The Minimum Operational Range in Spoofing GNSS-Based Navigation Clients

Ahmad Esmaeilkhah[1]

[1] Electrical Engineering Department, Engineering Faculty, Urmia University, Urmia, Iran

*Ahmad Esmaeilkhah, E-mail: a.esmaelkhah@urmia.ac.ir

Abstract

Deception of navigational subsystems of a client, ranging from a hunting GPS receiver to the military-class GNSS receiver onboard of a Cruise Missile, is one of the probable electronic attacks. One of the simplest and practical way too deceive these receivers is to re-broadcast the delayed navigational signals. The authors were studied the feasibility of this method in the "Best" attainable conditions while the generality of study retained. The results from introduced geometrical and mathematical models were used to define the minimum and maximum operational range of Repeater Deception System parametrically. Then the parameters were substituted by information of various GNSS constellations. Investigation of reliability of selected EW scenario concluded the article.

1. Introduction

Spoofing, the art of embedment or even substitution of acceptable but wrong information in place of the original one, is one of the key techniques which was and is used to deceive the receivers' processing infrastructures including human minds and electrical processing systems. Sun Tzu[1] believes any conflict is based upon a method of deception, which dates back to 500BC [1]. The Trojan War is one of the oldest use of a tool, a wooden hoarse, to deceive the opponents' decision-making infrastructure [2]. A detailed investigation of history reveals its rich records of use of this method [3, 4, 5].

By advent of GNSS[2] and penetration of its application in commercial, military and also many aspect of everyone's daily life, the threat of navigational spoofing is becoming an important and worrying issue[6]. The importance of this menace is mostly because of any interfere in authenticity of satellite-based navigation systems could disrupt the transportation system [7, 8], disarrange remote sensing infrastructures and corrupt the accuracy of military instrumentations [8]. Any of these can threat local or domestic security of a country.

The American version of GNSS, the Global Positioning System[3], has introduced with and Anti-Spoofing, or simply AS, capability which is under continuous operational use from 1994[9]. But the AS is only available for authorized military grade GPS receivers [9]. This means commercial users can be spoofed using a simple transmitter which regenerated the original navigational codes of observable GPS satellites [10]. This was first reported in 2017, but was never accepted or rejected officially [11].

The 1023 bit of GPS Course/Acquisition Code[4] can be regenerated and be retransmitted at rate of 1Mbps [10, 12]. As for GPS receivers which start to operate in Hot Start Mode, such as cell phone GPS receivers, the Almanac Data will not be processed [13], the regenerated navigational codes, such as C/A code, can be deceptive if delayed accurately. Theoretical and practical predictability of position of GNSS satellites in their constellation beside the availability of detailed information about navigational signals, their structure and also the way in which a GNSS receiver acquires its position, these navigational signals are theoretically and practically regenerate-able[i.e. 10, 12].To obtain an operationally acceptable GPS spoofing system and to regenerate the mentioned codes considerable amount of researches, data gathering and data processing are required, which will result in higher cost of GPS Spoofing systems and their associated processing, synchronizing and control infrastructures.

But there are another approach to obtain similar results. The spoofing is not directly related in generation of navigational code of selected GNSS constellation. The code(s) must be generated to deceive the GNSS receiver which use them to acquire its position by triangulation using relative delays of received navigational signals, for instance the C/A code [10]. So the deception operation will be successful if the spoofing system could precisely manipulate the timing of generated signals. Thus initial complicated problem can be simplified if the GPS signal generation to be omitted. This low-cost and easy-to-fabricate spoofing system, which will be called as Repeater Deception System or RDS throughout this paper, slightly amplifies the original navigational signals and after manipulation of its timing, re-broadcasts it. For example, as the GPS uses CDMA[5] method for sharing the propagation channel, the amplification of its signals is not so easy but theoretically and practically achievable [14].

[1] Chinese philosopher, strategist and author of "The art of war"
[2] Global Navigation Satellite System
[3] or simply the GPS
[4] Which is abbreviate as C/A code throughout the paper
[5] Code Division Multiplex Access

The method seems to be completely practical and some of related work about its development and even its deployment is published [14]. But this ideal method of electronic warfare must have some inherent limitative properties which one of them will be discussed here. Finally the question of "What is the Minimum Operational Range of this system?" will be answered.

