doi: 10.5028/jatm.v10.870

GPS Jamming Signals Propagation in Free-Space, Urban and Suburban Environments

Lester de A. Faria[1], Caio A. de Melo Silvestre[1], Marcelino A. Feitosa Correia[1], Nelson A. Roso[1]

Faria LA http://orcid.org/0000-0003-1785-446X
Silvestre CAM http://orcid.org/0000-0002-8740-7625
Roso NA http://orcid.org/0000-0002-7178-8224

How to cite

Faria LA; Silvestre CAM; Correia MAF; Roso NA (2018) GPS Jamming Signals Propagation in Free-Space, Urban and Suburban Environments. J Aerosp Tecnol Manag, 10: e0618. doi: 10.5028/jatm.v10.870.

ABSTRACT: GPS-based systems have been widely used in different critical sectors, including civilian, military and commercial applications. Despite of being able to provide great benefits, under certain circumstances they show to be highly vulnerable to intentional interferences. In this context, this article aimed to evaluate the vulnerability range of this kind of systems, focusing on different kinds of environments and based on different propagation models, to which the simulations were performed. Results show high vulnerabilities of GPS-based systems even when operating in a well-protected urban environment, in a short range and under low-power sources of radiation. Graphs are presented with the range of effectiveness for different power levels of jammer in different situations. Evaluations are performed not only for the acquisition but also for the tracking processes of the GPS receivers, therefore being possible to establish a safe operation range for having a trustful GPS signal and mitigate malicious actions. The comparisons allow, as well, highlighting the importance of using the correct propagation model, in order to achieve consistent results, depending on the desired situation.

KEYWORDS: GPS Receivers, Jamming, Vulnerabilities, Propagation models, Friis equation, COST-231 Hata model.

INTRODUCTION

Global Navigation Satellite Systems (GNSS) are currently being used to provide estimations of Position, Navigation and Timing (PNT) to all users that have a receiver and a line of sight to, at least, four satellites.

Considering the current existing GNSS, the best known one is the Global Positioning System (GPS), or NAVSTAR-GPS (Satellite Navigation with Time And Ranging), from the US Department of Defense (DoD). It was the first GNSS system fully available to the users, through the creation of a constellation of satellites. Other systems already in operation, or under development, are: the Russian GLONASS (Global Navigation Satellite System); the European GALILEO (Global European Navigation Satellite System); and the Chinese BNS (Beidou Navigation System) (Bakker 2006).

The GPS system supports critical applications for military, civilian and commercial users worldwide, having the USA government as its main sponsor. To date, it shows accessible to any operator through the use of simple GPS receivers. Currently, 14 of 16 critical infrastructure sectors have crucial dependencies on GPS signals (navigation, precision agriculture, financial market, communication, etc.). Even in military, where this dependency is not so clear, systems like Emitters Locating, Safe Communication and Multi-Static Radars depend on the time or frequency provided by GPS signals (Scott 2015).

[1] Departamento de Ciência e Tecnologia Aeroespacial – Instituto Tecnológico de Aeronáutica – Divisão de Engenharia Eletrônica – São José dos Campos/SP – Brazil

Correspondence author: Lester de A. Faria | Departamento de Ciência e Tecnologia Aeroespacial – Instituto Tecnológico de Aeronáutica – Divisão de Engenharia Eletrônica | Praça Marechal Eduardo Gomes, 50 – Vila das Acácias | São José dos Campos/SP – Brazil | Email: lester@ita.br

Received: May 29, 2017 | **Accepted:** Oct. 05, 2017

Section Editor: Cynthia Junqueira

Due to the high reliability and accuracy suggested by the GPS, operators tend to consider the GPS-based systems as safe and perennial, not thinking in a possible loss of the signals during operations and/or the consequences/impacts that it may have for the proper functioning of the GPS-based systems as a whole.

Unlike the encrypted GPS signals used by the US Department of Defense (DoD), which can be authenticated before using, the civilian GPS signals (C/A code) were never intended for safety- and security-critical applications. However, GPS PNT signals keep increasingly widely disseminated and used in both civilian and military applications, without any kind of countermeasure to eventual threats.

