Andrzej FELSKI
Polish Naval Academy
e-mail: a.felski@amw.gdynia.pl
ORCID 0000-0002-0326-3397

Tomasz KOWALIK
Polish Navy
(no ORCID No.)

DOI: 10.55676/asi.v3i1.51

SOFTWARE DEFINED RADIO AND OPEN SOFTWARE AS A CRITICAL THREAT FOR UNMANNED OBJECTS

RADIO PROGRAMOWALNE I OTWARTE OPROGRAMOWANIE JAKO KRYTYCZNE ZAGROŻENIE DLA OBIEKTÓW BEZZAŁOGOWYCH

Abstract

Implementation of the Global Navigation Satellite Systems into almost all aspects of life causes the specific, new troubles in the form of jamming and spoofing. The origin of the problem comes from the fact that power of received signals are weak, and format and modulation of the signals are publicly known. If so, it seems to be easy to transmit falsified data to the receiver. However in the opinion of some specialists the idea to generate false signals with GNSS structure seems to be very complicated. In this paper will be shown that in fact, this can be conducted with use of cheap and widely accessible tools, without demanding any extraordinary skills nor great funds. If so, this threat gathers the new meaning. Described experiment was performed within the framework of student's thesis on major navigation with the cheap software defined radio and open sources software, accessible via Internet.

Keywords: GPS threatened, jamming, spoofing, SDR

Streszczenie

Zastosowanie globalnych, satelitarnych systemów nawigacyjnych w niemal każdym aspekcie życia powoduje powstanie specyficznego, nowego zagrożenia pod postacią zagłuszania lub fałszowania sygnałów satelitarnych. Przyczyną problemu jest to, że sygnały docierające do Ziemi są niezwykle słabe, zaś ich struktura i sposób modulacji są powszechnie znane. W tej sytuacji nietrudno wyemitować w kierunku odbiornika sygnały fałszywe. Jednak w opinii wielu specjalistów próba wyemitowania fałszywych sygnałów posiadających taką strukturę jak te, które są emitowane przez satelity, wydaje się niezwykle złożona. W artykule wykazano, że w istocie można tego dokonać, posługując się tanimi i powszechnie dostępnymi narzędziami bez potrzeby posiadania nadzwyczajnych umiejętności lub funduszy. Jeśli tak, to zagadnienie nabiera nowego znaczenia. Opisany eksperyment został wykonany w ramach pracy nad pracą magisterską z nawigacji w oparciu o tanie radio programowalne oraz bezpłatne, dostępne za pośrednictwem Internetu oprogramowanie.

Słowa kluczowe: zagrożenie dla GPS, zagłuszanie, fałszowanie, radio programowalne

Artykuł wpłynął do redakcji: 22.05.2023 / Zatwierdzono do publikacji: 24.06.2023

1. INTRODUCTION

GPS – like systems are considered to be extremely accurate, very reliable, and this is a reason why Global Navigation Satellite Systems are implemented into almost all aspects of life. Now it is especially important for all unmanned vehicles when the GNSS receiver is treated as the self-evident data source about the position and the movement. However the power of GNSS signals received on the earth is very weak. This is a reason why it is easily subjected to environmental interference or deliberate generated transmissions of radiofrequency signals in the receiver's band. This is a very general jamming, which is more and more comprehended issue these days. In effect this can be observed as a decline of received signals power, ongoing until the moment of entire blockade of the receivers circuits. Whereas, spoofing refer to generate signals that acquire the identical structure with these which are transmitted from satellites, however contains false data. This leads to the situation when receiver's work seems to be correct while presented parameters can be completely false. Such process is available to complete with using equipment similar to this which is installed on satellites. In such case, the spoofing seems to be very difficult and expensive task.

There is a lot of papers about spoofing, which is in fact – some kind of hacking. Mentioned threats can refer to plenty areas of the human activity, such as the tracking some goods (precious or hazardous), traffic control (railways, air, car, as well as marine). A separate problem is the use of these systems in electronic commerce, what is inseparable with the general tracking cell phones users. What is more, the average GPS user does not realize, how important is the time synchronization in nowadays word and how commonly GPS is in use as the precise time-scale. Intention of this paper is to communicate how easy is the process of spoofing and how big threat it can create. The paper describes experiments with spoofing GPS receiver with the device built on the basis of easy and cheap electronic elements and software free-accessible via Internet.