2. Materials and Methods

2.1. The "Best Case" Method of Modeling

To investigate the issue, there are some considerations which must be dealt first. The most important of them all is the unavailability of actual and detailed information about operationally approved GNSS spoofing system such as RDS(s). The classified information about these EW[1]-related systems is not published officially and unofficial available information are not reliable. Also the dynamic nature of mechanical properties of GNSS constellations, such as the relative position of satellites in respect to a predetermined point of reference on Earth requires the problem to be simplified while generality of study to be preserved.

As we want to determine the lower limit of operational range of RDS, the study must be preformed as all the related parameters are adjusted in their "Best" conditions. Then resulted operational range will be judged logically. As the problem is studied in its "Best" but probably unachievable condition(s), the "Real" problem results will deviate from calculated ones, which worsen the situation. It is highly suggested to investigate the issue as a RDS operator which tries to spoof a flying airborne platform equipped with a GNSS receiver.

2.2. The Problem; Description and Simplifications

The original problem is too sophisticated to be studied directly. To reduce the complexity and to find a suitable insight into the problem, some assumptions are required to be considered. These assumption will not reduce the generality of the study and all of them comply with "Best Case Conditions[2]". The summery of assumptions are listed in Tab. 1 at the end of this section

2.2.1. The GPS Receiver

There are various types of commercial and military-grade GPS receivers with different capabilities, but their military-grade capabilities are out of interest[3]. Also due to BCC, it is assumed the GPS receiver is under influence of RDS regardless of its distance and altitude. This assumption eliminates the effect of RDS power, the characteristic of antennas of RDS transponder and GPS receiver, associated error of RDS tracking system, GPS receiver sensitivity and its anti-jamming capabilities. In reality all of these parameters are effective and are worsening the operational conditions. For example, limited capability of GPS receiver to detect the RDS signal limits the operational range of the RDS. Elimination of these parameters will not reduce the generality of study and most of them can be considered later.

2.2.2. Propagation Channel and Associated Considerations

The actual propagation channel is impossible to be modeled exactly. There are some prediction method which can be used to predict the effect of terrain in attenuation of RDS signals along their path to reach the flying GNSS receiver [i.e. 15]. But due to assumptions which mentioned in 2.2.1, the effect of terrain can be neglected.So to achieve the "Best" attainable conditions, the Earth is considered as a smooth sphere without any obstacle and terrain. Also the atmosphere assumed to be homogenous in azimuth and elevation. These considerations discard the effect of any atmospheric discontinuities such as rain, fog, cloud, etc. For an RDS operator, these are the best conditions for spoofing a GNSS receiver.

2.2.3. The Platform

As described in 2.1 the GNSS receiver is considered to be installed on board of an airborne platform. The type of platform is not important theoretically, but as most probable EW operations are against the airborne platforms, such as UAVs[4] and Cruise Missiles, this type of carrier is selected which generates better insight into the problem. Also as the effects of terrains are discarded, a ground-based platform can assumed as an airborne one at altitude equal to zero[5]; so the generality of study has been preserved.

The platform's structural complexity is out of interest because it has no effect on results of spoofing operation against described GNSS receiver while the assumptions of 2.2.1 to be used. The most important of them is the ability of RDS to amplify the received GNSS signals.

As mentioned in 2.1, the issue investigated as a RDS operation who tries to counter an airborne platform which is equipped with a GNSS receiver. In practical cases the inbound flight is more important than the outbound route. If we consider the flying platform as a Cruise Missile, there is not outbound flight and it will hit the target or start its automatic destruction procedure at the end of inbound flight. On the other hand, if we assume the inbound flying threat is an UAV, it will do its recognizance mission during the inbound flight and will send the acquired information using space-based satellite relays. The attack UAVs, also, the operation will be done at the end of inbound flight. Based on the complete equality of importance of introduced analyses for these routs, both of them have been selected for representation of results and the main is the practical importance of them.

---

[1] Electronic Warfare

[2] These conditions will be abbreviated as BCC.

[3] Mostly because of unavailability of confirmed information about these capabilities and their functionality of real electronic warfare environments.

[4] Unmanned Air Vehicles

[5] There are some instance of this type of application of jammers in recants conflicts, i.e. the use of Helium-filled Zeppelin-like balloons as high altitude but stationary carrier of jamming infrastructures.