Recent events made clear that intentional interference to GPS are real threats to both military and civilian systems. These potential vulnerabilities have been previously demonstrated in experiments performed in the Electronic Warfare Laboratory of Technological Institute of Aeronautics (ITA) (Silvestre 2014; Correia 2015; Faria *et al.* 2016) and in some other few publications found in literature (Cavaleri *et al.* 2010; Ledvina *et al.* 2010, Motella *et al.* 2010).

Currently, in internet, it is very easy to find not only jamming but also spoofing equipment available for buying. These equipments are not so expensive, being available in any quantity that one needs. Besides, a several number of tutorials can be found on websites and YouTube, teaching how to spoof and jam vectors, especially drones. It is just to "google it" and one finds security experts raising alarm over how to hack drones (Russon 2015).

Some countries are already aware of this type of threat (The Royal Academy of Engineering 2011), highlighting the need to take account of these vulnerabilities of GPS-based systems. However, the effects of the interfering signal propagation in different kinds of environment are not completely defined, nor studied, in open sources found in literature, leaving a gap of knowledge for those researchers who work with this kind of subject, especially when dealing/operating with/in more complex environments, such as urban and suburban surroundings. This theme seems to be fundamental not only for the establishment of a situational awareness but also for providing mitigation of eventual attacks and for an analysis of the efficiency of a jammer in complex environments.

Finally, it is important to highlight that all the considerations here provided/established for GPS signals propagation are easily extended for other GNSS systems, just by considering the proper signal carrier frequency, and applying the respective mentioned equations. For a question of simplicity, the results, in which this work relies, will be presented only for the GPS system.

THEORETICAL BASIS

GPS SYSTEMS

The GPS system provides position and timing information anywhere on the globe, since the receiver has a line of sight to four or more satellites. For that, right-circularly polarized waves are continuously emitted in three carrier frequencies, the L1, L2 and L5 (respectively 1575.42 MHz, 1227.6 MHz and 1176.45 MHz), where the latter is not fully operational yet.

The L1 and L2 carriers are modulated with PRN (Pseudorandom Noise) codes and with a BPSK (Binary Phase Shift Keying) modulation. Two PRN codes modulate the L1 frequency: the C/A code (coarse/acquisition clear code) and the encrypted P(Y) code (precision code). The C/A codes are available for civilian and military users, while the P(Y) code is for the exclusive use of the USA military and for those who have previous authorization of the US DoD (Balvedi 2006). In addition to the PRN codes, navigation data also modulates the L1 and L2 carriers, providing the basic information for calculating the positions of satellites and estimating the receiver position on the globe. L1 signal is defined as:

$$S_{L1} = A_P.P(t).D(t).\cos(2.\pi.f_1.t + \varphi) + A_C.C(t).D(t).sen(2.\pi.f_1.t + \varphi) \tag{1}$$

where S_{L1} is the frequency of the L1 signal, A_P is the amplitude of the P(Y) code, $P(t)$ is the phase of the P(Y) code and $D(t)$ is the navigation message, f_1 is the frequency of the L1 carrier, φ is the initial phase and, finally, A_C and $C(t)$ are the amplitude and the phase of the C/A code, respectively.

The GPS receivers provide the user position based on signals transmitted by satellites whose effective radiated power is approximately 280 Watts (in zenith direction). This signal arrives to the Earth surface with a power between –153 and –160 dBW, after travelling a distance of 20,200 km (Diggelen 2009).

In this article, we focus on the analysis of the L1 carrier frequency, which is the one used by the vast majority of civilian institutions outside the United States, as well as by the militaries that do not have authorization from the US DoD for using the encrypted data.

GPS INTERFERENCE BASIS AND PHASES OF OPERATION

In a simple way, in order to obtain the PNT information, a reference carrier shall be generated in the receiver and then modulated with a replica of the desired C/A code. Once each satellite has a very particular PRN code and this code is open-source for all users, the generation of this set (carrier/code) is not a difficult task.

In a second stage, the resulting signal must be correlated with the actual one, received from the satellite (Monico 2000), that is, the locally generated signal must be displaced until maximum correlation is obtained. Due to the property of the PRN codes, such maximum correlation is easily distinguished, determining whether that satellite is visible or not. This process is known as the "acquisition phase", whose purpose is to identify all visible satellites. Once the satellite is visible, one must estimate two different parameters: the frequency and the phase of the C/A code (Misra and Palod 2011).

