DE GRUYTER OPEN

DOI: 10.1515/aon-2016-0016

SŁAWOMIR ŚWIERCZYŃSKI, PIOTR ZWOLAN, ILONA RUTKOWSKA
Polish Naval Academy, Gdynia, Poland

JAMMING AS A THREAT TO NAVIGATION

ABSTRACT

The whole world is dependent on satellite systems as they are used in almost all fields of economic and social life, in transport, banking, industry, agriculture, etc. Thanks to the development of technology, most smartphones used everyday have been equipped with a built-in GNSS receiver, many cars with navigation systems and all vessels with GNSS receiver or a satellite compass for navigation. Systems working on similar frequencies can be used for jamming or spoofing satellite systems. Such purposeful system jamming can be damaging to users and society as a whole. This article includes a description of jamming and a presentation of one of possible receiver designs allowing for jamming signal detection. This receiver has been designed and built by the authors of the article.

Keywords:
GNSS, jamming.

INTRODUCTION

Humanity is dependent on satellite systems as they play a key part in modern societies' efficient functioning. During sailing the safety of navigation is very important. Often one does not wonder why a receiver lost the location of the vessel or is showing a miscalculated location when receiving satellite signal. It can be catastrophic when a ship finds itself in a region hard to navigate through without the ability to pinpoint its position. Satellite signal jamming is a pressing matter especially considering military or terrorism aspects. Whenever the readings are miscalculated or loss of signal occurs, it is often attributed to coincidental interference or a mechanical damage of the GNSS receiver system (i.e. the connection

between the antenna and the receiver, the antenna or receiver themselves). Nowadays a different problem has emerged, jamming, which is the purposeful interference with satellite signal. It has to be observed whether jamming is a threat to navigation and everyday life, both of which are hugely dependent on GNSS systems. In this article the authors present jamming as a threat to the modern world, which is dependent on GNSS systems and describe ways to detect an interfering signal.

JAMMING AND JAMMERS

Satellite signal interference can be classified as natural, coincidental and purposeful. Natural interferences are the most common, and they originate when the signal travels through different layers of the atmosphere, where due to the physical and chemical properties of those layers refracting and damping take place. Coincidental interference is caused by unplanned emission on particular radio frequencies. Purposeful interference is the most harmful, and three types of actions can be determined: spoofing, meaconing and jamming as well as purposeful actions aimed at disabling a satellite system (all actions pertaining to the destruction of satellites or their controls). Spoofing entails falsifying a signal, where a fake satellite signal is transmitted and the receiver recognizes it as original and thus, the presented location is miscalculated. Meaconing is interfering with and silencing a signal and then transmitting a different signal so as to mislead the receiving party. As a result of such action, we can navigate someone into a different location, change the course of a vessel or send an aircraft into a different drop zone. Jamming is another method of interfering on which this article is focused [Figurski et al., 2011].

Utilizing satellite systems allows users to position and track their own movements. Stolen goods can be tracked and logistic companies can track their vehicles. Such a widespread use of trackers makes a vast number of people uncomfortable, especially those who do not want to be followed or those who want to harm others for financial gain. Utilizing market available satellite signal jammers which affect all receivers within their operation radius can cause some people to be ‘invisible’ to GNSS monitoring systems.

The development of technology makes our lives easier, but at the same time creates many threats and affects our personal lives. Mobile phone users

utilizing GNSS signal can be easily located without permission. Government agencies of private institutions (hackers or detectives) can take advantage of that fact. By placing malware within the phones of potential victims, hackers can transmit their position. Company car drivers or company phones' owners do not want to be supervised by their superiors all the time. To protect against being 'spied on', GNSS jamming can be helpful, that is willful use of jammers that generate signals on the same bandwidth as GPS. The signal strength from satellite systems gathered by receivers is weak. Satellite orbiting at 22 000 km altitude sends a signal that travels through many atmospheric layers, characterized by different physical qualities and thus damps the signal. In technical specifications of receivers we can find that the signal gathered is around –170 dBm, whereas for correct functioning strength, larger than minimal is required. A receiver can lose data due to jamming signals which have the strength several times higher than the minimal received by the receiver [http://www.gps.gov/technical/icwg/IS-GPS-200H.pdf].

