HADMÉRNÖK

XIV. Évfolyam 2. szám – 2019. június

# ELECTRONIC WARFARE IN NAVWAR: IMPACT OF ELECTRONIC ATTACKS ON GNSS / GBAS APPROACH SERVICE TYPES C AND D LANDING SYSTEMS AND THEIR PROPOSED ELECTRONIC PROTECTION MEASURES (EPM)

# ELAKTRONIKAI HADVISELÉS ALKALMAZÁSA A NAVIGÁCIÓS HADVISELÉSBEN: AZ ELEKTONIKAI HADVISELÉS HATÁSA A GNSS ÉSVALAMINT A JAVASOLT ELEKTRONIKUS VÉDELMI RENDSZEREK

ALHOSBAN, AHMAD

(ORCID: 0000-0001-7494-6067)

Ahmad_alhosban@yahoo.com

***Abstract***

*Global Satellite Navigation Systems (GNSS) applications -using different satellite signals in space- are currently and hugely subjected to Electronic Attacks (EAs) such as Jamming, Spoofing, and/or Meaconing. Many accidents were observed in the past decade, while huge dependency on GNSS applications in governmental and private critical infrastructure, in both civil and military aspects. The EAs could be expensive and high-power such as the military-grade jammers, which are an integral pillar of navigation warfare (NAVWAR) strategies. On the other hand, EAs could be cheap and low-power such as the so-called Personal Protection Devices (PPD), which they are widely available. Electronic Attacks, most critically observed by ICAO and FAA, are in Ground Based Augmentation System -(GNSS/GBAS) Landing systems, in which is riskier and more critical than other applications due to the sensitivity of the final landing phase of all flights. The objective of this study is to evaluate the impact of the three different types of EA on the performance GNSS/GBAS landing system. On the other hand, to address and examine their latest proposed Electronic Protection Measures (EPM).*

***Keywords***:
*Global Navigation Satellite System, Ground Based Augmentation system, NAVWAR, Electronic Warfare, Electronic Attacks, Electronic Protection Measures*

***Abstract***

*A globális navigációs műholdrendszerek (GNSS) alkalmazásai, melyek különböző műholdas jeleket használnak az űrben, jelenleg komoly elektronikus támadásoknak (EAs) vannak kitéve, úgy mint a Jamming, Spoofing, és/vagy Meaconing. Számos baleset volt megfigyelhető az elmúlt évtizedben, miközben jellemző, hogy a kormányzati és magántulajdonú kritikus infrastruktúra nagymértékben függ a GNSS - alkalmazásoktól, polgári és katonai szempontból is. Az elektronikus támadások egyrészt drágák és nagy teljesítményűek is lehetnek, mint például a katonai szintű zavaró berendezések, amelyek a navigációs hadviselés (NAVWAR) szerves részei. Másészt az elektronikus támadások alacsony teljesítményűek is lehetnek és kedvező áron hozzáférhetőek, mint például az úgynevezett személyvédelmi eszközök (PPD), amelyek széles körben elérhetők. Az elektronikus támadásokat a Nemzetközi Polgári Repülési Szervezet (ICAO) és a Szövetségi Légiközlekedési Hivatal (FAA) a legkritikusabban figyeli a Földi telepítésű kiegészítő rendszeren (GNSS/GBAS), valamint a leszállási rendszeren, amely kockázatosabb és kritikusabb, mint más alkalmazások, a gépek leszállási fázisának érzékenysége miatt. A tanulmány célja az elektronikus támadások három különböző típusának a GNSS / GBAS teljesítménymérő rendszerre gyakorolt hatásának értékelése. Valamint a legutóbbi elektronikus védelmi intézkedések (EPM) megvitatása és megvizsgálása.*

***Kulcsszavak:***
*Globális navigációs műholdrendszerek, Földi telepítésű kiegészítő rendszer, NAVWAR, EW, EA, Elektronikus védelmi intézkedések*

A kézirat benyújtásának dátuma (Date of the submission): 2019.04.05.
A kézirat elfogadásának dátuma (Date of the acceptance): 2019.05.20.

## INTRODUCTION

Global Satellite Navigational Systems (GNSS) applications-using satellite signals in space-are currently and hugely subjected to Electronic Attacks (EA) such as Jamming, Spoofing, and/or Meaconing, if it had not already been interfered unintentionally by other host applications. Many accidents were observed in the past decade especially with the huge dependency on GNSS applications in governmental and private critical infrastructure, in both civil and military aspects. The well-known GNSS discrete frequencies (L1, L2, and L5, etc.) are so vulnerable to EAs. Because of their extremely low level of power density, they are propagated from long-distance satellites' orbits of about (22,000 Km) via Troposphere and Ionosphere layers. and they arrive the surface of ground at a weak power level. It's around (-160dBw for GPS L1, -154dBw for GPS L2(Military), Speculated -155dBw for Galileo E1/E2). Saying that, any non-significant exceeded level of any power by a jamming transmitter would be harmful, this impact ranging either destructively at most or electronically deceptively at least, so that GNSS signals cannot be acquired or/and tracked anymore by the GNSS receivers.

The EAs could be expensive, sophisticated and high-power such as the military jammers, which are an integral pillar of navigation warfare (NAVWAR) strategies. As other EW aspects, EAs are affecting the GNSS Position, Navigation and Timing (PNT) usage before and during any kinetic fight, Examples of such attacks were experienced in South Korea and Ukraine, in South Korea, GPS Signals were disrupted in many military aircrafts and ships between August 2010 and May 2013 by the deliberating Military-effect jammer from North Korea. [2]. In Ukraine, the Organization for Security and Cooperation in Europe (OSCE) has recently reported a military-grade GPS jamming on the UAVs missions, [2].

On the other hand, EAs could be cheap, low-power, and widely available such as the so-called Personal Protection Devices (PPD), which are been considered more and more frequently source of EAs; PPDs are small, light-weight jammers that are easily available in the internet market, their usage is forbidden in the majority of countries; but their possession is not regulated everywhere with the same strictness level. Examples of such attacks GBAS landing system at Newark Liberty International Airport/USA in 2012, when the certification process was disturbed by a truck jammer driving in a road nearby the airport as per Federal Aviation Administration (FAA)reported, [1;2]. And also reported in the Future Security Conference -7$^{th}$ in 2012, [8, p 197].