After the synchronization, the GPS system shall continue to operate so that the received signal remains synchronized with the reference code. Therefore, the signal is managed in the channels, or trackers, that must be able to refine the values of code phase and frequency, keeping the internal signals synchronized with the received ones, continuously. That is the "tracking phase". The tracking runs continuously over time and, if lost, a new acquisition should be performed for that satellite.

GPS JAMMING AND POWER LEVELS OF INTERFERENCE

Jamming is defined as "the emission of radio frequency with enough power and with the features needed to prevent, in a given area, the receivers to track GPS signals" (Oonincx and van der Wal 2014).

The low power that GPS signals arrives to the receivers allows the power of the jammer to be effective even at very low power levels, making interference in GPS relatively simple and inexpensive to carry out. Various jamming methods are available in the market, being possible to find very efficient ones for $ 1,000.00, which are capable of delivering at least 100 watts (Rrol 2003).

When evaluating the influence of a jammer on a receiver, one should use the J/S relationship (jamming/signal). When expressed in dB, it is the difference between the power of the interfering signal and power of the received one.

According to Sklar (2003), a J/S level of 27 dB is enough to prevent/avoid the acquisition phase of GPS receivers that use only the C/A code. However, to prevent the tracking process, a level of 47 dB J/S is required. That is, if a GPS receiver is already providing PNT information, only a J/S of 47 dB could avoid the generation of the information, but a J/S of 27 dB is enough to prevent a new acquisition process.

MODELS OF PROPAGATION

THE FREE-SPACE PROPAGATION FRIIS EQUATION

The Friis Transmission Equation provides the power received by an antenna, given another antenna some distance far and transmitting a well-known amount of power, under idealized conditions. It serves as a good approximation for estimating signal levels through free-space, considering only the main factors influencing the propagation and not presenting a high computational effort. It does not consider the atmospheric attenuation (or the path loss) and eventual influences of clouds and rain, but gives a good idea of the effectiveness of jamming necessary power to provide losses in the functioning of GPS-based systems. It can be written as Faria *et al.* (2016):

$$P_r = \frac{P_t A_{ef}}{4\pi(R)^2} = \frac{P_t \lambda^2}{(4\pi R)^2} = G_t G_r \frac{\lambda^2}{(4\pi R)^2} \tag{2}$$

or, in dB,

$$P_r = P_t + G_t + G_r + 20\log_{10}\frac{\lambda}{4\pi R} \tag{3}$$

where G_t and G_r are the transmitting and receiving antennas gains (with respect to an isotropic radiator), respectively, P_t is the transmitted power, A_{ef} is the effective area of the receiving antenna, R is the distance between antennas and λ is wavelength of the carrier. Based on Eq. 1, it can be seen that, not considering the path loss, the power density that reaches the GPS receiver is inversely proportional to the square of the distance (R) between the jammer and the GPS antennas. If a more complex propagation equation should be considered, Eq. 2 becomes (Faria *et al.* 2016):

$$P_r = P_t + G_t(\theta_t,\phi_t) + G_r(\theta_t,\phi_t) + \left(\frac{\lambda}{4\pi R}\right)^2 \left(1-|\Gamma_t|^2\right)\left(1-|\Gamma_r|^2\right)\left|a_t . a_r^*\right|^2 e^{-\alpha R} \tag{4}$$

where $G_t(\theta_t,\varphi_t)$ is the gain of the transmitting antenna in the direction (θ_t,φ_t), $G_r(\theta_r,\varphi_r)$ is the gain of the receiving antenna in the direction (θ_r,φ_r), Γ_t and Γ_r are the reflection coefficients of the transmitting and receiving antennas, a_t and a_r are the polarization vectors of the transmitting and receiving antennas and α is the absorption coefficient of the intervening medium.

For a question of simplicity, in this work it will be considered only the simplified version of the Friis Equation (Eq. 2), while not considering a specific environment and the influence of Earth surface is assumed to be entirely absent.