A signal of this strength can easily be interfered with. Interfering devices called jammers are commonly used for this purpose. The most popular market available models are characterized by the power output of 2 W and can jam all GNSS bandwidths. Their range is about 20 m. Jammers with higher power outputs can be found with greater range and which can jam frequency bandwidths as in the Figure 1.

Output port	Frequency	Average output-putting power	Channel output-putting power
LOJACK	173.075Mhz	35dBm	5dBm/30KHz(min)
CDMA	851-960MHz	35dBm	5dBm/30KHz(min)
DCS/PCS	1805-1990MHz	33dBm	2dBm/30KHz(min)
3G	2110-2170MHz	33dBm	2dBm/30KHz(min)
WIFI2.4G	2400-2500MHz	30dBm	0dBm/30KHz(min)
GPS	1575MHz	30dBm	5dBm/30KHz(min)
4G LTE	725-770MHz	34dBm	3dBm/30KHz(min)
4G WIMAX	2345-2400MHz	30dBm	0dBm/30KHz(min)
Power supply: AC adapter (AC220V-DC12V) Shielding Radius: (2-40) meters@-75dBm still depends on the strength signal in given area.			
Dimension: (width, height, length) 140x51x355mm			

Fig. 1. Portable jammer JM-16W-A (CDMA, GSM1800(DCS), GSM1900(PCS), 3G, GPS, WIFI, 4G WIMAX, 4G LTE) [http://www.jammer4uk.com/high-power-8-antenna-3g4gltewimaxcell-phonegpswifi-jammer-p-48.html (access 24.08.2016)]

GNSS jamming causes all receivers within the devices' range to not function properly. High powered jammers pose a threat not only to GNSS receivers, but also to reference stations, which can transmit wrong network updates or be disabled, and also to mobile network towers utilizing GPS systems for current time settings. Users who do not want to be under surveillance can use smaller jammers mounted on cars. Nowadays many jammers come with the small power output of 150 mW and the range of 10 m, whose signal come from the inside of a car (Fig. 2).

Fig. 2. Low power jammer [http://www.jammerall.com/products/Vehicle-Car-Anti-Tracker-Mini-GPS-Jammer-Blocker.html (access 24.08.2016)]

If jamming becomes very popular and many users take advantage of it in their vehicles and everyday life, then a high volume of car traffic near reference stations and network towers can interfere with their service. Paper maps are hardly used while driving, so when devices start to malfunction on occasions, one can wonder if jammers are not used in the vicinity. There are occurrences when jamming is beneficial and can save lives. Special cars equipped with jammers are constructed (Fig. 3).

They generate high powered signal on a wide bandwidth of frequencies. It is supposed to jam all devices which could be used by a terrorist for remote detonation in a given area (Fig. 4). Such jammers can be used to protect convoys or mass events where thousands of people gather.

Fig. 3. Special operation car equipped with a jammer [http://www.sesp.com (access 08.09.2016)]

Fig. 4. Utilizing jamming in the fight against terrorism [http://www.sesp.com (access 08.09.2016)]

PREVENTING JAMMING

Various science centers are researching the jamming phenomena. Detectors uncovering GNSS signal jamming are placed near high-volume traffic roads to show the scale of the phenomenon. It is hard to assess whether the discussed issue will grow exponentially in the near future. Nevertheless, the problem has been noticed by scientists. Currently it is more of an issue of individual cases.

A jammer generating a signal of a couple of watts of power can 'disable' devices in the range of several miles. It is dangerous in both military and civilian cases. Preparations must be made to prevent such incidents. Several companies are working on receivers that try to limit or remove the influence of jamming on GNSS receiver positioning capabilities. One of those is Novotel, which designed the GAJT technology (GPS Anti-Jam Technology) with versions transmitting on land, sea and mobile platforms such as UAV. Military vehicles or vessels can utilize the protection given by GAJT (Fig. 5).

Fig. 5. Utilizing GAJT technology on a vessel [http://www.novatel.com/products/gnss-antennas/gajt-anti-jam-antennas/gajt-710ms/ (access 26.08.2016)]

GAJT is a special antenna system (Fig. 6) which consists of several segments providing direction for receiving satellite signals. Using an elimination algorithm for particular zones, jamming can be ignored and the correct location can be presented.