Electronic Attacks, most critically observed by International Civil Aviation Organization (ICAO) and Federal Aviation Administration (FAA), are in GNSS/GBAS Landing systems, which are used for final landing phase of flights in both civil and military aviation domains, or during military operations in deployed theaters. However, GBAS landing systems are satellite-based navigational aids used in Critical Meteorological Conditions (CMC), such as heavy dust and heavy fog, where the visibility tends to zero in the final landing of an aircraft, in which their loss of Service during the Final Approach Segment (FAS) is considered a catastrophic disaster to aviation safety-of-life in terms of assets, human and military operations. At those cases, capability of service restore on the proper time has very low probability. Its highly risker in such safety-of-life applications of landing systems when compared with other safety –critical infrastructure applications such as banking or non-critical applications of GNSS huge usages. Moreover, GBAS stations

are usually located in a well-known surveyed reference sites in the vicinity of the airport near the runways. Which makes them more vulnerable to EAs, both the fixed ground reference stations and the downwind moving aircrafts when being landing close to runway surface.

The objective of this study is to evaluate the impact of the three different types of EAs (jamming, spoofing and meaconing) on the performance of GNSS/GBAS landing system. On the other hand, to address and examine the latest proposed Electronic Protection Measures (EPM) for such EAs, based on the three mitigation methods: the receiver-based mitigation methods, antenna-based methods and the siting-based methods.

It was observed a strong link between the concept of multipath and EAs, in terms of accumulating two or more signals at the receiving antenna in the so called technically interference. However, the over power jamming seems to be similar to the destructive multipath when the phases of the two signals are 180 degrees out of phase, assuming they were modulated and (authenticated) by the same navigation message of Position, Navigation and Timing (PNT). On other hand, spoofing/meaconing seem to be similar to the electronic deceptive side of the multipath signal with long delay time of the original signal that GNSS receiver would be un capable to correlate in proper time, that will mislead PNT information.

The methodology used in this study is the scientific analysis of the GNSS signal structure and signal processing, comparing EAs techniques versus Multipath effect by its nature of interference of the genuine signal, and finally using the results from a simulating tool applied in GBAS application to assess to which level this effect could be harmful. Those simulations were done over Europe including the main airports, with special concentration is focused on Liszt Ferenc International Airport in Budapest, Hungary. Followed by examining of the Electronic Protective Measures (EPM) being used to mitigate the signal damage/loss, which eventually cause at least the loss of service if not been electronically deceived.

## Scientific Problem and the Observed Accidents/Deliberating

Firstly; EA threats could be professionally intentionally, using expensive, sophisticated and high-power such as the military-grade jammers. Those are considered an integral pillar of navigation warfare (NAVWAR) strategies. Many accidents were observed and had been reported to higher authorities and related organizations such as ICAO and FAA, but here the two of them as most importantly:

1. During the NATO military exercise on the 8th Nov 2018, in Finland and Norway: navigation failure lead to collision of frigate with a tanker. There was collateral damage. Civilian airliners, cars, trucks, cargo ships and smart phones operating in and around experienced similar disruptions. The airline said its aircraft carried alternate navigation systems. A US defense official told CNN that the jamming had "little or no affect" on US military assets. [15]. This little or no effect is due using the military P/Y code that it’s much more immune against jamming as it will be illustrated later in this study. The Norwegian frigate "KNM Helge Ingstad" suffered a navigation failure leading to a collision with the tanker “Sola TS” on November 8, 2018 in the Hjeltefjord near Bergen. Figure (1): AFP Source: AFP

**Figure 1**: the Norwegian frigate suffered navigation failure [15]

2. EAs were experienced in South Korea and Ukraine: In South Korea, GPS Signals were disrupted in many military aircrafts and ships between August 2010 and May 2013 by the deliberating Military-effect jammer from North Korea. In Ukraine, the Organization for Security and Cooperation in Europe (OSCE) has recently reported a military-grade GPS jamming on the UAVs missions. [2]. Furthermore; EAs could be unprofessionally intentionally occurred, using cheap, low-power, small, light-weight jammers. Those are widely available such as the so-called Personal Protection Devices (PPD). They are considered more and more frequently source of EAs, and easily available in the internet market. Their usage is forbidden in the majority of countries. The most related accident to be addressed here is the GBAS landing system (Honeywell SLS-4000) which was approved by the FAA at Newark Liberty International Airport/USA in 2012 as CAT I (GAST C). While the certification process was disturbed by a truck jammer driving in a road nearby the airport as per FAA reported, [1;2]. And also reported in the Future Security Conference - 7th in 2012, [10, p 197]. As seen in the Fig (2), the airport is fully and closely surrounded by crowded traffic roads. This increase its GBAS vulnerability of being interfered or attacked. When the geographic vicinity of the Liszt Ferenc International Airport in Budapest Hungary is compared with Newark Airport, as seen in Fig (3), its little better but not significantly much differ from. The nearest road is about 350 meters from any of the two proposed suggested sites of any future GBAS system would be installed in.


**Figure 2**: Newark Airport layout (Edited by the Author)


**Figure 3:** Layout of Liszt Ferenc Airport at Budapest (Edited by the Author)

The real scientific problem in not only the citing criteria, but also that the GNSS signals are so vulnerable to EAs because of their extremely low level of power density, satellites transponders' are orbiting about (22,000 Km) above the Ground level, and they are transmitting their signals via Troposphere and Ionosphere layers, so that the signals arrive the earth surface to users in a weak signal to noise ratio, around -160dBw for GPS L1, -154dBw for GPS L2(Military), Speculated -155dBw for Galileo E1/E2). The other part of the problem is that capability of service restore on the proper time has very low probability. It's so high risky in safety-of-life applications of landing systems when compared with other safety –critical infrastructure applications such as banking or non-critical GNSS applications. Furthermore, GBAS stations are usually located in a well-known surveyed reference sites in the vicinity of the airport near the runways. Which makes them more vulnerable to EAs. Anyhow, currently GBAS systems are hardly achieving CAT I/GAST

C performance, only due to other system errors originally invoked by other than interference or EAs.

