UDK:621.396.96(047)=861
COSATI: 17-07, 17-02, 17-04

Jamming of GNSS Signals

Ivan Pokrajac[1)]
Nadica Kozić[1)]
Ana Čančarević[2)]
Radiana Brusin[1)]

GNSS technology has been used for many applications. Beside military applications, GNSS technology is used for mini UAVs – drones. One of the possible approaches for achieving anti-drone capabilities is a jamming receiver of GNSS at drone. The GNNS jammers broadcast jamming signal in the frequency band used for satellite navigation in order to deny service of GNSS. In this paper we have considered the possibility to generate optimal jamming signal to deny service of all GNSS. Some of the results are shown in this paper

Key words: **global navigation system, satellite system, jamming, signal generating, wideband signal, measurement results.**

Introduction

THE Global Navigation Satellite Systems (GNSSs) are used in many applications, either for commercial purpose, either in military applications. GNSS is a standard generic term for satellite navigation systems that provide autonomous geo-spatial positioning of a receiver with global coverage. Nowadays, there are three main GNSSs: *GPS* from the United States, *Glonass* from Russia and the European Union has *Galileo.* China is expanding their regional *Beidou* [1]. They all work almost in the same way and provide ability to continuously determine positions of the objects (receivers of GNNS signals).

In the last decade there is an expansion of the mini unmanned aerial vehicles (UAVs) – drones. Nowadays, they have been used in many areas (aerial photography, traffic monitoring, disaster monitoring, etc). Nevertheless, the increasing use of drones poses great threats to public security and personal privacy. For example, an attacker might strap explosives or other dangerous materials to a drone to carry out an attack, an example is a mass drone attack on Syrian base; criminals can use drones to smuggle illicit materials across borders; an operator can control a drone carrying a high-fidelity camera to fly over walls and spy on inhabitant's private information. The increasing frequency of incidents caused by drones makes it necessary to deploy anti-drone systems [2].

For autonomous or semi-autonomous operation, drones demand reliable navigation, so one of the possible approaches for achieving anti-drone capabilities is a jamming receiver of GNSS at drone. GNSS jammers are usually small portable devices able to broadcast disruptive signals in the GNSS bands. A jammer can overpower the much weaker GNSS signals and disrupt GNSS-based services in a geographical area with a radius of several kilometers [3]. Typically, the jamming signal deteriorates the position solution or induces total loss of lock of the GNSS signals.

In this paper, effects of GNSS jammer on GNSS receiver are presented. Signals broadcasted by GNSS jammer are characterized by linear frequency modulations: the instantaneous frequency of the signal sweeps a range of several MHz in a few microseconds affecting the GNSS receiver, which leads to deteriorated position thus making navigation unreliable.

This paper consists of six parts. Introduction is given in Section I. Concept of GNSS is given in Section II. Principle of jamming GNSS signals is given in Section III. In Section IV, types of jamming signals are presented and obtained results are given in Section V. Conclusions are given in Section VI.

Basic concept of GNSS

GNSS-based positioning has an essential role in modern society. Reliable navigation functionality is an imperative in more and more applications nowadays on land, sea and air [4]. Several infrastructures rely on GNSS-based positioning, hence GNSS can provide reliable and continuous services [5]. A major dependency to reliable localization has been emerging, especially within safety-critical applications.

The basic GNSS concept is shown in Fig.1, which illustrates the five steps involved in using GNSS to determine time and position, then applying this information [6].

[1)] Military Technical Institute (VTI), Ratka Resanovića 1, 11132 Belgrade, SERBIA
[2)] University of Defense, Military Academy, Pavla Jurišića Šturma 33, 11000 Belgrade, SERBIA
Correspondence to: Ivan Pokrajac; e-mail: ivan.pokrajac@vs.rs