THE URBAN AND SUBURBAN COST-231 HATA MODELS

In COST (1999), an empirical modeling was developed for signal propagation in urban and suburban areas, based on experimental measurements performed in European cities. This is shown as an extension of the modeling previously proposed by Hata-Okumura (Abhayaeardhana *et al.* 2005), which, in order to calculate the propagation loss, takes into account only four parameters: the frequency, the distance, and the heights of the transmitting and of the receiving antennas. Furthermore, the gains of both antennas must be considered as isotropic (which considers antennas as omnidirectional).

The COST-231 Hata model is only defined, and valid, for the frequency range from 500 MHz to 2000 MHz, containing correction factors for both urban and suburban environments. The basic equation for the propagation loss is:

$$P_L = 46.3 + 33.9\log(f) - 13.82\log(h_b) - ah_m + \left(44.9 - 6.55\log(h_b)\right)\log(d) + C_m \tag{5}$$

where f is the frequency, in MHz, d is the distance between the transmitting antenna (jammer) and the receiving one, in km, and h_b is the height of the transmitting antenna, in meters. The C_m parameter must be set as 0 dB for suburban environments and as 3 dB for urban ones, which is a necessary correction to adapt the model from one environment to the other. The parameter ah_m, for urban environments and for frequencies above 400 MHz, equals to:

$$ah_m = 3.2\left(\log(11.75ah_r)\right)^2 - 4.97 \tag{6}$$

while for suburban environments, this parameter is defined as:

$$ah_m = \left(1.1\log(f) - 0.7\right)h_r - \left(1.56\log(f) - 0.8\right) \tag{7}$$

where h_r is the height of the receiving antenna, in meters. It should be noted that this model is restricted to the cases in which the transmitting antenna is placed in the highest point of the surroundings.

SIMULATION RESULTS AND ANALYSIS

In order to evaluate, and estimate, the jamming effectiveness against GPS-based systems in different environments, as a function of the distance and jammer power, all three propagations models were modelled and simulated in MATLAB and the results are presented below.

Firstly, based on the Friis equation (Eq. 2), the J/S ratio (effectiveness of a jammer) was simulated, considering a wide range of Effective Isotropically Radiated Power (EIRP) and distances between the jamming and the receiving antennas (in km). The EIRP corresponds to the effective power radiated by the transmitting antenna in the direction of the higher gain, in relation to an isotropic antenna. In Eq. 2, it is represented by the sum of the values P_t and G_t. In this simulation, losses were neglected, with a value of G_t as 0 dBi and P_t varying from 100 W to 1000 W.

The J/S values of 47 dB and 27 dB, in relation to a GPS signal level of –157 dBW (Kaplan and Hegarty 2006) were used as the boundaries of the tracking and acquisition processes, respectively, considering both jammer and receiving antennas with gains equal to 0 dBi. In addition, it must be emphasized that the transmitting and the receiving antennas are in line of sight and additional loss factors were neglected. Figure 1 depicts the J/S ratio as a function of EIRP and distances. A color scale was implemented in order to facilitate the understanding and the situational awareness of the reader.

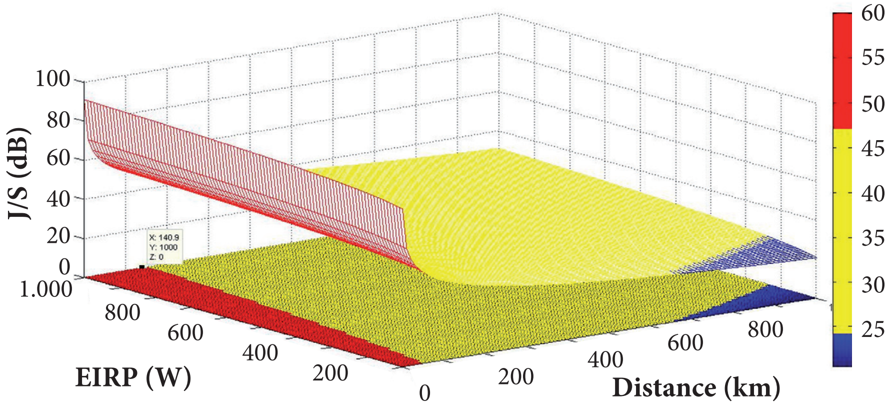

Figure 1. J/S ratio as a function of EIRP and distances, according to Friis equation (Eq. 2).