2.2.4. The Repeater Deception System

Ideally, the RDS repeats the received GNSS signals. The received signals will be amplified sufficiently, will be delayed precisely and will be re-broadcasted. So the received and transmitted signals are identical in contained information, but the transmitted signals have been amplified slightly and delayed accurately. For instance, link budget calculation for Block IIR GPS satellites shows the nominal available power for GPS signal in L1 frequency band[1] is about -130dBm. So the precise amplification of signals is a challenging issue and must be considered for practical deployment.

Tab. 1. List of categorized assumed conditions

#	Assumption	BCC	Category
1	The GNSS receivers operate in their normal mode of operation.	N/A	GPS
2	The GNSS receiver is under influence of RDS regardless of its distance and altitude.	YES	
3	The amplification is not distortive and its gain is logically acceptable.	YES	Repeater Deception System
4	The introduced delay is adjustable. This is an inherent feature of RDS.	N/A	
5	The Earth is assumed as spherical body without any terrain and obstacle.	YES	Propagation Channel
6	Atmosphere assumed to be homogenous in azimuth and elevation.	YES	
7	Inbound airborne is selected.	YES	Platform
8	The carrier's structural complexity and its effect on the received signal from RDS by GNSS receiver is neglected.	YES	

2.2.5. The Applicability of Assumptions

As the mentioned, some assumptions are selected to simplify the problem. So the applicability of them and the condition in which they are applicable are an important issue. To clarify, some discussion is required.

- GNSS receiver's normal mode of Operation: this assumption is due to lack of confirmed information about specification and functionality of military-grade GNSS receivers. Obviously, the RDS operational range will be smaller for these receivers.
- Unconditional Influence of RDS: In reality, the RDS has limited output power. On the other hand, the GNSS receiver's sensitivity is not infinite. This assumption ensures the RDS effects the GNSS receivers while it is within its LoS[2] range.
- Ideal RDS functionality: This is, really, an attainable feature. It is important to fine tune the amplification gain in respect with distance between the RDS and inbound carrier. Otherwise the GNSS receiver's pre-amplifier will be saturated and the onboard processing infrastructure could detect the EW operation. This usually result in discarding the GNSS output and reliance on INS system.
- Smooth spherical Earth: The Earth is not Smooth nor spherical. But due to limited range of real RDS, which is about tens of kilometers at its maximum, and curvature of the Earth. Also the RDS operator installs the system somewhere with maximum coverage area, i.e. over a mast. These facts validates this assumption, at least for RDS coverage area.
- Homogenous atmosphere: In general, is atmosphere can be considered as a homogenous medium, regardless of its condition, within the RDS coverage range in most of times. Obviously, the rain and fog can attenuate the RDS signal and worsen the conditions. So if the weather condition is varying fast, the calculated RDS operational range should be revised in accordance with correspondent weather attenuation.
- Assumptions about the platform are discussed thoroughly in 2.2.3.

3. Mathematical Modeling

To start the mathematical modeling of problem, an exactly defined scenario which determined the position of observer, the position of selected GPS satellite in respect with the observer and location of the RDS is needed. The selected framework should be as close as possible to the real conditions.

3.1.1. The Scenario and Its Compliance with BCC

To construct a suitable scenario, an arbitrary point on the surface of the Earth is selected as the stationary ground-based target which is spotted and is nominated as "A". The facilities which located at "A" are equipped with a RDS which is in compliance with conditions of 2.2.4. The altitude of the RDS will be discussed later but it has isotropic coverage[3]. Also the observer is stationary and located at "A" too. This observer is operator of RDS and tries to do his/her "Best" to deceive the incoming precision-guided platform which is equipped with a GNSS receiver, as described in 2.2.1.

The observer choses a visible GNSS satellite so the RDS will re-broadcast its navigational signals with adjusted delay. Logically the observer choses the satellite with strongest and most clear signal. As all of the GNSS satellites of a certain category are identical and flying at almost same altitudes and due to considerations of 2.2.2, the selected satellite will be the possible closest one. The closest possible distance of the observer and the satellite will happen if the satellite passes exactly overhead of the observer. This is the "Best" possible condition for the observer to tune his/her RDS. Let's take a snapshot of this situation. The snapshot is essentially important because the selected satellite is not stationary and

[1] ~1575.42 MHz

[2] Line of Sight range.