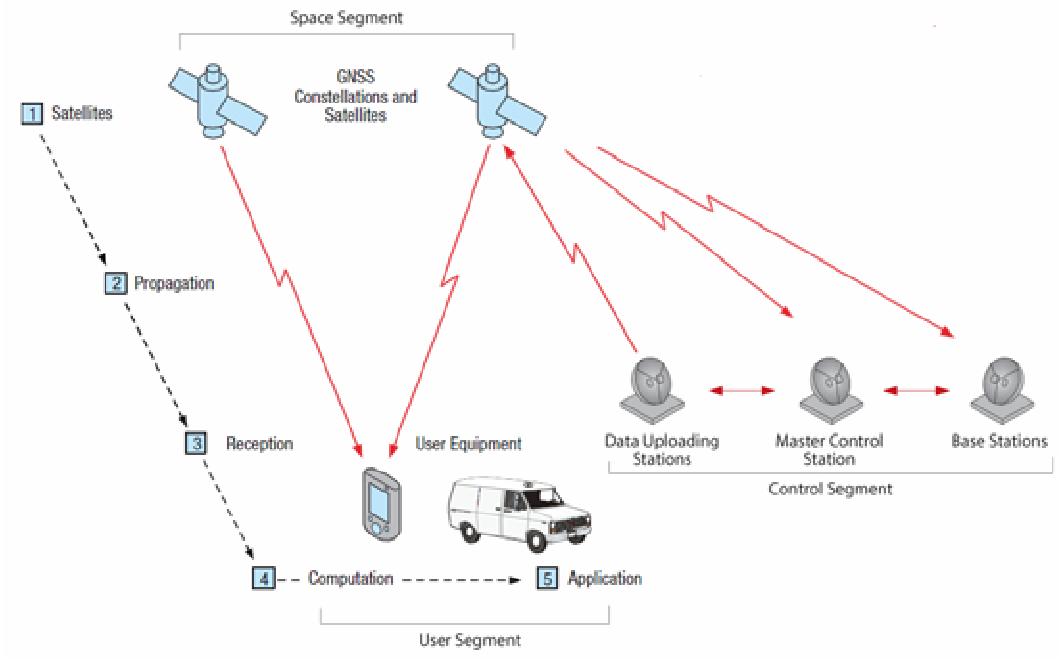


Figure 1. Basic concept of GNSS

Main GNSSs are GPS, Galileo and Glonass. Each of them consists mainly of three segments: (a) space segment, (b) control segment and (c) user segment, Fig.1 [6].

The space segment consists of GNSS satellites, orbiting above 20.000 km above the Earth. Each GNSS has its own constellation of satellites, arranged in orbits to provide desired coverage. Each satellite in a GNSS constellation broadcasts a signal that identifies it and provides its time, orbit and status.

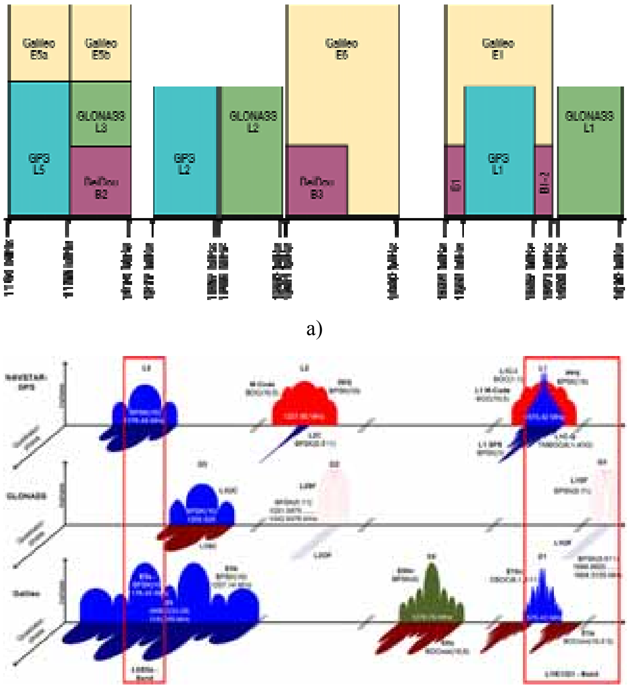
Control segment comprises a ground-based network of master control stations, data uploading stations and monitor stations; in case of GPS two master control stations, four data uploading stations and ten monitor stations, located throughout the world.

User segment consists of equipment that processes the received signals from the GNSS satellites and uses them to derive and apply location and time information. The equipment ranges from handheld receivers used by hikers to sophisticated, specialized receivers used for high-end survey and mapping applications.

GNSS receivers are able to compute their Position Velocity and Time (PVT) using the trilateration technique and exploiting the signals transmitted by different satellites. Receiver needs at least four satellites to obtain a position. This means there needs to be a line of sight between the receiver's antenna and the four satellites. The distance between receiver and satellite antennas is usually in the order of 20000 km. The use of more satellites, if they are available will improve the position solution.