Fig. 6. GAJT Antenna [http://www.novatel.com/products/gnss-antennas/gajt-anti-jam-antennas/gajt-710ms/ (access 26.08.2016)]

To prevent jamming we need to assess whether an interference source exists and where it is located. With a strong jammer signal, no antenna or system will allow our receiver to present a location. In consequence, the only solution to eliminate the interference is to find and destroy or disable the jammer. To locate the source of interference an incident detection and reporting system must be used. One such system is a receiver module by GlobalTop Technology Inc. GMMU5J (Fig. 7).

Fig. 7. GMMU5J Receiver [http://download.maritex.com.pl/pdfs/wi/GPSGMMU5J.pdf (access 26.08.2016)]

The receiver has an inbuilt Anti-JACK™ (Anti-Jamming Assessment Command Feedback) function which detects and informs about incidents of jamming. It has double anti-jamming protection. After detecting jamming the GPS module changes the voltage level signal on output 2 (pin 2) (for example to be used with an outside control system such as alarm protection) and sends an NMEA protocol warning to an outside device (a computer with NMEA software) through UART (Universal Asynchronous Receiver and Transmitter). It has two levels of sensitivity of jamming signal detection, with four modes of operation, as well as energy saving mode for jamming signal detection. GMM-U5J is one of the newest systems from the u5 series with 'Anti-J.A.C.K' modules. Other modules with anti-jamming systems can be found on the market. Quectel and u-blox products have advanced detection and noise reduction functions. In those modules a mechanism of detecting of initializing devices interfering with GNSS signal is installed. After activating the 'jamming monitor' function the module is able to differentiate between background noise and a jamming signal and can inform users in case a jammer is detected.

Utilizing a receiver module with 'Anti-J.A.C.K' function, one can construct a device to detect the jamming source. To design the system, one of many 'DesignSpark' free software products can be utilized.

The receiver was constructed with two modules:

- a converter enabling communication between two popular serial interfaces USB and UART as a ready-made component;
- GPS GMMU5J receiver module.

The receiver has been designed and constructed by the authors themselves. The schematics and PCB board for the receiver are presented in the following figures.