[3] In reality the RDS could use a directional antenna and required tracking infrastructure. To eliminate these complexities, an isotropic coverage assumed for the installed RDS.

for GPS constellation this will happen in about every 12 hours for it. The snapshot can be seen in Figure. 1.

3.1.2. Redefining the Problem by Mathematical Models

Using the established scenario of 3.1.1, the problem is ready to be mathematized. First of all, it is required to calculate the theoretical "Upper-limit" of delay of RDS. Then the "Inherent" and "Requested" delays will be introduced. Investigation of spoofing mechanism finalizes the modeling procedure.

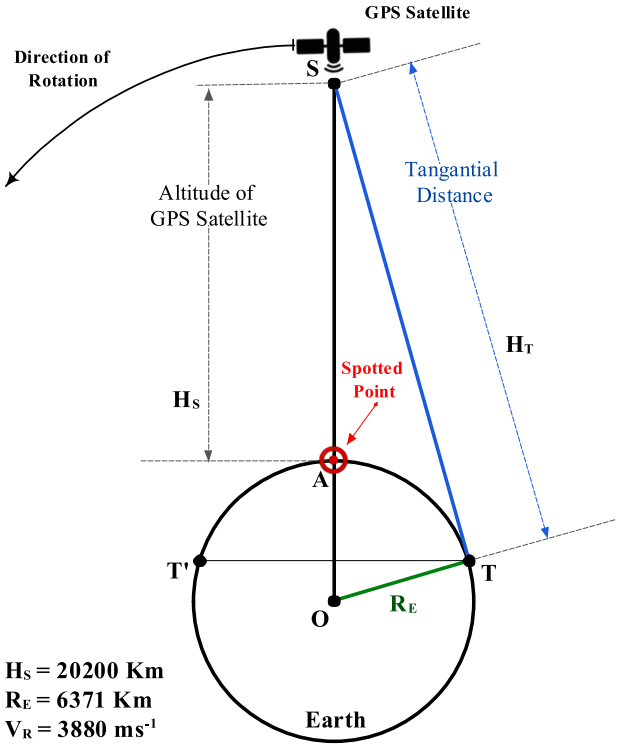

Figure. 1. The Snapshot of the selected scenario. Without lose of generality, the GPS has selected as navigational constellation and V_R is the orbital speed of satellite.

3.1.2.1 The Upper-Limit of RDS Delay

This is a geometrically-forced limitation which is a function of constants such as radius of the Earth, altitude of satellite over the surface of the Earth and propagation speed of electromagnetic fields in atmosphere. If the satellite transmits a signal, the observer at "A" will receive it first and the observers at T and T' will receive delayed versions of it. Assuming the altitude of GNSS satellite as H_S, the radius of Earth as R_E and using some geometric calculus the maximum valid delay of the received signal can be calculated.

$$\Delta H_{\max} = H_S\left(\sqrt{1+\frac{2R_E}{H_S}}\right)\times 10^{+3} \quad \text{(m)} \quad (1)$$

$$\Delta T_{\max} = \frac{\Delta H_{\max}}{v_p} = \frac{H_S}{v_p}\left(\sqrt{1+\frac{2R_E}{H_S}}\right) \quad \text{(Sec)} \quad (2)$$

Where v_p is the propagation speed of transmitted electromagnetic signals through the atmosphere and will be assumed to be equal to speed of light in vacuum. Substitution of given values of Figure. 1 for R_E and H_S in (2) will result in $\Delta T_{max} \approx 9.8$mSec. This is the maximum acceptable amount of delay for any ground based observer which receives navigational signals of GPS constellation. Obviously any received signals which delayed more then mentioned value can be discarded by the ground-based receiver easily.

3.1.2.2 Inherent and Requested Delay

There is an essential properties of RDS which must be taken into account. The RDS, just like any other LTI system, has its "Inherent" delay. This delay, which is required for received signal to be propagated through RDS subsystems for filtering, amplification and any other analog or digital processes, is a natural specification of system and the user has no control over it. So the introduced delay of a RDS system, which will be shown by ΔT, is consist of two independent parts: the "Inherent" delay, or t_γ, and the "Requested" delay or t_δ. So

$$\Delta T = t_\gamma + t_\delta \quad \text{(Sec)} \quad (3)$$

Which the t_δ is adjustable. Obviously the minimum achievable delay is governed by the inherent delay of RDS.