Finally, EAs could be unintentionally, such as some GNSS bands are shared with certain radars, amateur radio. Other sources are Distance Measuring Equipment (DME). Also the TV harmonics, malfunctioning electronic equipment.

## GNSS/GBAS Signal Structure w.r.t Electronic Warfare

In the concept of Electronic Warfare (EW), the Electronic Attack (EA) is defined as the use of the electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Electronic attack includes reducing an enemy's effective use of the electromagnetic spectrum, the use of either electromagnetic or directed energy as a primary destructive mechanism, and the use of countermeasures, [3]. Electronic warfare is integrated and synchronized with lethal fires in order to disrupt and increase the enemy's decision making reaction time. It supports friendly forces with different kinds of information about the enemy's electronic systems. Electronic countermeasures can be offensive or defensive. Offensive activities are generally conducted at the initiative of friendly forces. Defensive electronic countermeasures protect personnel, facilities, capabilities and equipment. Including communications systems such as wireless networks, cyberspace networks and radios, as well as the non-communications systems such as radars, Air Traffic Control and navigation, etc., [4;13].

EW's produces NAVWAR effects by protecting or denying transmitted global navigation satellite system (GNSS) or other radio navigation aid signals. EA is used to create NAVWAR effects by degrading, disrupting, or deceptively manipulating positioning, Navigation, Timing (PNT) transmissions. Electronic Support Measures (ESM) assist NAVWAR through DF and geolocation of intended or unintended transmissions that interfere with effective and timely PNT signal reception. EPM is used to deliver NAVWAR capabilities protecting space, control, or user segments of the GPS/GNSS architecture from disruption or destruction. [3].

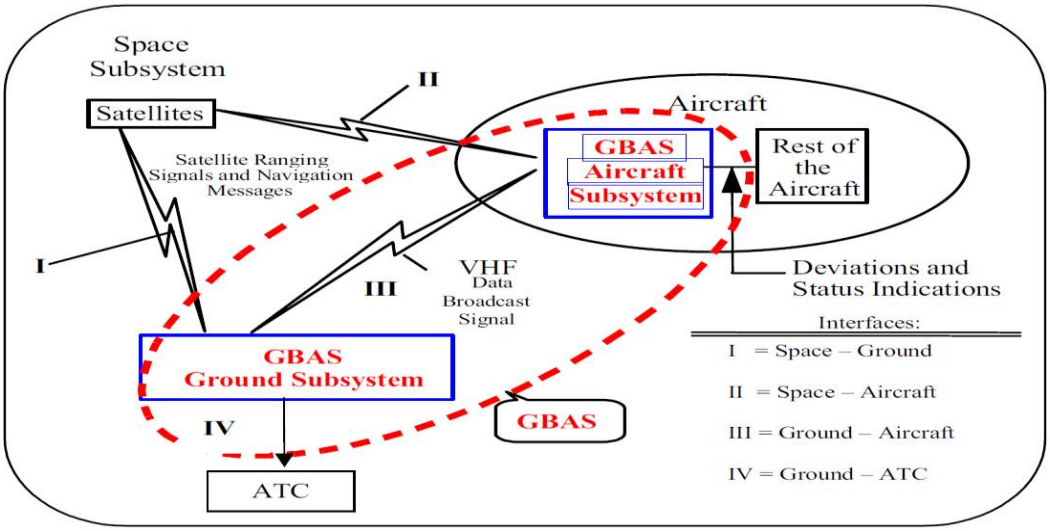



**Figure** 4: GBAS system links, [14]

In GBAS landing systems, there are Four types of links, shown in Figure (4):

1. Space- Ground GBAS Downlink, with weak GNSS signal (Currently GPS): S/N is -160dB. Its more vulnerable to EAs due to fixed position. The GPS errors included are: Ionosphere, Multipath, Rx, hardly achieving GAST-C (CAT I) performance of 99.74% Ap. Moreover, Electronic protection techniques as LPI, is used such as spreading the spectrum and antenna based but still experienced accidents.
2. Space – Aircraft Downlink: It's also a weak GNSS signal (Currently GPS): -160dB. And it's less vulnerable to EAs due to mobile dynamic position, due to higher altitude about at least 200 feet above ground level makes it more immune to ground jammers but not UAVs based ones. Furthermore, using Up-looking MLA GPS Antenna somehow mitigates interferences. GPS errors: Ionosphere, Multipath, Rx, hardly achieving GAST-C (CAT I) performance of 99.74% Ap. The Electronic Protection Techniques as LPI, is used as well, such as spreading the spectrum and antenna based but still experienced accidents.
3. Ground – Aircraft Uplink: it's a Protected VHF link carrying the continuously sent integrity and corrections messages. Its characterized by its higher power to noise S/N, so more immune to EAs.
4. Ground – ATC Link: which is a secured land lines that nit in the scope of EW electromagnets attacks. And really doesn't affect the operation of the system as it informative link to ATC about the health status of the system.

At the satellite transponder side, which is the space segment, the GPS signal structure is sent by the satellites Space Segment, [10, p77], consists of Two Carrier Frequencies (L1 and L2) and Two codes, both characterized by a pseudorandom noise (PRN) sequence Figure (5) and Table (1) below. The first is the coarse/acquisition or (clear/access) code (C/A-code). It has the frequency $f_o/10$ and is repeated every millisecond. The codes of the two registers are not classified, and the C/A-code is available to civilian users. The other code is the precision (or protected) code (P-code). It has the frequency $f_o$ and is repeated approximately once every 266,4 days. It is also not classified, but the P -code is encrypted to the Y-code by Anti spoofing (A-S). Since the Y-code is the sum of the P-code and the encrypting W-code, access to the P-code is only possible when the secret conversion algorithm is known, so its jamming immunity is better. A third code called the W-code is used to encrypt the P-code to the Y-code when A-S is implemented. The coding of the navigation message requires 1500 bits and, at the frequency of 50 Hz, and its transmitted in 30 seconds.