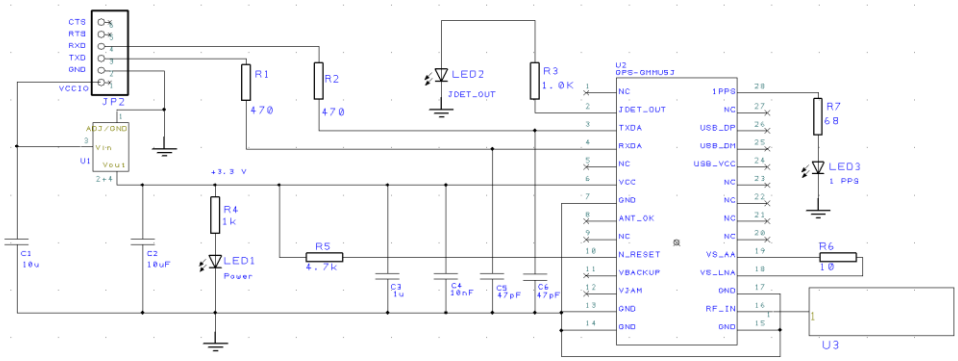

Fig. 8. Receiver schematics

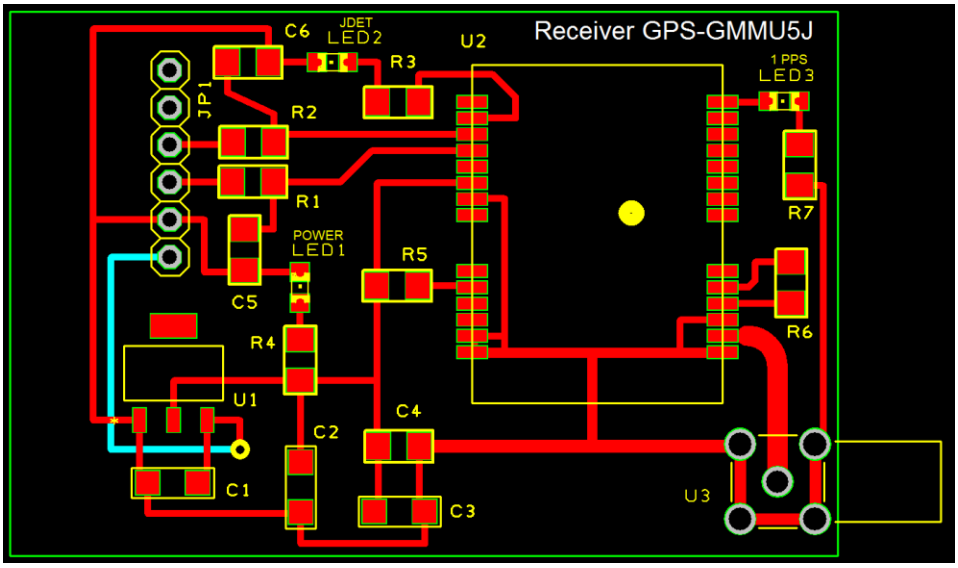

Fig. 9. Receiver PCB board

The DesignSpark software has enormous libraries of elements to create projects. It may happen that one is creating a device and its elements are not found in the DesignSpark libraries (i.e. GMMU5J). For such a case we must create a new element, add it to the library to place on the schematics and create a PCB board. The pictures below present the process of creating an additional element used in the project.

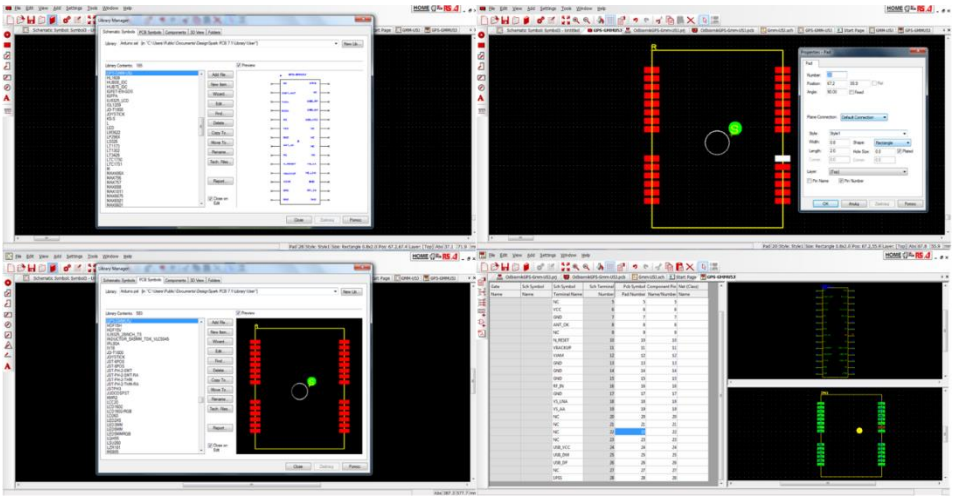

Fig. 10. The process of creating an additional element used in the project

Before creating the real life device we can see a 3D visualization in the DesignSpark software as presented in the picture below.

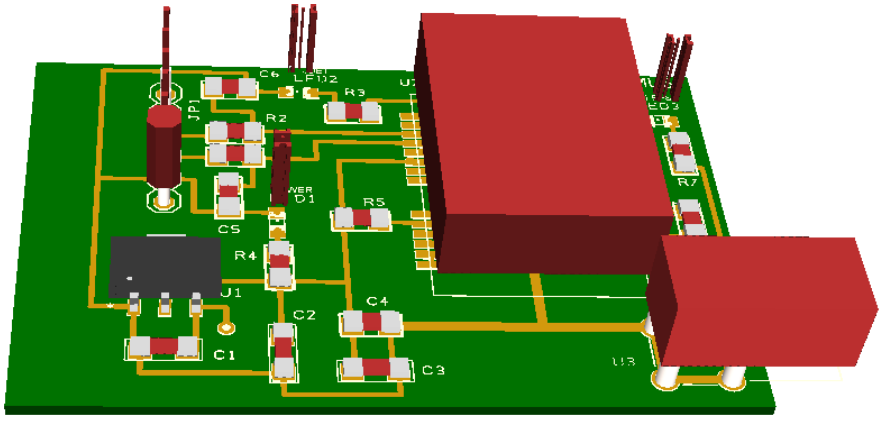

Fig. 11. Receiver 3D visualization

The constructed devices based on GMMU5J module are presented in the Figure 12.