3.1.2.3 Modeling the Spoofing Mechanism

As the observer at "A" tuned its RDS to receive, amplify, delay and re-transmit navigational signals of selected satellite, all of nearby GNSS receivers will receive the delayed signal. The delayed signal simulates the original navigational signal form selected satellite(s) but at distances equal to R around the RDS. Figure. 2 illustrates the geometrical arrangement of described issue.

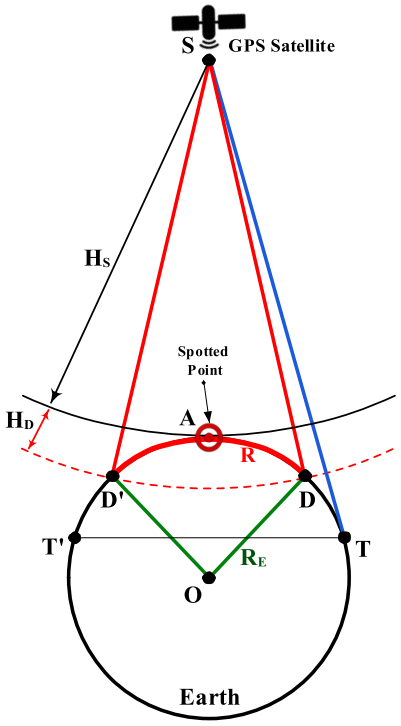

Figure. 2. Snapshotted geometrical arrangements to calculate the spoofing results. GPS constellation is selected as an example and the model is valid for any GNSS system.

So the observers which are located in a circle of radius of R around the RDS will receive navigational signals of the satellite and of the RDS simultaneously. But the deceptive transmitted signal of RDS is slightly stronger and it will replaced the original one which is weaker. Obviously the value of R is dependent to the value of delay and some geometric parameters as

$$R = R_E Cos^{-1}\left(1-\frac{H_D\left(H_D+2H_S\right)}{R_E\left(R_E+H_S\right)}\right) \quad \text{(Km)} \qquad (4)$$

Which H_D is the extra length generated by the introduced delay. All the parameters must be substituted in kilometers.

4. Results and Findings

To investigate the issue, the Minimum Operational Range, or R_{min}, must be defined. Due to the curvature of the Earth, the maximum line-of-sight coverage range of RDS, the R_{max}, can be calculated as:

$$R_{\min} < R_{\max} \le R_{LoS} = 1.23\left(\sqrt{h_{RDS}}+\sqrt{h_{Platform}}\right) \qquad (5)$$

Which h_{RDS} is the altitude of RDS over the spotted point and the $h_{Platform}$ is the nominal altitude of flying platform which is equipped with suggested GNSS receiver, both in meters. So if an airborne platform nears the spotted point of "A", it will be under direct influence of the RDS form R_{LoS} kilometers away. This limits the maximum acceptable delay of RDS which its calculation is out of scope of this article.

Theoretically the R_{max} can be equal to calculated LoS range, but it is hard to achieve or even impossible in practice. This is due to existence of obstacles and terrain on the surface of the Earth. On the other hand, the R_{min} is supposed to be equal to zero, covering the spotted point and its adjacent areas. Let's check how ΔT determined in R_{min}. Obviously for any obtained value of ΔT, the original signal transmitted by satellite is required travel H_D kilometers more, shown in Figure. 2, to reach the Earth surface.

$$H_D = \Delta T.v_p \times 10^{-3} \quad \text{(Km)} \qquad (6)$$

At D and D' both of the original signals and the re-broadcasted one have similar phase shift in respect with original signal at "A". The ΔT consists of two parts, as described in 3.1.2.2, and the most important of them is the Inherent delay. So if the observer at point "A" adjusts t_δ=0 then $\Delta T=\Delta T_{min}= t_\gamma$. The ΔT_{min} is the minimum achievable delay. So $H_{D\min} = t_\gamma.v_p \times 10^{-3}$. Substitution in (1) results in:

$$R_{\min} = R_E Cos^{-1}\left(1-\frac{H_{D_{\min}}\left(H_{D_{\min}}+2H_S\right)}{R_E\left(R_E+H_S\right)}\right) \quad \text{(Km)} \qquad (8)$$

Figure. 3. Illustrated the R_{min} for seven major international or local space-based navigation systems. As seen the R_{min} increases non-linearly as the Inherent delay of RDS increases. As seen the dependency of R_{min} to the altitude of satellite of each constellation, causes different but almost identical curves for 6 of them. The Iridium constellation is located at LEO orbit and the altitude of its satellite is 1/6 to 1/3 of the others, H_S≈781Km. Operating at lower altitudes cause smaller values of operational range for RDS while re-broadcasting signals of this constellation.