This paper is divided into three parts. At the beginning of the text, the importance of this problem is mentioned. In the second one some general information about discussed spoofing process is given. And finally some results of spoofing experiments made with free-accessible components are presented.

2. BACKGROUND OF THE SURVEY

Description of all details of open GNSS signals can be found in official documents so all information for this procedure, such as frequency of the signal, modulation, as well as message content are known. So the procedure of evaluate false signal can be easily generate with the proper application and radio-transmitter. Such signal will be interpreted as correct satellite signal in the receiver although it will consists the false navigation data. But in the opinion of many experts this is impossible to force the receiver to receive spoofer's signals when if it tracking real satellite signals. This

DOI: 10.55676/asi.v3i1.51

is because the spoofer's signal is recognised in this moment as the same signals. So in the some sense receiver is "closed" on additional signals with the same codes (SV identifiers). These opinions were crossed out in 2013, when the research team of University of Texas led by Professor Humphreys successfully demonstrate spoofing[1]. Similar experiment was conducted by researchers from Stanford and Cornell Universities[2]. Then they proved, as highly vulnerable to spoofing is GPS receiver and how it is difficult for the user to detect this attack.

Spoofing possibilities became showed not only in the academic area. Very brightly it is visible on the military field. According to some suspicions, incident with the US RQ-170 "Sentinel" drone forced to landing in December 2011 on Iran territory is the example of spoofing attack[3] what is a first example of this threat for autonomous objects. There are suggestions, that Iranians adopted spoofing and in addition they sent some wrong instructions to this object. Anyway finally they caused the mentioned drone to land on enemies territory. In turn December 2012, Iran announced that they captured the next US drone by using the same technology[4]. According to US Coast Guard, in June 2017 at least 20 ships near the Novorossiysk at Black Sea had incorrect GPS positioning. There are opinions, that this is the evidence that Russians can use spoofing too[5]. Today can be found a lot the suggestion in the press that Russians universally use this technique in Ukraine that to counteract the weapon which is based on GPS.

Problem of jamming or spoofing the GPS is very common in field of maritime transportation. Lot of announcements is accessible on web page of Navigation Centre of US Coast Guard. For example, the message of 23, August of 2022 (GPS Problem Report, 2022) which can be interpreted as jamming activity at the beginning and spoofing as the next: "Merchant ship in the area of Strait of Hormuz informs as they approached Dubai area they experienced loss of GPS signal. It took 4 hours before signal was back. Ship reports other ships informing on VF 16 channel that they too have lost GPS signal. Ship informs losing GPS signal in all systems and receivers (GPS, Sat C, Satellite Log, AIS). GPS signal would come back for a minute, however it would show wrong location and back at Das Island. Ship informs total of 4 hours experienced without GPS. All GPS issues started 2 hours before passing Abu Musa Island and 2 hours after passing the island"[6]. In this message should be noticed, that wrong work of GPS receiver means in the same time problems with many other devices, as

[1] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, P.M. Kintner Jr., *Assessing the spoofing threat: Development of a portable GPS civilian spoofer*. In ION GNSS 21st. International Technical Meeting of the Satellite Division, Savannah, GA, 16–19 September 2008.

[2] M.L. Psiaki, T.E. Humphreys, *GNSS spoofing and detection*. Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016. DOI: 10.1109/JPROC.2016.2526658.

[3] S. Bian, Y. Hu, B. Ji, *Research status and prospect of GNSS anti-spoofing technology*. Scientia Sinica Informationis, vol. 47, no. 3, pp. 275–287, 2017. DOI. 10.1109/AIM.2017.8014219.

[4] D. Cenciotti, *Iran has captured another U.S. spy drone. Once again with minimal damage*, The Aviationist, 4.12.2012, https://theaviationist.com/2012/12/04/scan-eagle/ [access: 20.05.2022].

[5] D. Goward, *Mass GPS Spoofing Attack in Black Sea?* The Maritime Executive, https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [access: 12.07.2022].

[6] GPS Problem Report/ Status/Navigation Center, https://www.navcen.uscg.gov./contact/gps-problem-report [access: 23.08.2022].

Sat communication, Automatic Identification System (AIS), Satellite Compass etc., and this can mean the entire loss of the control over the autonomous vessel and AIS blocked. This seems be extremely important in the context of unmanned vessels in the future[7].

Mentioned above cases are bound with activities of professionals, who surely possessed the very complicated equipment. The question comes into being, whether this is possible for not specialists?