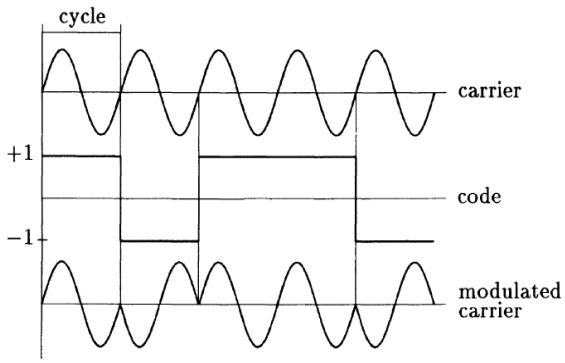



**Figure 5:** GPS coding structure [10]

| Component | Frequency (MHz) | |
|---|---|---|
| Fundamental frequency | $f_0$ | = 10.23 |
| Carrier L1 | 154 $f_0$ | = 1575.42 (≙19.0 cm) |
| Carrier L2 | 120 $f_0$ | = 1227.60 (≙24.4 cm) |
| P-code | $f_0$ | = 10.23 |
| C/A-code | $f_0/10$ | = 1.023 |
| W-code | $f_0/20$ | = 0.5115 |
| Navigation message | $f_0/204\,600$ | $= 50 \cdot 10^{-6}$ |

**Table 1:** GPS Signal components [10]

Pseudo Random Noise Codes PRN is the generation of the PRN sequences in the codes and it is based on the use of hardware devices called tapped feedback shift registers. While the Navigation Message essentially contains information about the satellite health status, the satellite clock, the satellite orbit, and various correction data. Moreover, it contains the predicted satellites orbital elements (broadcast ephemerides) necessary to compute satellite coordinates in WGS84 system, and directly used to process receiver coordinates. Its subdivided into five sub-frames, each sub-frame is transmitted in 6 seconds and contains 10 words with 30 bits. More details about GPS signal structure are found in [10].

In general, GNSS world includes four main satellite systems, the USA GPS system, the Russian GLONASS system, the European Galileo system, and the Chinese Beidou System. There are differences in signal structure among them, but they used the same principle of producing the position, velocity and time (PVT) solution to the different users. More detailed information about differences in signal structure and performance for GPS, GLONASS and the Galileo systems can be found in [6]. The new European Global Navigation System Galileo is not fully operational yet. It is anticipated to be in Full Operational Capability (FOC) in 2021 if not beyond. More details about the three main phases of Galileo navigation project in [8;9]. Moreover, GLONASS system uses different frequencies and different modulation scheme. On the other hand, China has launched their Beidou navigational system but not globally, it is up to date a regionally covering the far-east region only,[6]. Figure (6) below shows a new projected GNSS signals structure.

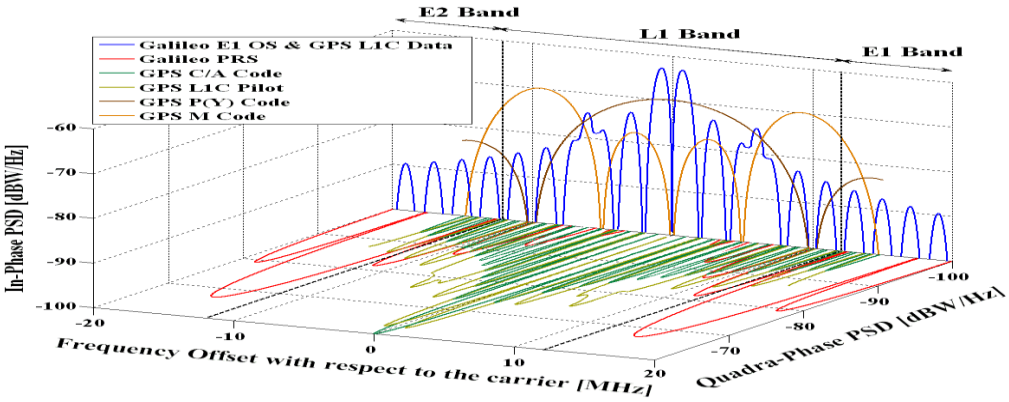



**Figure 6 :** New Modern GNSS signal structure[6]

All the GPS receivers uses fixed-tuned receiver type because the satellites within the 24/29 GPS constellation are broadcasting at the same frequency. But with spreading codes that allow selection of one satellite's signal by a receiver, or a channelized receiver. The Direct Sequence spread Spectrum DSS is used in both the BPSK modulation scheme and the Galileo BOC modulation scheme as basic LPI technique, [11; p 84].

## GNSS/GBAS Signal Processing w.r.t Electronic Warfare

At the receiver side, which is mainly the ground segment (here in GBAS system the ground station or the Aircraft receiver), the carrier, code and the navigation message is decoded and demodulated to form the useful information of the PVT using the code correlation techniques. Such as: Code correlation Narrow and Wide, squaring technique, Cross correlation technique, Code correlation plus squaring technique, and the Z-tracking technique. The Data Acquisition is done by: Either the Code pseudorange in which the precision of roughly 3 m and 0.3 m is achieved with C/A-code and P-code pseudorange respectively. Or the Phase pseudorange: can be measured to better than 0.01 cycles which corresponds to millimeter precision, [10; p83]. See Figure (7).