Each satellite system has specific signal characteristics, but each system attempts to be compatible with the others in order to prevent the interferences and attenuation between the signals. It is important to consider that the processing of all signals should be performed using the same receiver, thus a complex receiver design is supposed to be designed and built [7].

GNSS radio signals are quite complex. Their frequencies are around 1.5 GHz. The GNSS frequency plan shall respect the radio-regulations as they are discussed and agreed on at ITU forums. The available spectrum which can be used for the development of Radio-Navigation Satellite Systems (RNSS) is shown in Fig.2a. Spectrum of GNSS signals is shown in Fig.2b.



a)

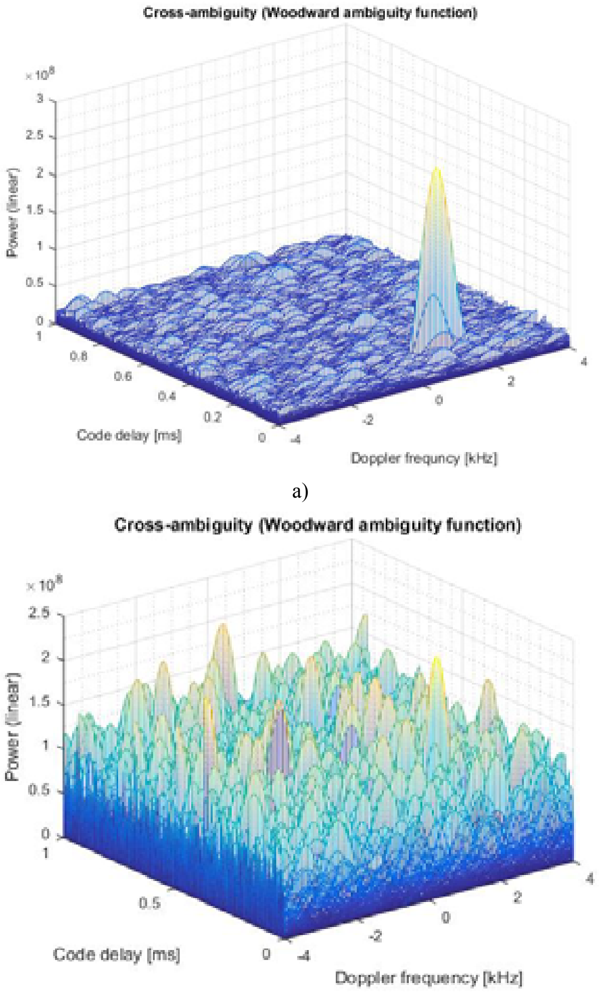
b)

Figure 2. a) GNSS frequency plan, b) spectrum of GNSS signals

Due to the long satellite–receiver distance, by the time GNSS signals reach the ground they have very low minimum received power. These vulnerabilities can be exploited, either intentionally or unintentionally, and cause GNSS signal to become unavailable in a given geographical area.

3. Jamming of GNSS

In most cases, the basic goal of intended jamming of GNSS signals is to deny GNSS-based services in an area of interest. In this case systems are not able to give GNSS services and process of navigation or time synchronization is blocked. However, this is possible using strong power jammer, which can be clearly detectable and modern systems are able to switch to the other sub-system for navigation, such as inertial navigation systems. The second concept can be based on the use of some intermediate power values for jammer. In this concept GNSS receivers are still able to provide acquisition and locking to corresponding GNSS signals but estimation of position is inaccurate. Power of jammer signals is severe enough to decrease GNSS receiver performances.



a)

b)

Figure 3. a) CAF in the presence of GNSS signal GPS L5; b) CAF in the presence of GNSS signal GPS L5 and jamming signal

The impact on the different stages of the receiver is briefly discussed in [8]. Other examples of impact assessment of interference on GNSS receivers can be found in [4, 9, 10]. One of the possible impacts is in the acquisition stage of the GNSS receiver. In the GNSS receivers the digital signal processing stage starts in the acquisition block. The role of acquisition block is to determine the signal presence and to provide a rough estimate of the signal code delay and Doppler frequency [11]. In the acquisition block correlation of the received signal as an input signal with corresponding pseudo random noise (PRN) sequences is performed. Results of this operation are cross-ambiguity function (CAF). The CAF is a function of the Doppler frequencies and code delays. When the GNSS signal is present and in the absence of interference, a single dominant peak should appear in the CAF as is shown in Fig.3a. Position of this single peak corresponds to the signal code delay and Doppler frequency.