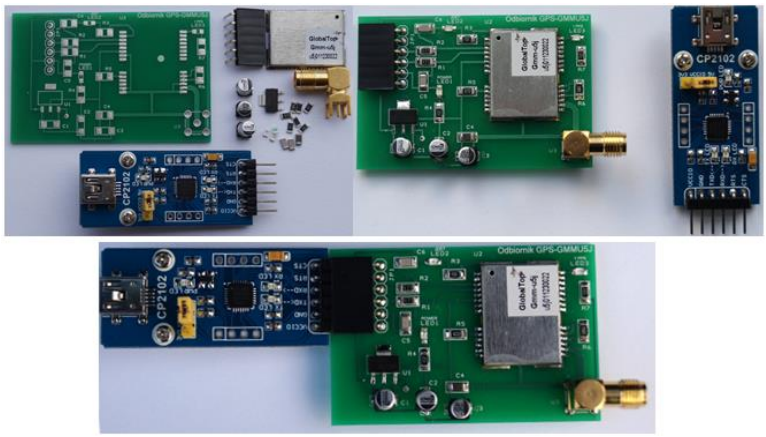

Fig. 12. Jamming detecting

The functioning of the receiver can be assessed by utilizing any software for serial transmission and reading information in the NMEA 0183 standard. The authors tested the receiver with two free software applications. The first one was GPS viewer (Fig. 13). The application shows the availability of satellites and levels of signals received by the receiver. The NMEA information can be chosen and saved to a file.

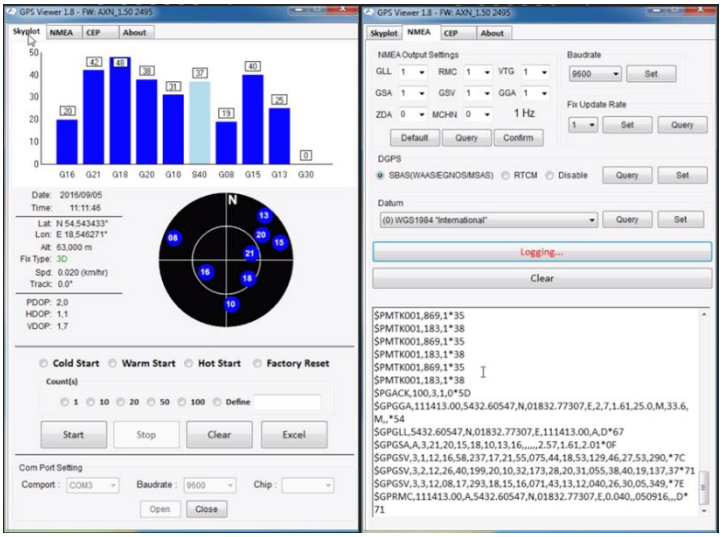

Fig. 13. GPS Viewer

Utilizing this application, one can only check the status of satellite systems. Even if the signal levels are low or disappear, one cannot assess the reason for lack of positioning or if there is a jammer present in the vicinity. The other tested application was GPS Test Tool which, apart from visualizing the received signals and status of satellite systems, also has the function of detecting jamming. The functioning receivers' visualization is shown in the Figure 14.