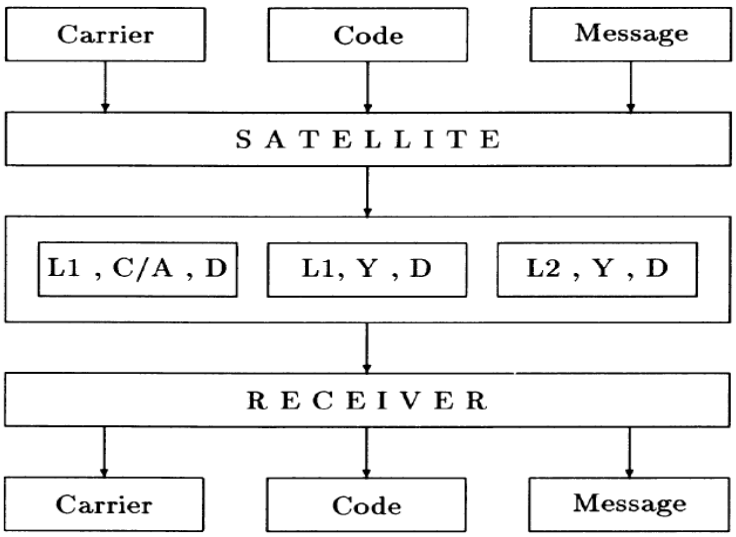



**Figure 7:** GPS signal processing flowchart[10]

| Code | Strength reduction at L1 | at L2 |
|---|---|---|
| C/A-code | −156 to −160 | - |
| Y-code | −159 to −163 | −162 to −166 |

| | |
|---|---|
| Squaring | −30 dB |
| Cross correlation | −27 dB |
| Code correlation plus squaring | −17 dB |
| Z-tracking | −14 dB |

**Table 2:** S/N ratio against EAs in correlation techniques[10]

Comparing the S/N ratio with respect to different correlation techniques in terms of the used EPM of the DSSS signal, the Z-tracking is the strongest among them against EAs. Table (2). These receiver-based techniques of data acquisition are not only used to retrieve the useful information of PNT, but also considered mitigation methods of interference or EAs if intentionally invoked. Even though they are not so efficient if the taking into consideration the occurred accidents mentioned previously. However, the new signal structure and the new signal processing in Galileo and the modernized GPS are hopefully will add another value in receiver based mitigation methods.

## Impact of EAs on GNSS/GBAS Using Multipath Approach

The well-known EAs types are classified technically into three main categories. They could be spot or chirp or swept or continuous wave affect. depending on their utilizing of frequencies coverage and electromagnetic power density over those frequencies. [1; 11]:

1. Jamming: it's the Intentional interference deliberate radiation of electromagnetic signals at GNSS frequencies. The aim is to overpower the extremely weak GNSS signals so that they cannot be acquired and tracked anymore by the GNSS receiver. They cause loss of LOCK (Destroy/ Neutralizing). And as said they could be Military grade jammers dual band, denial system ,10km-150 km or PPDs: civilian, dual band, with range of 30-350 Km. Figure (8).

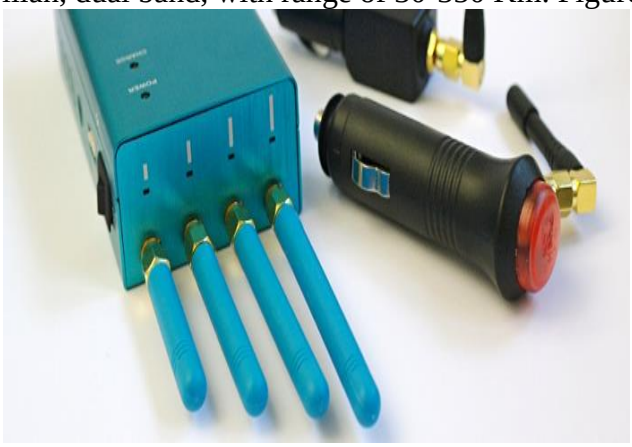


**Figure 8:** PPDs low power widely available[1]

2. Spoofing: it's the Generation and transmission of fake GNSS signals. The aim to lead a GNSS receiver astray (Deception), possibly without the GNSS receiver being aware of the attack. Technically they are more challenging than jamming, according to the complex GNSS signal structures especially for several GNSS signals in parallel.

3. Meaconing: it's the little brother of spoofing, it is the re-transmission of received GNSS signals (Deception). This avoids the burden of implementing the generation of the complex GNSS signal structures. Also it causes the GNSS receiver to provide erroneous PNT information, because the reception and re-broadcast process changes the relative delays of the GNSS signals as seen by the receiver, compared to the relative delays of the authentic GNSS signals at the receiver's location.

In general, The Model of Jamming in EA for any communication system including GNSS down links, [11, p 253]:

$$J/S = ERP_j - ERP_s - L_j + L_s + G_{Rj} - G_R$$

Where:

*J/S:* the ratio of jammer power to the desired signal power (Here the received power *from* satellite) at the input of the receiver being jammed in dB

$ERP_j$ : the effective radiated power of the jammer in dBm

$ERP_s$: the effective radiated power of desired signal transmitter (Satellite) in dBm

$L_j$ : the propagation loss from the jammer to the targeted receiver (GBAS or Aircraft) in dBi

$L_s$: the propagation loss from the desired signal transmitter (Satellite)to the targeted receiver (GBAS or Aircraft) in dBi

$G_{Rj}$ : the receiving antenna gain (GBAS Antenna or Aircraft Antenna) in the direction of the jammer in dBi

$G_R$: the receiving antenna gain (GBAS or Aircraft) in the direction of the desired signal transmitter (Satellite) in dBi

In comparison with Multipath phenomenon which is the propagation phenomenon that results in radio signals reaching the receiving antenna by two or more paths; in other words, it's an interference in its nature. [14]. The multipath can be:

1. constructive (when the reflected phase angle is 0) ≈ resemble the Spoofing and Meaconing (deceptive) in EA
2. destructive (when the reflected phase angle is 180) ≈ resemble the brute force jamming (destroy) in EA
3. interference in terms of both amplitude varying and/or phase shifting ≈ resemble both.

And it's given by the following equation:

$$r(t) = \underbrace{A_0.d(t-\tau_0).c(t-\tau_0).\cos(2\pi f_{L1}t-\theta_0)}_{LOS\,/\,Direct-signal} + \underbrace{A_1.d(t-\tau_1).c(t-\tau_1).\cos(2\pi f_{L1}t-\theta_1)}_{reflected-signal}$$

Where:

$A_0$, $\tau_0$, $\theta_0$: are the amplitude , the propagation delay, and the carrier phase shift respectively of the direct signal.