In the case when jamming signal is present there is no single dominant peak in the CAF as shown in Fig.3b. Results of CAF, presented in Figure 3 are calculated based on L5 GPS signal for PRN of 30th satellite cross-correlated with replica of this signal time delayed and frequency shifted.

The signals detected by the acquisition stage are passed to the tracking block which is responsible for providing fine estimates of the signal parameters. These estimates are used to generate GNSS measurements such as pseudoranges, carrier phases and Doppler shifts. Jamming has a direct consequence on the quality of the measurements produced by the tracking stage causing increased measurement variances, biases and measurement outliers.

Provided that the interfered signal can still be processed by both acquisition and tracking stages, the GNSS receiver would be able to output an estimation of the position, which will be degraded by the fact that it will be based on interference-affected pseudoranges.

Jamming signals

The jamming signal may deteriorate the position solution or induce totally loss of lock of the satellite signals. Different receivers react differently to jamming - also the effect depends on the properties of the jamming signal. The basic principles of GNSS receivers are however fairly similar, but the internal processes and algorithms vary and certain filtering may mitigate the effect of the jammer on the positioning accuracy and availability. In all receivers, intentional GNSS jamming affects the signal-to-noise-ratio (SNR) of the received signals. The effect can be observed somewhat similarly as the phenomenon perceived in the context of multipath propagation or general signal attenuation due to for example foliage: the SNR decreases and the signals become weaker. When the signal is weak enough, the receiver cannot generate ranging measurements anymore and the position solution cannot be computed. [12]

Jamming signal can be characterized by its center frequency and by its power described as jamming-to-signal ratio (J/S) in dB. The J/S decreases with the distance from the jammer to the receiver [1].

GNSS is very tolerant of pulsed radio frequency interference (RFI), even if it is very powerful, because the pulses are usually short in comparison to the duration of a GPS or Glonass data bit, which is 20ms. On the other side GNSS has a difficulty to handle continuous RFI whether it is broadband or narrowband or tone interference [13]. But the spread spectrum can attenuate narrowband RFI in the correlation process [14].

In most modern jammers it is possible to generate different jamming signals and to produce different jammer waveforms. Difference between jammer signal and jammer waveform is that waveform consists of more jammer signals that represent a sequence of jamming signal of interest. The basic jamming signal in modern jammers is a pulsed RF signal. The RF pulse is generated at specific central frequency. Time length of each pulse is τ seconds and is repeated every T seconds. In the frequency domain this RF pulse is the mathematical function sin(x)/x and the spectrum of an RF pulse consists of spectral lines centered on central frequency and spaced $1/T$ Hz apart. These components are called the spectral lines of the RF pulse. A sweep wave is build up by generating a series of N pulsed RF signals, each with a different central frequency, from f_{START} to f_{STOP}. Length of the sweep wave is defined as $T=N\tau$. The complex envelopes of the jamming signal can be given by:

$$s(t) = A(t)\cdot\exp\left(j2\pi\int f(t)dt\right) \qquad (1)$$

where $f(t) = f_C + kt$ represents instantaneous frequency of the signal, f_C is central frequency and k is sweep rate, $A(t)$ is amplitude of the signal. Usually, amplitude of the signal is constant during the time period of T, and the complex envelopes of the jamming signal can be given by

$$s(t) = A\cdot\exp\left(j2\pi\left(f_C+\frac{k}{2}t\right)t\right), \forall 0 \le t \le T \qquad (2)$$

Previous equation describes sweep signal that occupied one frequency bandwidth of interest at central frequency. In many application of electronic attack, it is necessary to cover wider frequency bandwidth with jamming signals in order to block communication. The coverage of wider frequency bandwidth can be achieved by generating jamming waveform based on the use of Time Division Multiplexing (TDM). Using TDM, it is possible to generate different RF pulses or sequences of RF pulses at different central frequencies and different frequency bandwidths. For example the waveform of M slots in TDM assumes that there is M different jamming signals generated at different central frequencies. In this case the complex envelopes of the jamming signal can be given by:

$$s(t) = \begin{cases} A\cdot\exp\left(j2\pi\left(f_{C_1}+\frac{k_1}{2}t\right)t\right), \forall 0 \le t \le T \\ A\cdot\exp\left(j2\pi\left(f_{C_2}+\frac{k_2}{2}t\right)t\right), \forall T_1 \le t \le T_2 \\ \vdots \\ A\cdot\exp\left(j2\pi\left(f_{CM}+\frac{k_M}{2}t\right)t\right), \forall T_{M1} \le t \le T_M \end{cases} \qquad (3)$$

where f_{CM} is M-th central frequency and k_m is sweep rate at *m-th* central frequency.