3. METHODOLOGY OF SPOOFING THE GPS

According to many references, for example[8], the GPS spoofing attacks must consists two steps: at first, attacker lures the victim GPS receiver to migrate from the legitimate signal to the spoofing signal (takeover step). This phase can be either brute forced or smooth. In the first case, a spoofer simply transmits the false signals at a high power, causing the victim to lose track of the satellites and lock-on to the stronger spoofing signals. In this version some "jump" of receiver position and/or speed as well as course can be observed. If so, some method of cross-checking of the data from different navigation sources can be implemented as a method for alarming the user. In this variant spoofer produce for himself false ephemerides data. In contrast, smooth takeover begins by transmitting signals synchronized with the original ones and then gradually false signal should be amplified over the original one to cause the migration. The advantage of smooth takeover is the stealthiness since it will not generate abnormal "jumps" in the received signal. However, smooth takeover requires specialized hardware to real-time track and synchronize with the original signals at the victim's location. Next, in the second step, the attacker can manipulate the GPS receiver by either shifting the signals' arrival time or modifying the navigation messages. This case is difficult to notice by GPS user without any additional information.

Regardless of the employed technique, spoofing demands the radio transmitter working in the GPS band. If the transmitter has to broadcast signals in the GPS structure, the system to the formation of these signals is indispensable. It is important to remember that these signals contain navigational data, suitable codes, and, what is the most important, need to be precisely timed. In smooth mode attacker must synchronise own system with real satellites, so authentic ephemerides are needed. All that suggests the extraordinary complexity of the process and the necessity of the possession of specialistic tools, but in fact all this elements are easy accessible. Transmitter can be made with software defined radio when the rest is accessible via Internet as a free software.

[7] A. Felski, K. Zwolak, *The Ocean-Going Autonomous Ship – Challenges and Threats*, J. Mar. Sci. Eng. 2020, 8, 41, DOI: 10.3390/jmse8010041.

[8] T.E. Humpreys et all, *Assessing the spoofing…*, op. cit.; M.L.Psiaki, T.E.Humpreys, *GNSS spoofing…*, op. cit.

4. EXPERIMENTS

Described cases were acquired within the framework of student's diploma thesis[9]. In experiments the programmable radio HackRF One, by Great Scott Gadgets[10] was applied. This is the very popular device with advantage of the low price and the wide range of the frequency, from 1 to 6 MHz. The device can be used both as the receiver, and as the transmitter.

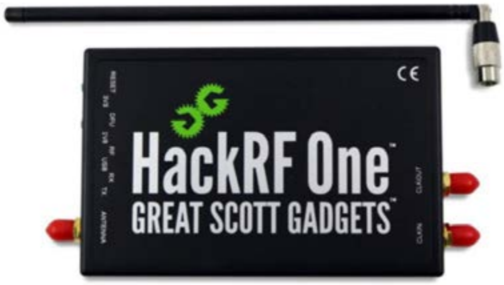


Figure 1. Software-defined radio used for experiments

Source: photo authors.

In the experiment the device was used as the transmitter generating signals about the GPS structure. Software was applied from hackrf_transfer.exe[11]. For these experiments, the antenna ANT500 (product of the same company) with the band from 1 up to 75MHz has been used. Connections of the device with computer was realised with cable with connectors micro-USB and USB-A. As the interference for GPS was produced, important is the power of the transmitter. HackRF One is equipped with one controlled output with the maximum power in the antenna port of 50mA/3,3V. During experiments, which was conducted in the closed area of Polish Naval Academy, transmitter worked with the minimum power. In practice the range of the system was no more than of 5 meters from the spoofer.

For the experiment following elements were regulated:

- transmitted frequency in 1575,42MHz;
- sampling rate (possible is from 2 to 20 Million samples per sec);
- amplifier (On/Off);
- level of the signal gain in db.