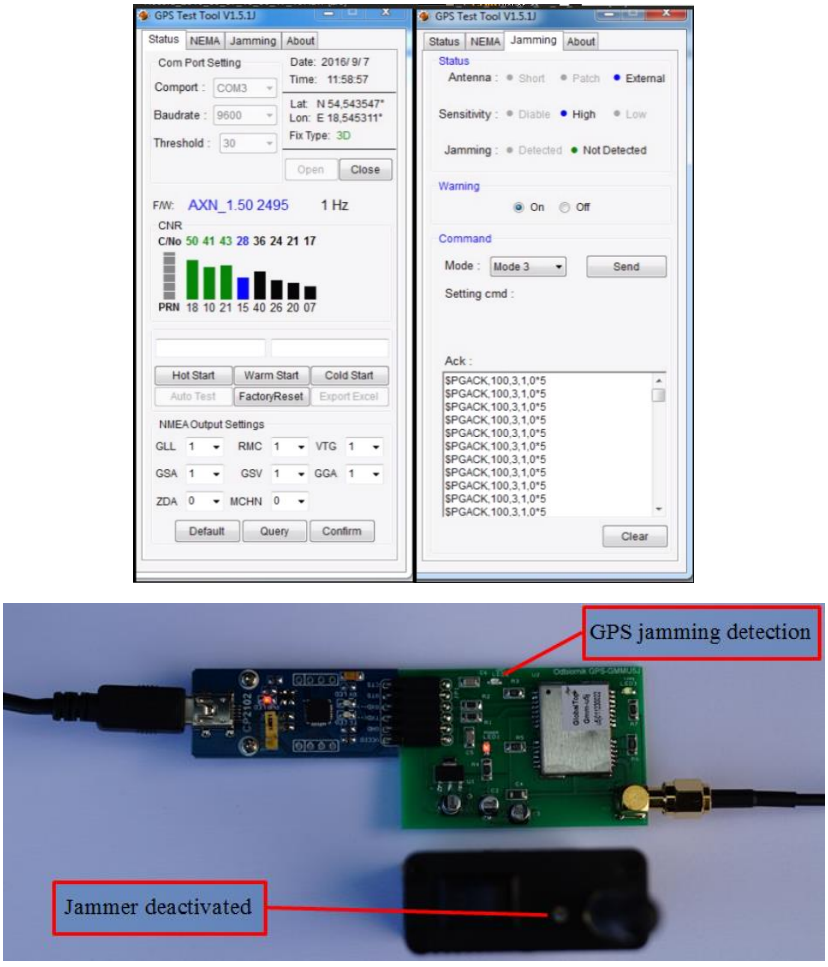

Fig. 14. Functioning receiver and 'GPS Test Tool' visualization

After the receiver was constructed, its implemented functions connected with jamming were tested. In testing, two devices were utilized, GX-40B by TTS and a jammer by Spy Electronics LTD, as shown in the Figure 15.

Fig. 15. GX-40B by TTS jamming device and Spy Electronics LTD jamming device

After detecting jamming the receiver changes the status to high on output 2 (pin 2) which results in a diode lighting up symbolizing interference, as shown in Figure 16.

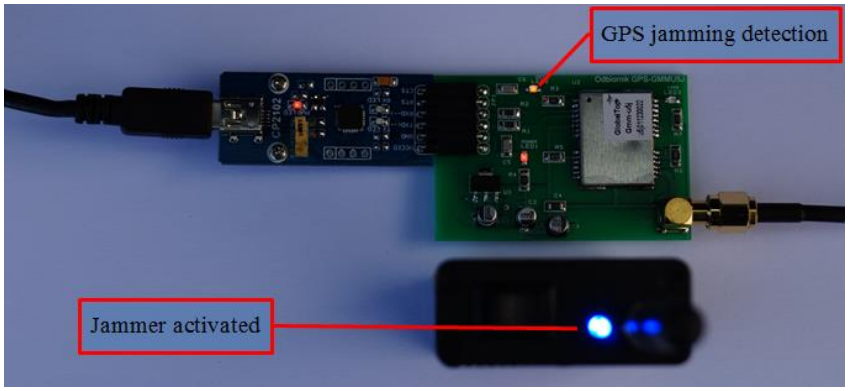

Fig. 16. Diode jamming detection and report

Additionally, the GPS Test Tool has a function which switches the receiver into jamming detection mode. In case of discovering interference using the NMEA protocol, a message is sent, which results in an icon popping up symbolizing interference detection, as shown in Figure 17.