Signal spectrum of jamming waveform based on the use of TDM is shown in Fig.4. In this case there are three time slots. In the first time slot frequency band from 1559 MHz to 1591 MHz is jammed, in the second time slot frequency band from 1593 MHz to 1610 MHz is jammed, and during the third time slots the band from 1550 MHz to 1620 MHz is jammed. By using this jamming waveform it is possible to deny usage of GPS L1, GLONASS G1 and Galileo E1.

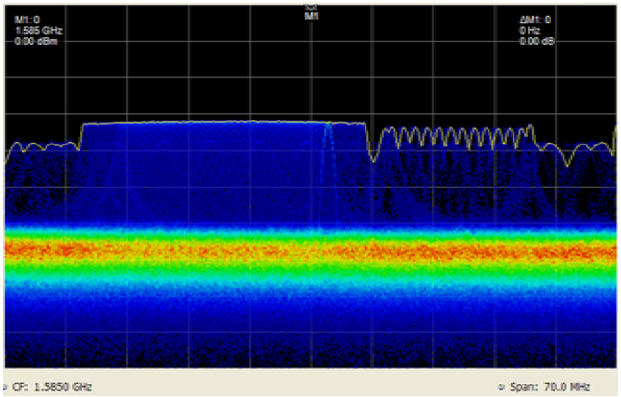


Figure 4. Power spectrum of jamming signal

System model

The primary components of the GNSS user segment are antenna and receiver, as shown in Fig.5. Depending on the application, the antenna and receiver may be physically separate or they may be integrated into one assembly. GNSS antenna receives the radio signals that are transmitted by the GNSS satellites and sends these signals to the receiver. Using a PC as user equipment, navigation data from GNSS receiver are collected for further analysis.

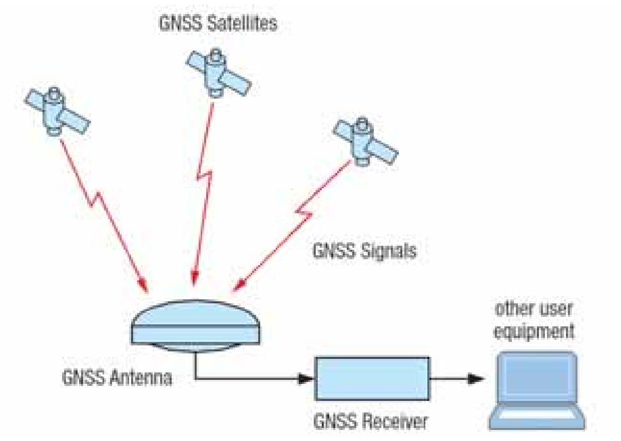


Figure 5. Components of the GNSS user

In this system model jamming signal is superposed with GNSS signals at the antenna of GNSS receiver. The aim of this system model is to show that by using jamming waveform based on TDM, it is possible to successfully jam receivers of GNSS, and that it is not necessary to jam continuously all frequency bands of interest (Fig.2). In our experiments two different GNSS receivers are used. These receivers are part of different military equipment.

For the first receiver, three scenarios of jamming are tested. In the first two scenarios jammer covers GPS L1, L2 and L5 bands using jamming waveform based on TDM. The parameters of multi-sweep, consisting of three sweep signals, are shown in Table 1. Durations of time slots within multi-sweep are equal. Different durations of time slots are used in different multi-sweeps. In these scenarios, in different multi-sweeps, three different duration of timeslots are used: 5µs, 200µs and 999µs.

Table 1.

Bands	Center frequency [MHz]	Bandwidth [MHz]
L1	1576	31
L2	1228	31
L5	1176	31

In the third scenario jammer covers only GPS L1 band. In this case, sweep parameters correspond to parameters for L1 band from Table 1. Duration of time slots within sweep is 30µs.

The second GNSS receiver gets signals from two GNSSs, GPS and Glonass, so jammer covers all bands from both. Durations of time slots in different multi-sweeps are 100 µs, 200µs, 500µs and 999µs. In both cases and in all scenarios jammer to noise ratio (J/N), has been set to be equal.

Results

Positioning solutions were analyzed with and without the jammer. The receiver had a decreased performance in the presence of jamming. The position solution was not available during the entire time of experiment.