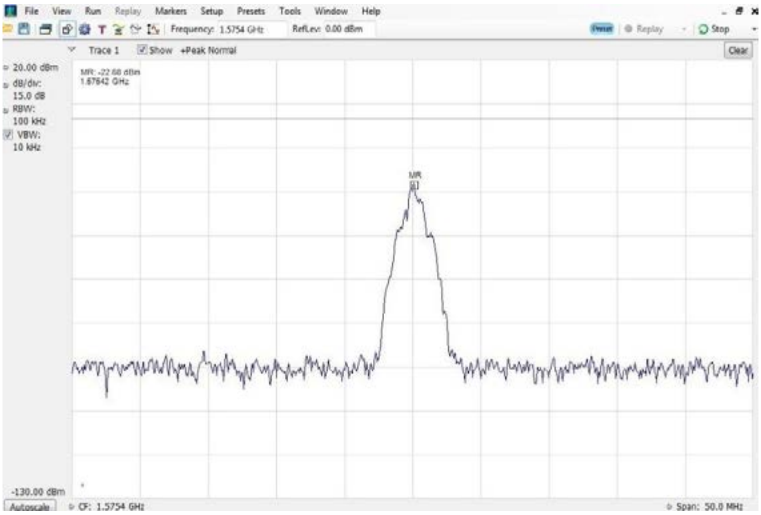
At a beginning the transmitted radio signal were verified with the use of spectrum analyser RSA5100A of Textronix. Figure 2 presents the result of the analysis of the generated signal. Here transmitter is connected to the analyser with the cable. On

[9] T. Kowalik, *Capabilities to disturb GNSS systems*, Master thesis (in Polish), Polish Naval Academy, Gdynia 2022.

[10] Great Scott Gadgets, https://github.com/greatscottgadgets/hackrf [access: 12.05.2022].

[11] User osqzss, GitHub, https://github.com/osqzss/gps-sdr-sim [access: 12.05.2022].

the graph apparently that the central frequency of the signal is 1,57542 GHz, signal level in this case medianly carried out –22 dBm, and the shape of the envelope curve is agreeable with the shape of the C/A GPS signal. It is worth adding that as far as the central frequency was very stable, then the power level displayed to continuous oscillations from –16 to –40 dBm. Similar verification with the use of the antenna showed the fall of the power of the signal to –60 dBm which evidently diminished as the distance increased. At the same time, the signal bandwidth has expanded a little.



Frequency: 1.5754 GHz
RefLev: 0.00 dBm
Trace 1 ☑ Show +Peak Normal
20.00 dBm
dB/div: 15.0 dB
RBW: 100 kHz
☑ VBW: 10 kHz
MR: -22.60 dBm
1.57542 GHz
-130.00 dBm
CF: 1.5754 GHz
Span: 50.0 MHz

Figure 2. Spectrum of the generated signal

Source: own study.

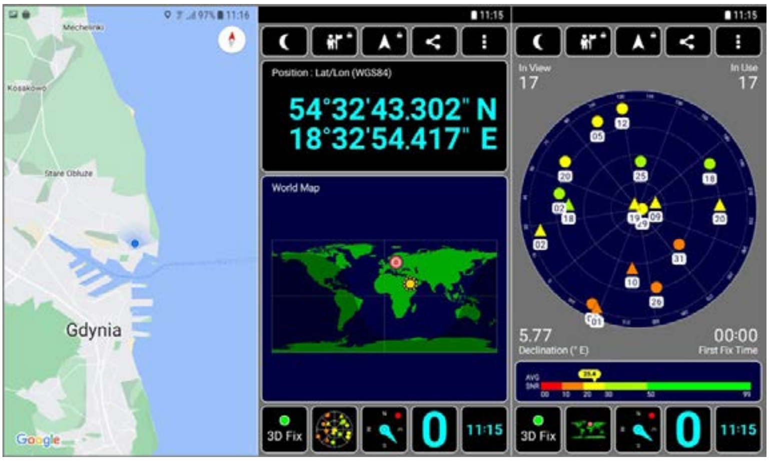
Before the beginning of spoofing experiments the reaction of GPS receivers on such signal was examined. It appeared that the signal generated in the GPS band, even without manipulations, had worked as a jammer. During the experiments Samsung Galaxy A5 has been tested. Firstly the reaction of receivers on spoofing signals without the access of real satellite signals was tested. Reactions was the same as in the presence of the jammer – mainly the signal to noise ratio was decreasing, depending of the distance between transmitter and receiver.

For spoofing experiment first of all ephemerides of the system must be delivered. It was made with free accessible software gps-sdr-sim[12]. The first step, when the receiver was isolated in the room, without real signals of the satellites, spoofing process was very easy. Device "jump" from historical position to the false without any troubles. Experiment was executed in Gdynia, but ephemerides has been modelled for Gibraltar. After the switch on the spoofer, in few seconds exactly, the position "jumped" to Gibraltar.

[12] gps-sdr-sim, Accessible at GitHub, osqzss/gps-sdr-sim: Software-Defined GPS Signal Simulator [access: 12.05.2022].