But it should be noted that such model (Friis equation) becomes incipient when there is no line of sight between the jammer and the target, with the gains of the antennas as mentioned above. Thus, the jammer effective distances show to be inconsistent, when analyzing a jammer close to the ground in a complex environment, without an established line of sight. For these complex cases (urban and suburban environments), the COST-231 Hata model should be used.

In order to evaluate these cases, other simulations were performed, considering the propagation of a non-modulated signal on the L1 carrier (1,575.42 MHz). This was considered for both urban and suburban environments, modelled by the COST-231 Hata model. In the same way that was performed for the free-space simulations, a wide range of EIRP and distances between the jamming and the receiving antennas (in km) were used, providing the respective J/S ratio. The height of the jammer was considered as 60 meters while the GPS receiver was fit to 2 m in relation to the ground, placed at a distance *d*, one from another. The J/S values of 47 dB and 27 dB, in relation to a GPS signal level of –157 dBW (Kaplan and Hegarty 2006) were also used as boundary for the tracking and acquisition processes, respectively.

Figures 2 and 3 depict the J/S ratio as a function of EIRP and distances for the suburban and urban environments, respectively, while Table 1 summarizes a comparison of the boundary distances of the acquisition and the tracking processes for three different EIRP (100 W, 500 W and 1000 W) in the three considered situations.

As can be seen in Table 1, the boundary distances to avoid the acquisition and tracking process are presented, after using the free-space propagation model and the COST-231 Hata model, either in urban or in semiurban environments. In these cases, comparing the jammer efficiency values generated by the COST-231 Hata propagation models and the Friis transmission model, a high discrepancy between the three simulations is observed.

Analyzing the results for the free-space propagation case, under an interference of a 100 W signal, the GPS-based systems would be avoided to track the code at a distance of 41.38 km, that is, they would be completely "jammed" or "blocked". However,

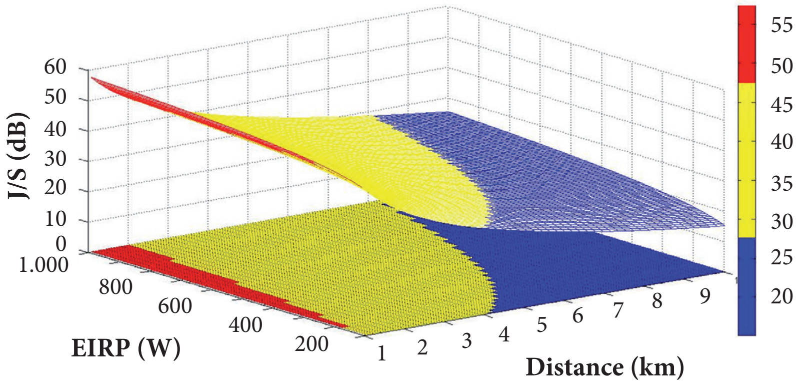

Figure 2. J/S ratio as a function of EIRP and distances, according to COST-231 Hata model, suburban environment.

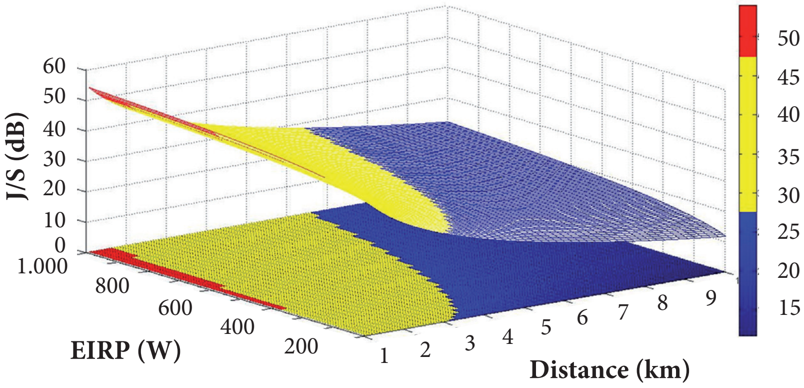

Figure 3. J/S ratio as a function of EIRP and distances, according to COST-231 Hata model, urban environment.