$A_1$, $\tau_1$, $\theta_1$: are for the one reflected multipath signal.

The phase rate of change is assumed to be zero.

Analyzing both equations in terms of power, time of action and data affect, the resultant table could be interpreted:

| **Parameter** | **EA (jamming, spoofing, meaconing) level** | **Multipath Interference level** | **Mitigation level** |
|---|---|---|---|
| **Power J/S** | Jamming CW<br>Jamming Chirp | MP level A destructive at least | CW by filtering almost negligible<br>Chirp is deceptive without Authentication<br>Loss of signal track and lock<br>Power level at receiver end |
| **Time of action** | CW continuously during landing<br>Chirp depends on frequency scanning process | For fixed stations is continuously<br>For a moving aircraft is temporarily | By Signal structure<br>By power level at time of affect |
| **Data affect** | Deceptive misleading information , degrading of availability of integrity and accuracy | High error , deceptive and degrading availability of integrity and accuracy | By signal structure , receiver level and coding, P/Y code is more immune |

**Table 3:** Comparison table between EAs and Multipath [edited by the author]

Airborne multipath model, which modules the Airborne multipath Designator (AMD): is the Multipath level, 0 to 1 levels, the 1 level is the highest value and could be constructive or destructive depending the phase θi, [14]. Going toward zero by B = A/2, or further A/4

resemble mitigation level optimistically depending on mitigation techniques for evaluation purpose of Impact on Availability using simulator tool, and it's given by the following equation:

$$RMS_{multipath}(\theta_i) = a_o + a_1 \cdot e^{-\frac{\theta_i}{10}}$$

Where:
i: Is the ith ranging source
ao , a1 , and θi are parameters determined by the table shown below:

| Airborne Multipath Designation (AMD ) | $\theta_0$ (degrees) | $a_0$ (meters) | $a_1$ (meters) |
|---|---|---|---|
| A | 10 | 0.13 | 0.53 |
| B | 10 | 0.065 | 0.265 |

**Table 4:** AMD parameters[14]

Based on that, those parameters and assumption were run in a simulating tool, over some important areas over Europe:27E-9W&34N-62N and USA:65E-127E&23N-50N, the results also were compared with previous study within the same area but using different simulating tool, as shown in Figure (9), for the purpose of validation.

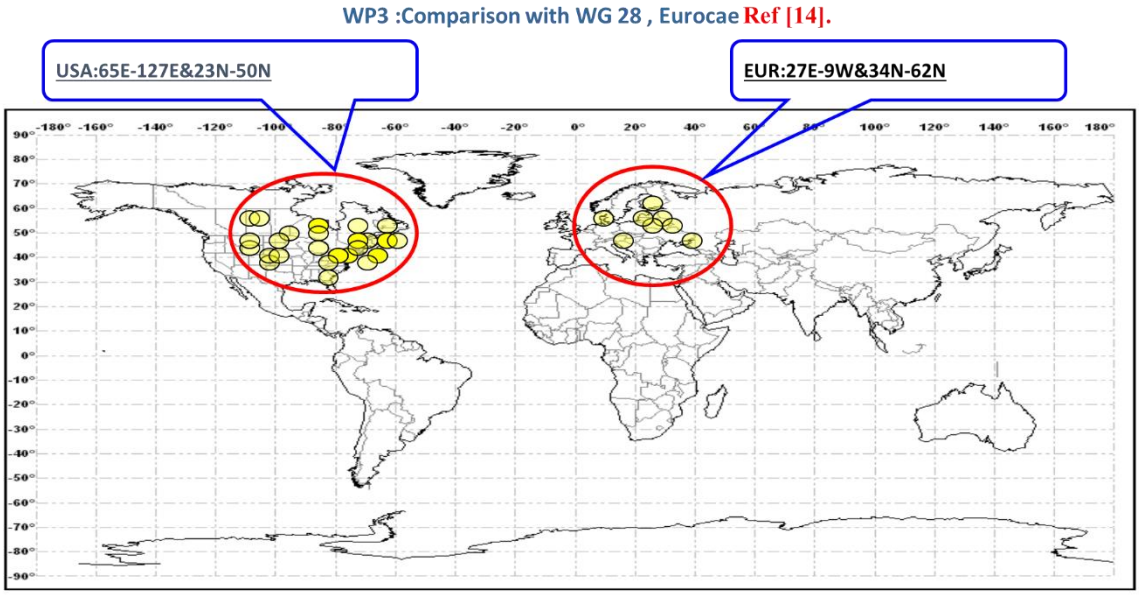



**Figure 9:** the simulated areas in Europe and USA[14]

The Impact of the Analogy Multipath was examined against the GBAS availability to see to which mitigation level the CAT II/III can be achieved. And the results were as shown in Fig (10): [14].

