 2008/0291079, A1 2008.

[10] Extreme space weather: impacts on engineered systems and infrastructure, Royal Academy of Engineering, London 2013, [online], http://www.raeng.org.uk [access 12.09.2016].

[11] Falen G. L., Analysis and Simulation of Narrowband GPS Jamming Using Digital Excision Temporal Filtering, Master's Thesis, Air Force Institute of Technology, Ohio 1994.

[12] Fante R. L., Vaccaro J. J., Wideband cancellation of interference in a GPS receive array, 'IEEE Trans. Aerosp. Electron. Syst.', 2000, Vol. 36, pp. 549–564.

[13] Federal Aviation Administration, GPS Privacy Jammers and RFI at Newark: Navigation Team AJP-652 Results, March 2011, [online], http://laas.tc.faa.gov/CoWorkerFiles/GBAS%20RFI%202011%20Public%20Version%20Final.pdf [access 07.07.2011].

[14] Felski A., Nowak A., Gortad M., Investigation over jamming in the aspect of the construction of the GNSS receiver, European Navigation Conference, Bordeaux 2015, [online], https://www.researchgate.net/profile/Andrzej_Felski/contributions [access 12.05.2015].

[15] Global Navigation Space Systems: reliance and vulnerabilities, The Royal Academy of Engineering, London 2011, [online], http://www.raeng.org.uk/gnss [access 12.08.2016].

[16] Hobiger T., Gotoh T., Amagai J., Koyama Y., Kondo T., A GPU based real-time GPS software receiver, 'GPS Solut', 2010, Vol. 14, Issue 2, 207–216.

[17] Hofmann-Wellenhof B., Lichtenegger H., Wasle E., GNSS Global Navigation Satellite Systems: GPS, GLONASS, Galileo & More, Springer, Wien, New York 2008.

[18] Kalyanaraman S. K., Braasch M. S., GPS adaptive array phase compensation using a software radio architecture, 'Navigation', 2010, Vol. 57, pp. 53–68.

[19] Kaplan E. D., Hegarty C. J., Understanding GPS: Principles and Applications, 2nd ed., Artech House: Norwood, MA, USA, 2006.

[20] Kraus T., Bauernfeind R., Eissfeller B., Survey of in-car jammers — analysis and modeling of the RF signals and IF samples, Proceedings of the 24th International Meeting of the Satellite Division of the Institute of Navigation Portland, 2011.

[21] 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.

[22] Ledvina B. M., Powell S. P., Kintner P. M., Psiaki M. L., A 12-Channel Real-Time GPS L1 Software Receiver, Proceedings of the 2003 National Technical Meeting of the Institute of Navigation, Anaheim, CA, USA, 22–24 January 2003, pp. 767–782.

[23] Ledvina B. M., Psiaki M. L., Humphreys T. E., Powell S. P., Kintner P. M., A Real--Time Software Receiver for the GPS and Galileo L1 Signals. Proceedings of the 19th International Technical Meeting of the Satellite Division of the Institute of Navigation, Fort Worth, TX, USA, 26–29 September 2006, pp. 2321–2333.

[24] Lisi M., GNSS jamming detection, localization and mitigation, [online], http://www.slideshare.net/MarcoLisi/gnss-jamming-detection-localization-and-mitigation [access 01.07.2016].

[25] Misra P., Enge P., Global Positioning System: Signals, Measurement and Performance, 2nd ed., Ganga-Jamuna: Lincoln, MA, USA, 2006.

[26] 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, Proceedings of the 24th International Technical Meeting of the Satellite Division of ION, Portland 2011, [online], http://gpsworld.com/gnss-systeminnovation-know-your-enemy-12475/ [access 05.06.2016].

[27] Mitigating the Threat of GPS Jamming, Novate White Paper, 2012.

[28] O'Brien A. J., Gupta I. J., Mitigation of adaptive antenna induced bias errors in GNSS receivers, 'IEEE Trans. Aerosp. Electron. Syst.', 2011, Vol. 47, pp. 524–538.

[29] Rama Rao B., Kunysz W., Fante R., McDonald K., GPS/GNSS Antennas, Artech House Boston, London 2013.

[30] Rash G. D., GPS jamming in a laboratory environment, Proceedings of the 53rd Annual Meeting of the ION, Albuquerque 1997.

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

[32] Soloviev A., van Graas F., Beam steering in Global Positioning System receivers using synthetic phased arrays, 'IEEE Trans. Aerosp. Electron. Syst.', 2010, Vol. 46, pp. 1513–1522.

[33] Space Weather Full Report, Royal Academy of Engineering, London 2013, [online], http://www.raeng.org.uk/publications [access 15.07.2016].

[34] Swaszek P. F., Radin D. S., Seals K. C., Harnett R. J., GNSS Spoof Detection Based Upon Pseudoranges from Multiple Receivers, ION ITM, 2015.

[35] http://www.allenvanguard.com/product/equinox [access 12.08.2016].

[36] http://www.allenvanguard.com/product/scorpion [access 12.08.2016].

[37] http://www.gps-world.biz/index.php/products/gps-jamming-detection/products-solutions [access 02.08.2016].

Received August 2016
Reviewed December 2016

ANDRZEJ FELSKI
Polish Naval Academy
Śmidowicza 69 Str., 81-127 Gdynia, Poland
e-mail: a.felski@amw.gdynia.pl

STRESZCZENIE

Zagłuszanie sygnałów GNSS, które może być skutkiem zarówno przypadkowych, jak i celowych działań, jest ostatnio oceniane jako jedno z największych zagrożeń dla użytkowania satelitarnych systemów nawigacyjnych. Jest to szczególnie istotne w obliczu stosowania systemów opartych na idei GPS w życiu codziennym i przy powszechnym zaufaniu przeciętnych użytkowników we wskazania tych systemów. Pomimo oficjalnego zakazu posługiwania się zagłuszaczami, są one powszechnie dostępne, zwłaszcza za pośrednictwem Internetu. Jeszcze do niedawna specjaliści podzielali pogląd, że bardzo szerokie pasmo sygnału GPS nie jest podatne na zagłuszanie, w przeciwieństwie do klasycznych technik radiowych, ponieważ i tak w warunkach naturalnych poziom sygnału w tym systemie jest niższy od poziomu szumów, a ponadto jest kodowany losowo. Jednakże obecnie z pożądanym skutkiem stosowane są tzw. jammery, co potwierdza wiele doniesień. Przeciętny użytkownik nie ma dostatecznej wiedzy na temat specyfiki zagłuszania, jak również nie dysponuje odpowiednim oprzyrządowaniem, aby wykryć sygnały zagłuszające. Zaledwie w ostatnich miesiącach pojawiły się pierwsze odbiorniki, które są zdolne uprzedzać obecność sygnałów zakłócających. Dostępne są również monitory zagłuszania zdolne wskazać nawet kierunek, z którego sygnał zakłócający dochodzi. Istnieją też odbiorniki mające specjalne rozwiązania umożliwiające pracę w warunkach zakłóceń, jednak nie są powszechnie dostępne. W artykule przedstawiono zasadnicze możliwości przeciwdziałania zagłuszaniu w systemach klasy GNSS.