Figures 6 and 7 show on diagrams the results of positioning accuracy of GNSS with and without jamming when the jammer is set with parameters from scenario 1. Durations of time slots are shown in the figures.

The center position on diagrams (x and y coordinates are zeros) presents the exact position of GNSS receiver. Positioning accuracy is presented through x and y coordinates in meters.

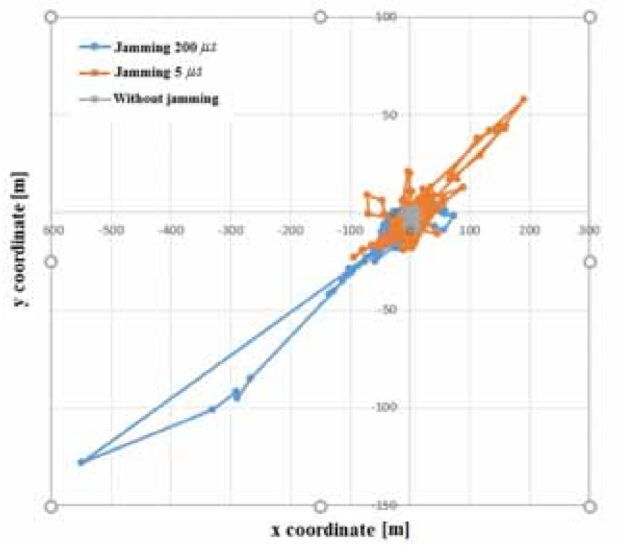


Figure 6. Positioning accuracy

Positioning based on GNSS service without jamming is accurate within a few meters. The actual error in the position domain is strongly dependent on the positioning algorithm employed, and a general rule to quantify the performance degradation in terms of positioning error is hard to be found. From Figures 6 and 7 it can be concluded that positioning based on GNSS service when jamming waveform is based on TDM has worse accuracy than when jammer is set with parameters from scenario 3 (in Fig.8 the results of positioning accuracy of GNSS with and without jamming are shown). Also, from the figures, it can be noticed that positioning depends on durations of time slots within multi-sweep.

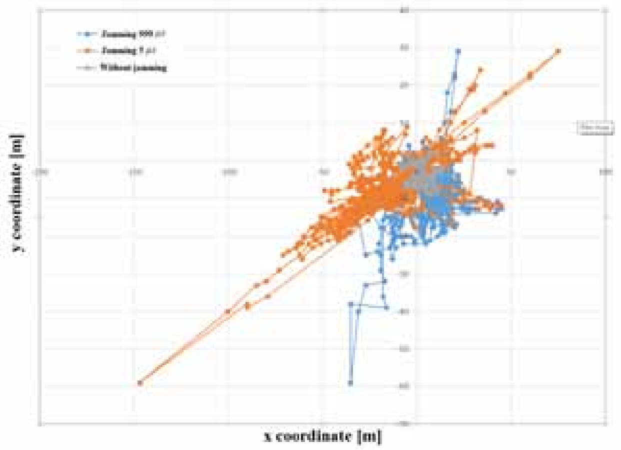


Figure 7. Positioning accuracy

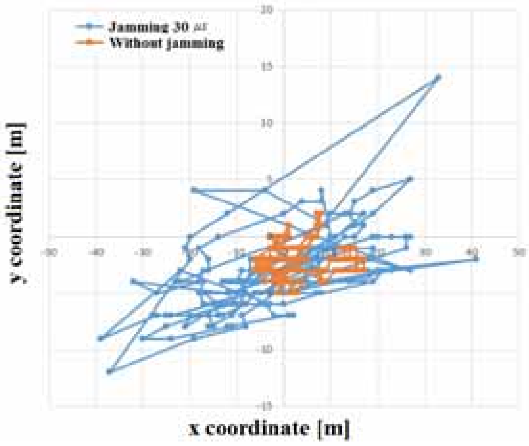


Figure 8. Positioning accuracy

In Figures 9 and 10, on diagrams, the results of positioning accuracy of latitude and longitude of GNSS for the second receiver are shown, with and without jamming.