Table 1. Distance for acquisition and tracking phases, as a function of EIRP, according to free-space model and COST-231 Hata model, considering both suburban and urban environment

EIRP	Urban environment		Suburban environment		Free-space	
	Acquisition	Tracking	Acquisition	Tracking	Acquisition	Tracking
100 Watt	3.495 km	< 1 km	4.455 km	1.192 km	465 km	41.38 km
500 Watt	5.798 km	1.576 km	7.141 km	1.768 km	1030 km	102 km
1000 Watt	6.949 km	1.700 km	8.677 km	2.152 km	1495 km	142.3 km

already at a distance of approximately 465 km, these same systems would be avoided from carrying out the acquisition process. These distances seem to be relatively high, considering an actual situation of jamming, but it must be highlighted that it reflects the simplification used in the general equation. As mentioned before, the used equation serves only for estimating signal levels through free-space, considering the main factors influencing the propagation and not considering the atmospheric attenuation (or the path loss). For a more realistic analysis, the results presented in the urban and suburban environments columns must be considered.

In these very specific cases, after using the COST-231 Hata empirical model for urban environments, which shows to be a lower limit for the effectiveness of the jammer, we obtain a boundary acquisition distance of approximately 3.5 km, while for the tracking of the code we find a value below 1 km. This latter result could not be determined in our simulations due to the existence of a minimum distance restriction between the transmitter and receiver, which is 1 km.

Results for the COST-231 Hata empirical model for suburban environments show to be always intermediate values and will not be discussed in this article, due to a question of brevity.

Therefore, considering only the very specific case of a jammer with a power of 100 W, we find that GPS-based systems are highly vulnerable, in the best case, at a distance of 3.5 km, considering the specified scenario. This result leads to a concern for those who operate these systems, once even in an urban environment, where we cannot find the origin of the threat, the systems can be interfered.

Exploring a little more the results, if we go to an EIRP of 1000 W, we find higher distances, showing a high vulnerability for GPS-based systems that cannot be ignored. Values in the order of 1495 km for a free-space interference are shown and of almost 7 km for urban environments are able to avoid the acquisition phase. If we analyze the results provided by the models, even larger differences can be observed, when comparing them with lower power jammer systems, emphasizing the importance of a correct choice of the model to be used, in order to correctly dimension the potential damages caused by a jammer.

FINAL REMARKS

GPS devices have been widely disseminated and used in different systems, both for civilian and militaries applications. However, despite being able to provide great benefits, it should be taken into account that these systems are, under certain circumstances, vulnerable to intentional interference. The deepening dependence of the civil and military infrastructures on GPS and the potential for financial gain or high-profile mischief makes GPS jamming a gathering threat.

In the present article, the main characteristics of the GPS positioning system were succinctly characterized. Among them, it is clear that the low power that the signal arrives to the receiver makes easy to jam them, with low power, impeding the processes of acquisition and tracking of satellite signals.

Previous studies have already used this concept to estimate the effectiveness of jamming signals in free-space. However, such model become incipient when applied in more complex urban, or suburban, environments.

Thus, in order to increase/highlight the situational awareness of a potential eventual jamming, the distance range of jammers with different EIRPs was simulated, using both the Friis and the COST-231 Hata empirical propagation models.

As expected, the values obtained through the free-space propagation model highlight the ineptitude to dimension the interference effectiveness in more restrictive suburban and urban environments. This could be determined by the empirical propagation model, which, although having been obtained through tests in European cities, is already able to give an idea of the vulnerability range that GPS-based systems are submitted, even in other parts of the world.

Therefore, the present work shows not only the J/S ratio for a wide range of EIRP jamming signals, considering different distances, but also presents the boundary distances for avoiding the tracking and acquisition phases by a GPS-based system. Furthermore, through the previous results, a very clear picture of the importance of using the correct model for predicting and estimating a safe zone for operating GPS-based systems is provided.

As future work, it is expected to propose some kinds of countermeasures that could be implemented in the GPS-based systems in order to avoid such jamming threats.