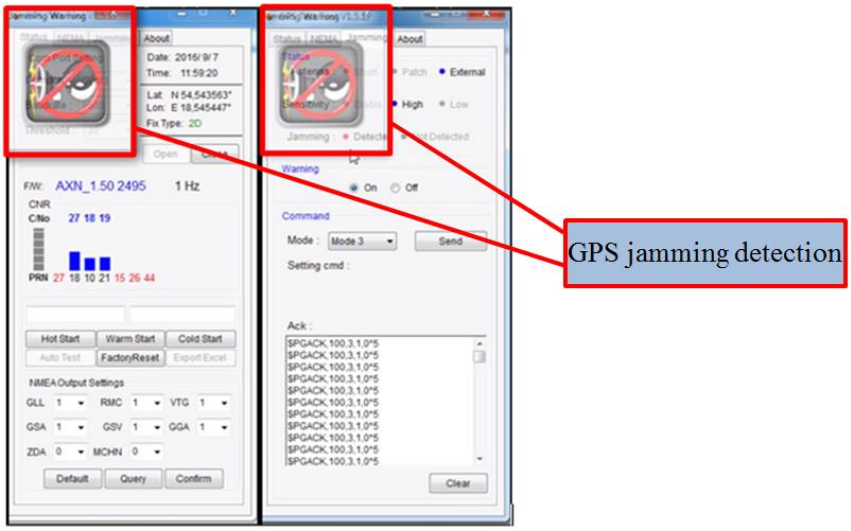

Fig. 17. 'GPS Test Tool' jamming visualization

CONCLUSIONS

Society has become dependent on satellite systems which are utilized in many fields of our lives. There are several threats where a lack of satellite signal can cause a catastrophe. One of these threats is jamming. It can be used by civilians and by the military. They can be used by employees to protect against surveillance, or much worse by crime groups for grand theft auto or by terrorist organizations. Jamming has caused insurance companies to have lower statistics in stolen car recovery.

To successfully combat jamming we must know that the lack of position location in receivers is caused by jamming. Some receivers have jamming detection functions. Detecting the source of interference, one can disable it so that all devices using satellite signals could operate properly in the area of operation of such interference generator.

REFERENCES

[1] Figurski M. et al., Influence of interference in GPS measurements, GPS vs. jamming, 'Geodeta', 2011, No. 01, pp. 46–51, [online], https://geoforum.pl/upload/review/file/188_s46_51_z.pdf [access 24.08.2016].

[2] Specht C., System GPS, Publ. Bernardinum, Pelpin 2007.

[3] http://ascenkor.img.or.kr/downloads/Ascen%20Module%20Application%20Note%20-A10.pdf, [access 08.09.2016].

[4] http://ascenkor.img.or.kr/downloads/AscenKorea-AKMU5J-Datasheet-V0H.pdf, [access 08.09.2016].

[5] http://download.maritex.com.pl/pdfs/wi/GPSGMMU5J.pdf [access 26.08.2016].

[6] http://www.gps.gov/technical/icwg/IS-GPS-200H.pdf [access 08.09.2016].

[7] http://www.jammer4uk.com/high-power-8-antenna-3g4gltewimaxcell-phonegpswifi-jammer-p-48.html [access 24.08.2016].

[8] http://www.jammerall.com/products/Vehicle-Car-Anti-Tracker-Mini-GPS-Jammer-Blocker.html [access 24.08.2016].

[9] http://www.novatel.com/products/gnss-antennas/gajt-anti-jam-antennas/gajt-710ms/ [access 26.08.2016].

[10] http://www.sesp.com [access 08.09.2016].

[11] http://www.sesp.com [access 08.09.2016].

Received November 2016
Reviewed December 2016

SŁAWOMIR ŚWIERCZYŃSKI
Polish Naval Academy
Śmidowicza 69 Str., 81-127 Gdynia, Poland
e-mail: s.swierczynski@amw.gdynia.pl

PIOTR ZWOLAN
Polish Naval Academy
Śmidowicza 69 Str., 81-127 Gdynia, Poland
e-mail: p.zwolan@amw.gdynia.pl

ILONA RUTKOWSKA
Polish Naval Academy
Śmidowicza 69 Str., 81-127 Gdynia, Poland
e-mail: ir48@wp.pl

STRESZCZENIE

Systemy satelitarne uzależniły cały świat i są wykorzystywane niemal we wszystkich dziedzinach życia gospodarczego i społecznego, w transporcie, bankowości, przemyśle, rolnictwie itp. Rozwój technologii spowodował, że większość smartfonów, które używamy, ma wbudowany odbiornik GNSS, w wielu samochodach montowana jest nawigacja,

a wszystkie jednostki pływające korzystają z odbiornika GNSS lub kompasu satelitarnego. Uzależnienie od systemów, które pracują na podobnych częstotliwościach, może być wykorzystane w celu zakłócenia (jamming) lub przejęcia kontroli (spoofing) nad systemami satelitarnymi. Takie celowe zakłócenia mogą być bardzo szkodliwe dla użytkowników (społeczeństwa). W artykule opisano zjawisko jammingu oraz przedstawiono jedno z rozwiązań konstrukcyjnych odbiornika umożliwiającego detekcję sygnału zakłócającego. Odbiornik ten został zaprojektowany oraz zbudowany przez autorów artykułu.