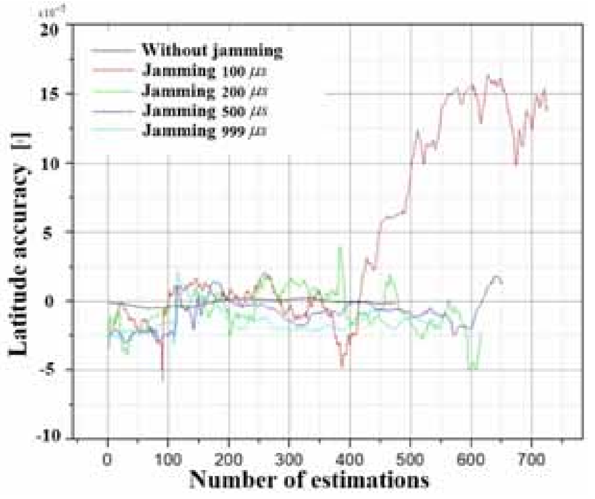


Figure 9. Positioning accuracy - latitude

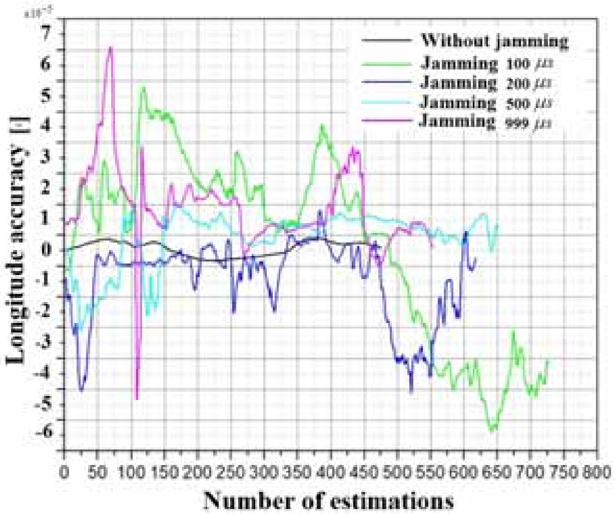


Figure 10. Positioning accuracy – longitude

As expected, from the figures it can be concluded that worse positioning accuracy is obtained when the jamming is present than when GNSS positioning is done without jamming. Also, it can be noticed from the figures that positioning depends on durations of time slots within multi-sweep.

Typically, the jamming signal deteriorates the position solution or induces total loss of lock of the GNSS signals depending on the perceived J/S at the receiver.

Conclusion

Use of drones poses great threats to public security and personal privacy. For autonomous or semi-autonomous operation, drones demand reliable navigation, so one of the possible approaches for achieving anti-drone capabilities is jamming GNSS at drone.

Jammers broadcasting a strong power are easily detectable. The ones broadcasting an intermediate power are more dangerous, as they can decrease the receiver's performance without making it lose lock or prevent the acquisition of the satellite signals. This paper illustrated the fact that accuracy and signal availability were considerably compromised when jamming waveform is based on TDM.

References

[1] DA SILVA,D.A.M.Č.: *GPS Jamming and Spoofing using Software Defined Radio*, University Institute Of Lisbon, Department Of ISTA, PORTUGAL, 2017.

[2] XIUFANG,S., CHAOQUN,Y., WEIGE,X., CHAO,L., ZHIGUO,S., JIMING,C.: *Anti-Drone System with Multiple Surveillance Technologies: Architecture*, Implementation, and Challenges, IEEE Communication Magazine, April 2018, pp.68-74.

[3] BORIO,D., O'DRISCOLL,C., FORTUNY,J.: *GNSS Jammers: Effects and countermeasures*, 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing, Noordwijk, 2012, pp. 1-7.

[4] BHUIYAN,M.Z.H., KUUSNIEMI,H., SODERHOLM,S., AIROS,E.: *The Imact of Interference on GNSS Receiver Observables – A Running Digital Sum Based Simple Jammer Detector*, Radioengineering, September 2014, Vol.23, No.3, pp. 898-906.

[5] BORIO,D., GIOIA,C., DIMC,F., BAŽEC,M., FORTUNY,J., BALDINI,G., BASSO,M.: An Experimental Evaluation of the GNSS Jamming Threat, 24th Electrotechnical and Computer Conference ERK 2015, Portorož, SLOVENIJA, September, 2015, Vol.A, pp. 269-272.

[6] JEFFREY,C.: *An introduction to GNSS – GPS, GLONASS Galileo and other Global Navigation Satellite Systems*, NovAtel Inc, Calgary, Alberta, CANADA, 2015, First edition.