AUTHOR'S CONTRIBUTION

Conceptualization, Faria LA and Silvestre CAM; Methodology, Silvestre CAM; Investigation, Faria L A; Silvestre CAM and Correia MAF; Writing – Original Draft, Faria LA; Roso NA and Silvestre CAM; Writing – Review & Editing, Faria LA; Roso NA and Silvestre CAM; Resources, Faria LA; Silvestre CAM and Correia MAF; Supervision, Faria LA.

REFERENCES

Abhayaeardhana VS, Wassell IJ, Crosby D, Sellars MP, Brown MG (2005) Comparision of Empirical Propation Path Loss Models for Fixed Wireless Access Systems. IEEE 61st Vehicular Technology Conference. doi: 10.1109/vetecs.2005.1543252

Bakker PF (2006) Effects of radio frequency interference on GNSS receiver output. Stevinweg: Delft University of Technology.

Balvedi GC (2006) Efeitos dos dutos troposféricos na propagação e recepção de sinais GPS (MSc Thesis). São José dos Campos: Instituto Tecnológico de Aeronáutica. In Portuguese.

Cavaleri A, Motella B, Pini M, Fantino M (2010) Detection of spoofed GPS signals at code and carrier tracking level. Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (Navitec). doi: 10.1109/navitec.2010.5708016

Correia MAF (2015) Susceptibilidade de sistemas complexos dependentes de GPS a interferências intencionais (Esp. Thesis). São José dos Campos: Instituto Tecnológico de Aeronáutica. In Portuguese.

COST Action 231 (1999) Digital Mobile Radio Towards Future Generation Systems, final repost. European Communities, EUR 18957.

Faria LA, Silvestre CAM, Correia MAF (2016) GPS-dependent systems: vulnerabilities to electromagnetic attacks. Journal of Aerospace Technology and Management – JATM 8(4):423-430. doi: 10.5028/jatm.v8i4.632

Kaplan E, Hegarty C (2006) Understanding GPS: principles and applications. Norwood: Artech House.

Ledvina BM, Bencze WJ, Galusha B, Miller I (2010). An in-line anti-spoofing device for legacy civil GPS receivers. Proceedings of the ION International Technical Meeting; San Diego, USA.

Misra R, Palod S (2011) Code and carrier tracking loops for GPS C/A code. International Journal of Pure and Applied Sciences and Technology 6(1):1-20.

Monico JFG (2000). Posicionamento pelo NAVSTAR-GPS descrição, fundamentos e aplicações. São Paulo: Editora Unesp. In Portuguese.

Motella B, Pini M, Fantino M, Mussalano P, Nicola M, Fortuny-Guasch J, Wildemeersch M, Symeonidis D (2010) Performance assessment of low cost GPS receivers under civilian spoofing attacks. Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (Navitec). doi: 10.1109/navitec.2010.5708018

Oonincx PJ, van der Wal, AJ, editors (2014) Optimal deployment of military systems: technologies for military missions in the next decade. The Hague:T. M. C. Asser Press.

Rrol JV (2003) Vulnerability assessment of the U.S transportation infrastructure that relies on the Global Positioning System. The Journal of Navigation. doi: 10.1017/s0373463303002273

Russon MA (2015) Wondering how to hack a military drone? It´s all on Google; [accessed 2016 Nov 04]. http://www.ibtimes.co.uk/wondering-how-hack-military-drone-its-all-google-1500326

Scott L (2015) Approaches for Resilient Positioning, Navigation and Timing (PNT). Association of Old Crows; [accessed 2015 Oct 15]. http://crows.org/item/gps-interference-origins-effects-and-mitigations.html

Silvestre CAM (2014). Vulnerabilidade do sistema GPS a interferências intencionais (Esp. Thesis). São José dos Campos: Instituto Tecnológico de Aeronáutica. In Portuguese.

Sklar JR (2003) Interference mitigation approaches for the global positioning system. Lincoln Laboratory Journal 14(2):167-180.

Diggelen FV (2009) A-GPS: Assisted GPS, GNSS and SBAS. Boston/London: Artech House.

The Royal Academy of Engineering (2011) Global navigation space systems: reliance and vulnerabilities. London (England).