DOI: 10.55676/asi.v3i1.51

Experiments in the presence of real satellite signals was carried out in the open area, with the clear visibility of the sky. In this stage ephemerides must be compatible with the trough. For this purpose almanac broadcasted by NASA via Internet was used (https://cddis.nasa.gov/archive/gnss/data/daily/). This files are modified every hour, so this solution give opportunity to simulate constellation only by one hour and only for one place (in static mode). Anyway it was surprisingly easily made. Here is presented experiment from 22 May of 2022, at 11:15 UTC. At the beginning, before to start the spoofer, GPS module in Smartphone work properly presenting correct position LAT = 54°32’43,3”N and LON = 018°32’54,4”E. Blue symbol on Google Maps shows active position (see Figure 3), as well as some other information (for example S/N ratio) is presented. It is worthy to stress, that in this moment some GLONASS satellites are accessible (presented as triangles), however only GPS satellites are in use.

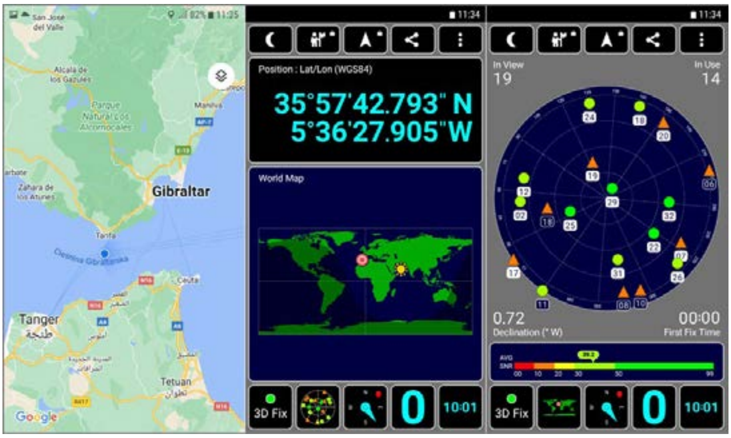


Position : Lat/Lon (WGS84)
54°32'43.302" N
18°32'54.417" E

In View 17
In Use 17
5.77 Declination (° E)
00:00 First Fix Time

Figure 3. Starting data during experiment with real satellites (22-05-2022 11:15UTC)
Source: own study.

At the beginning additional jammer has been used for extinguishing of true satellite signals. When receiver display “no signals” spoofer was switched-on and after that position fluently moved to Gibraltar signalling no faultiness’s! Sky plot presents all “new” satellites (transmitted via spoofer) and still present the presence of GLONASS satellites observed in Gdynia! This is intelligible, as spoofer generates only GPS signals and GLONASS one are received from the space. Also it should be noticed, that GPS module shows wrong time, which is determined in the spoofer (10:01), the different than Smartphone (11:34).



Position : Lat/Lon (WGS84)

35°57'42.793" N
5°36'27.905"W

World Map

In View 19 | In Use 14

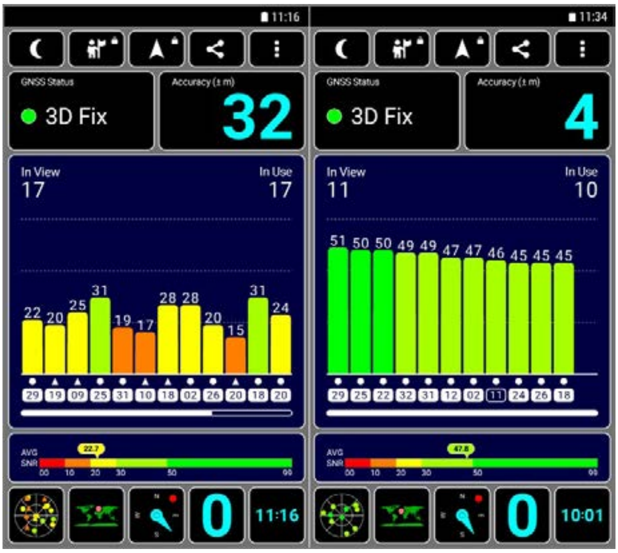
0.72 Declination (° W) | 00:00 First Fix Time

3D Fix | 0 | 10:01

Figure 4. Data after spoofer switched on

Source: own study.

More complicated is discussion about satellites when spoofer works. On Figure 5 are presented graphs with received signals (left–before spoofing and right–after). Important is to notice the strength of received signals after spoofing starts. This is clear answer why so easy spoofing was made. It is not clear why number of satellites in view got smaller.