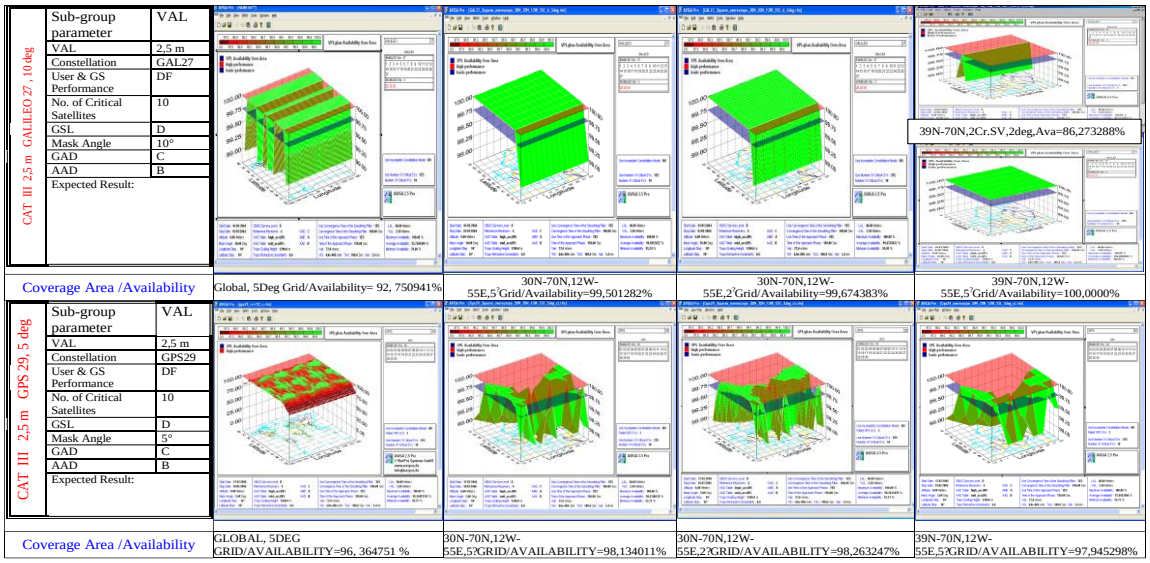



**Figure 10:** Simulation Results[edited by the author]

And they can be summarized as follows:

1. Galileo constellation was able to meet the aeronautical requirements of both 99,99% and 99,75% over Europe only with the given input parameters of the best GBAS configuration of CB-DF and for VAL= 2,5M (CAT III requirements), and it was very close (99,404%) over USA. But GPS was not able to meet these requirements.
2. GPS constellation is not guaranteed, this means that the green spot of good availability is continuously moving and cannot be assured over a certain geographic area like a specific airport for example, while we can warrantee that using Galileo Constellation.
3. Galileo constellation guaranteed the availability of 100% over a fixed areas of the globe, these areas look like stripes belts bounding the earth over a certain latitudes depending on the input parameters that have been used.
4. Availability of Galileo constellation in terms of GBAS application over Europe is better than over USA.
5. Results were validated with the results of WG-28 using the same parameters but different simulator tool. They are similar (with 0,02%) due to the parameters used to compute the availability; this ensures and validates the work also.

However, mitigation methods could be classified to the following three types:

1. Receiver-based mitigation methods: Which includes; firstly, the Correlator Techniques such as the Standard Correlator in which the early-late autocorrelations spaced with (1) one chip spacing; and the Narrow Correlator in which the early-late autocorrelations spaced with (0.1) of chip spacing. Secondly, the Signal Structure Techniques; mainly the new Binary Offset Carrier (BOC) Spreading of the power spectrum, that places a small amount of additional power at a higher frequency in order to improve the signal tracking performance, that leads to the decreasing the multipath error. Also the (BPSK)

spreads the power with a rectangular pulse shape and spreading code chip rate of 1,023 MHz around the center frequency L1. BOC type signals are usually expressed in the form BOC (fshift, fchip) where frequencies are indicated as integer multiples of the GPS C/A.

2. Antenna-based mitigation methods: such as Flat Antenna Array, Curved Antenna Array Stack Antenna, and the Array Curved (B) Antenna Array. Those types are basically creating Nulls toward the chirp jammers and reduces their effect on the main lobe, its functional looks like as protection by deception. Figure (11).

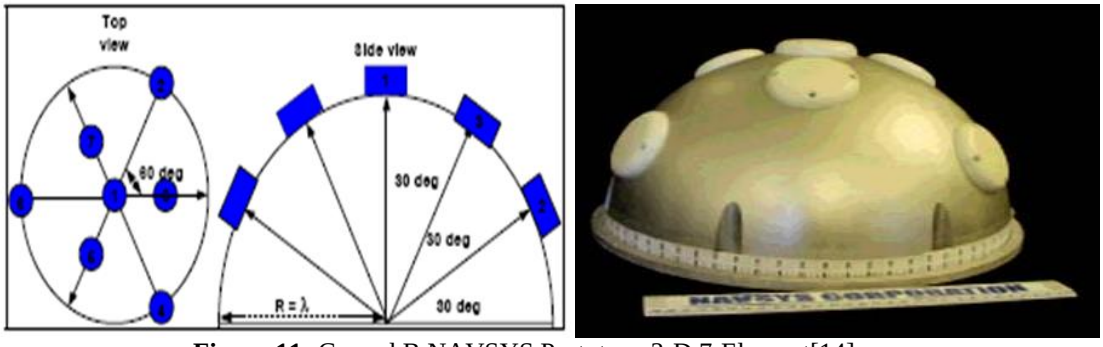
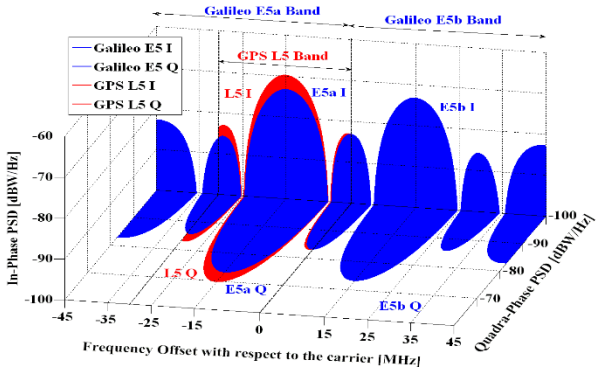



**Figure 11:** Curved B NAVSYS Prototype 3-D 7-Element[14]

1. And Finally; the Sitting-based mitigation methods: As per the Sitting Criteria proposed by ICAO or FAA regulations concerning GBAS systems. They were put mainly to prevent multipath reflections and unintentionally interferences caused by the nearby obstacles and metal surfaces. As well as other Harmonics of Adjacent transmissions of Radars and common used frequencies bands.