[7] http://gpsworld.com/multi-constellation-dual-frequency-single-chip/

[8] BORIO,D., DOVIS,F., KUUSNIEMI,H., PRESTI,L.Lo: *Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers*, Proceedings of the IEEE, June 2016, Vol.104, No.6, pp. 1233-1245.

[9] DOVIS,F.: *GNSS Interference Threats and Countermeasures*, Norwood, MA, USA: Artech House, 2015.

[10] WILDEMEERSCH,M., PONS,E.C., RABBACHIN,A., GUASCH,J.F.: *Impact study of unintentional interference on GNSS receivers, European Commission*, Joint Researh Centre, JRC Scientific and Technical Reports, 2010.

[11] KAPLAN,E.D., HEGARTY,C.: *Understanding GPS: Principles and Applications*, Mobile Communications, Norwood, MA, USA: Artech House, 2015.

[12] KUUSNIEMI,H., AIROS,E., ZAHIDUL,M., BHUIYAN,H., KROGER,T.: *Effect of GNSS jammers on consumer grade satellite navigation receivers*, Proceedings of the European Navigation Conference (ENC), Gdanks, POLAND, April 2012, pp. 1-14.

[13] MISRA,P., ENGE,P.: *Global positioning system. Signals, Measurement, and Performance*, Ganga-Jamuna Press, Lincoln, Massachusetts, USA, 2012.

[14] GLOMSVOLL,O.: *Jamming of GPS & GLONASS signals*, Nottingham geospatial institute, department on civil engineering, Nottingham, GB, September 2014.

Received: 03.04.2018.
Accepted: 12.10.2018.

Ometanje signala globalnih navigacionih satelitskih sistema

Tehnologija globalnih navigacionih satelitskih sistema ima široku primenu. Osim za vojne primene, tehnologija globalnih navigacionih satelitskih sistema se koristi i za funkcionisanje mini bespilotnih letelica – dronova. Jedan od mogućih pristupa za borbu protiv dronova je ometanje prijemnika globalnih navigacionih satelitskih sistema na dronu. Ometači globalnih navigacionih satelitskih sistema emituju ometački signal u frekvencijskom opsegu koji se koristi za satelitsku navigaciju kako bi se onemogućio servis globalnih navigacionih satelitskih sistema. U ovom radu razmatrana je mogućnost generisanja optimalnog ometačkog signala za onemogućavanje servisa svih globalnih navigacionih satelitskih sistema. Dobijeni rezultati su prikazani u radu.

Ključne reči: **globalni navigacioni sistem, satelitski sistem, ometanje, generisanje signala, širokopojasni signal, rezultati merenja.**

Интерференция сигналов глобальных навигационных спутниковых систем

Технология глобальных навигационных спутниковых систем имеет широкое применение. Помимо военных применений, технология глобальных навигационных спутниковых систем также используется и для эксплуатации мини-беспилотных летательных аппаратов - дронов. Одним из возможных подходов к борьбе с беспилотниками является вмешательство в приёмники глобальных навигационных спутниковых систем на дронах. Детекторы глобальных навигационных спутниковых систем передают сигнал помех полосы пропускания в полосе частот, используемой для спутниковой навигации, чтобы отключить обслуживание глобальных навигационных спутниковых систем. В данной статье рассматривается возможность генерации оптимального сигнала помех для отключения обслуживания всех глобальных навигационных спутниковых систем. Полученные результаты приведены в статье.

Ключевые слова: **глобальная навигационная система, спутниковая система, помехи, генерация сигнала, широкополосный сигнал, результаты измерений.**

Perturbation des signaux chez les systèmes globaux de navigation satellite

La technologie des systèmes globaux de navigation satellite est utilisée largement. A part les emplois militaires la technologie des systèmes globaux de navigation satellite s'utilise aussi pour le fonctionnement des aéronefs mini sans pilotes – les drones. Une approche possible pour la lutte contre les drones est la perturbation des récepteurs de ces systèmes de navigation chez le drone. Les perturbations des systèmes globaux de navigation satellite émettent le signal de perturbation dans le domaine fréquentiel qui s'utilise pour la navigation satellite pour empêcher le service des systèmes globaux da navigation satellite. Dans ce travail on a considéré la possibilité de la création du signal optimal de perturbation pour l'empêchement du service de tous les systèmes globaux de navigation satellite. Les résultats obtenus sont présentés aussi dans ce travail.

Mots clés: **système global de navigation, système satellite, perturbation, création des signaux, signal de grande portée, résultats de mesurage.**