GNSS Status ● 3D Fix | Accuracy (± m) 32

In View 17 | In Use 17

AVG SNR 22.7

0 | 11:16

GNSS Status ● 3D Fix | Accuracy (± m) 4

In View 11 | In Use 10

AVG SNR 47.8

0 | 10:01

Figure 5. Graf presenting status of receiving signals (left – before spoofing and right – when spoofing is activated)

Source: own study.

5. DISCUSSION

The goal of this paper is to show how easy and trivial spoofing process is, as well that hardware and software for this is easy accessible. Presented method, as it base on open access software, has some borders anyway. This can be done only in static mode and generated signals are usable only during one hour. Though that will do also to disturb the receiver of the user who moves, not making mention on GPS users in static mode and disruption which lasts one hour can be costly for many users. In addition, experiments was conducted using amateur radio, so range of spoofer was short. However this limitation results in absence of stronger transmitter and the more excellent GPS simulator. Any way results shows, that spoofing can be easily produced and in real life seems be very big problem in the near future, as one ought to perceive this threat also on the part of amateurs and terrorists.

6. CONCLUSIONS

GNSS is commonly used in many military and civilian applications to provide continuous, secure and reliable positioning, speed measurement, course and timing services for users who require navigation, timing and location services. Aside from the wide use it in all aspects of people’s life and work, it is the main source of information for autonomous vehicles, so the authenticity and integrity of satellite navigation signals are particularly important. In case of unmanned systems it has negative influence on the navigation of the vehicle, but also threatens the loss of the contact. If the receiver suffers spoofing or jamming but does not take any counteraction the results calculated by the receiver are likely to cause huge errors. It is few publications about methods of spoofing and it gets out of them that this assignment is difficult and expensive. According the experts’ opinion spoofing demands the highly qualified staff and the complicated apparatus. The present announcement proves that this is not a truth, because this is realizable almost unprofessional methods, and consequently the threat is greater than till now one founded. In this paper the simple method how spoofing can be easy realised is presented with the free accessible software and tiny and cheap hardware. if unmanned vehicles , for example Marine Autonomous Surface Ships, will rely only on GNSS signals, then in soon we should be afraid about the growths of such threat.

REFERENCES

Bian S., Hu Y., Ji B., *Research status and prospect of GNSS anti-spoofing technology*, “Scientia Sinica Informationis” 2017, vol. 47, no. 3, DOI. 10.1109/AIM.2017.8014219.

Cenciotti D., *Iran has captured another U.S. spy drone. Once again with minimal damage*, The Aviationist, 4.12.2012, https://theaviationist.com/2012/12/04/scan-eagle/ [access: 20.05.2022].

Felski A., Zwolak K., *The Ocean-Going Autonomous Ship – Challenges and Threats*, "J. Mar. Sci. Eng." 2020, vol. 8(41), DOI:10.3390/jmse8010041.

Goward D., *Mass GPS Spoofing Attack in Black Sea?*, The Maritime Executive, https://www.maritimeexecutive.com/editorials/mass-gps-spoofing-attack-in-black-sea [access: 12.07.2022].

GPS Problem Report/ Status/Navigation Center, https://www.navcen.uscg.gov./contact/gps-problem-report [access: 23.08.2022].

gps-sdr-sim, osqzss/gps-sdr-sim: Software-Defined GPS Signal Simulator [access: 12.05.2022].

Great Scott Gadget, https://github.com/greatscottgadgets/hackrf [access: 12.05.2022].

Humphreys T.E., Ledvina B.M., Psiaki M.L., O'Hanlon B.W., Kintner Jr P.M., *Assessing the spoofing threat: Development of a portable GPS civilian spoofer*, ION GNSS 21st. International Technical Meeting of the Satellite Division, 16–19, September 2008, Savannah, GA.

Kowalik T., *Capabilities to disturb GNSS systems*, Master thesis (in Polish), Polish Naval Academy, Gdynia 2022.

Psiaki M.L., Humphreys T.E., *GNSS spoofing and detection*, "Proc. IEEE" 2016, vol. 104, no. 6, DOI: 10.1109/JPROC.2016.2526658.

User mossmann, GitHub, https://github.com/greatscottgadgets/hackrf/blob/master/host/hackrf-tools/src/hackrf_transfer.c [access: 12.05.2022].

User osqzss, GitHub, https://github.com/osqzss/gps-sdr-sim [access: 12.05.2022].