Inasmuch of the promising new signal structures and higher power coming down the road, the interference (both Multipath and EAs) impact on GBAS availability is expected to be mitigated to a significant degree. In this study, this mitigation level was simulated optimistically as A/10 value (one tenth of the amplitude of the genuine desired signal). Fig (12). The GNSS modernization will be 6dB more power with new modulation schemes (BOC) as follows:

1. GPS block IIF/M, P/Y code, used currently by US Army, but they are classified.
2. GPS Block III satellites carrying GPS 2022, [16].
3. Galileo, new planned signal structure 2022, [8].




| Designation | Bandwidth (MHz) | Allocation |
|---|---|---|
| L5-band | 1164–1188 | L5 (GPS) |
| | 1188–1214 | E5 (Galileo) |
| L2-band | 1215–1239 | L2 (GPS) |
| | 1237–1260 | G2 (GLONASS) |
| | 1254–1258 | E4 (Galileo), narrow band |
| | 1260–1300 | E6 (Galileo) |
| L1-band | 1559–1563 | E2 (Galileo), narrow band |
| | 1563–1587 | L1 (GPS) |
| | 1587–1591 | E1 (Galileo), narrow band |
| | 1593–1610 | G1 (GLONASS) |

**Figure 12:** Galileo and GPS new Frequency plan for different services[8; 16]

## CONCLUSIONS

In this study; the EA in NAVWAR was evaluated in terms of concept, impact and mitigation techniques. The Analogy of interference of signals at the Receiving Antenna and inside Receiver Signal processing were addressed between different types of EA and Multipath interference. Furthermore, the Impact of EA on GBAS was analyzed over Europe and USA using The Multipath approach mitigation levels. The required performance of GBAS for aviation Requirements can be met by Galileo, but not by the current GPS, especially for CAT-II/III performance. This is because of the less errors affecting the availability of Accuracy and Integrity invoked by EA or (MP Analogy) compared to GPS. However, Galileo will use more signal power and better Signal structure than Current GPS. Current Military GPS uses P/Y coding which is less affected by EA, but not open to non-USA folks. That's means the EA mitigation techniques using robust signal structure and robust signal processing are more effective than those techniques used in Antenna based or sitting based, nevertheless, both are important are important and have their significant contribution in Interference (Multipath and EAs) mitigation.

## BIBLIOGRAPHY

[1] Inside GNSS, "GNSS Jamming and Spoofing: Hazard or Hype? ", June, 4, 2018; https://www.space-of-innovation.com/gnss-jamming-and-spoofing-hazard-or-hype/, Downloaded on 6th March 2019.

[2] Military Embedded Systems, Navigation Warfare Article, Nov. 2015, "special report on Navigation/GPS Technology in Military Application, Link: https://www.novatel.com/assets/Documents/Navigation-Warfare-Article.pdf, downloaded on 9th March 2019.

[3] Field Manual (FM) 3-36, Army doctrine for electronic warfare (EW) planning, NATO, Washington DC; Nov 2012, available on the link : https://armypubs.us.army.mil/doctrine/index.html; downloaded on 27th Feb. 2019

[4] Zsolt Haig, ELECTRONIC WARFARE IN CYBERSPACE. Security and Defense Quarterly, 7(2), 2015 pp22–35; https://securityanddefence.pl/pdf-103299-36215?filename=ELECTRONIC%20WARFARE%20IN.pdf; downloaded on 27th Feb. 2019.

[5] James T. Curran , Michele Bavaro , Pau Closas , Monica Navarro, "On the Threat of Systematic Jamming of GNSS" conference paper, researchgate, September 2016.

[6] Bernd Eissfeller, G. Ameres, Victoria Kropp, Daniel Sanroma." Performance of GPS, GLONASS and Galileo", ION, Jan. 2007, Research gate website https://www.researchgate.net/search.Search.html?type=publication&query=Performance%20of%20GPS,%20GLONASS%20and%20Galileo, downloaded on the 10th March 2019.

[7] Manuel Cuntz, Andriy Konovaltsev, Achim Dreher, and Michael Meurer . "Jamming and Spoofing in GPS/GNSS Based Applications and Services – Threats and Countermeasures", Springer-Verlag Berlin Heidelberg 2012, presented in Future Security conference 2012, CCIS 318, pp. 196–199, 2012.

[8] European Space Agency ESA, Galileo Navigation website, 18 Oct 2018, latest news, https://gssc.esa.int/navipedia/index.php/Galileo_Future_and_Evolutions, downloaded on 11 March. 2019.

[9] European Space Agency ESA, Galileo Navigation website, 18 Oct 2018, latest newshttps://www.esa.int/Our_Activities/Navigation/Contract_signing_to_boost_performance_and_security_of_Galileo_services, downloaded on 11 March. 2019.

[10] B. Hofmann-Wellenhof, H. Lichtenegger, J. Collins ,"Global Positioning System Theory and Practice" ,Fifth, revised edition, Springer-Verlag Wien GmbH, New York, 2001.

[11] David Adamy, "EW 103: Tactical Battlefield Communications Electronic Warfare", 2009, Artech House. London.

[12] JP 3-13.1, Electronic Warfare, Feb 2012, website: https://apps.dtic.mil/dtic/tr/fulltext/u2/a562410.pdf, downloaded on the 16th March 2019

[13] Zsolt Haig, "CONVERGENCE BETWEEN SIGNALS INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT MEASURES. Revista Academiei Forţelor Terestre Nr. 3 (75)/2014 pp 327-335 http://www.armyacademy.ro/reviste/rev3_2014/HAIG.pdf

[14] Alhosban Ahmad, "Impact of Multipath Error On the availability of Integrity In GBAS Application", 2006, France/Germany Project, published in ICG Expert meetings Dec 2015 Vienna Austria by UNOOSA, and ResearchGate websites: http://www.unoosa.org/pdf/icg/2015/presentations/19.pdf

[15] GPS Signal jammed in Norway and Finland , 2018, https://www.news.com.au/technology/innovation/military/gps-signals-jammed-norway-finland-warn-pilots-russia-may-blind-their-navigation-systems/news-story/ee28be793012e9b9e66d59ffba439242

[16] Official U.S. government information about the Global Positioning System (GPS) and related topics, GPS.gov, website: https://www.gps.gov/policy/cooperation/#russia, latest seen news, downloaded on 6th Mar 2019.