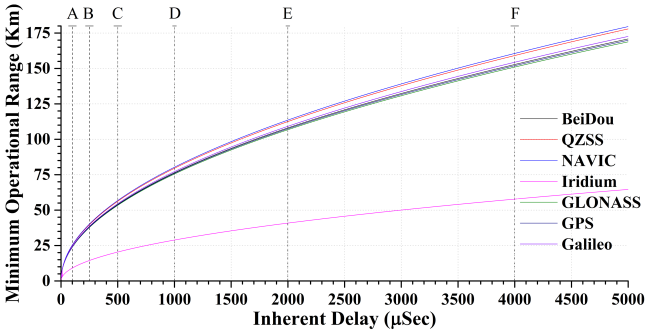

Figure. 3. The Minimum Operaional Range for RDS with differect inherent delays.

If a RDS with t_γ=500ηs is tuned to receive and re-transmit signals of GPS constellation, its minimum operational range is 53.73Km. This means the minimum addressable deceptive range is 53.73Km and all the nearby receivers will be drifted along one axis as much as mentioned above. The worst constellation which the RDS may be tuned on is NAVIC and its minimum operational range is 56.78Km. The curves of Figure. 2 are marked at 0.10, 0.25, 0.50, 1.00, 2.00 & 4.00 microsecond and the correspondent values of four major space-based navigation system beside of the Iridium constellation are listed in Tab.2.

Tab. 2. The calculated minimum operational range of RDS at marked values of its inherent delay as shown in Figure. 3.

Measurement Points		Minimum Operational Range of RDS for Different Navigational Constellations (Km)				
Code	t_γ (µSec)	BeiDou	Iridium	GLONASS	GPS	Galileo
A	0.10	24.15995	9.13288	23.87183	24.027	24.411
B	0.25	38.20029	14.4405	37.74473	37.990	38.598
C	0.50	54.0235	20.4225	53.37924	53.727	54.586
D	1.00	76.40114	28.8832	75.49002	75.982	77.197
E	2.00	108.0485	40.851	106.76006	107.45	109.17
F	4.00	152.8066	57.7832	150.98451	151.96	154.39

5. Discussion & Suggestions

To investigate the effect of minimum operational range of RDS on efficacy of its electronic warfare operation against the described GNSS receiver, three different issues should be taken into account. First of all, the relative flight direction of the flying platform in respect with spotted point of "A" as inbound or outbound is important. The installation altitude of the RDS and altitude of flying platform, which effect the R_{max}, are effective parameters too. And finally, the inherent delay of RDS, which controls the R_{min}, is the most important of them all. To simplify the investigation procedure, the installation altitude of RDS and of flying platform is assumed to satisfy the (5). Although it is almost impossible to meet this assumption, but it simplifies the problem without lose of generality. In this way, the flying platform's GNSS receiver is always receiving signals form RDS while $R<R_{max}$. To

reduce ambiguity, the "inbound" and "outbound" terms will be re-defined and be investigated separately.

5.1. The Rational behind Selected Scenarios

One important question is: "why these three scenarios, as listed in Tab. 3 and described thoroughly in 5.2 and 5.3, are important? To answer, some operational insights into the rational behind the conduction of airborne operations are required. The various approaches to do that are

- The inbound flight operation could be categorized into attack operations using cruise missiles or suicide drones and UAVs, low-cost one-way recognizance flying platforms and high altitude passing recognizance aircrafts during its approach phase of flight.
- The outbound flight could be an opponent's UAV which takes off from battlefield while is under direct influence of a tactical RDS, a passing high altitude recognizance aircraft while is in its outbound phase of flight or an allied flying vehicle which is, by mistake, under direct influence of an allied RDS and is in its outbound route toward its target(s).

Any other operational flights could be modeled using these two categories or could be simplified to fit within them.

5.2. Deception of Inbound Flying GPS Receiver

The "inbound" flying platform starts its flight at distances greater than R_{LoS}. So the onboard GPS receiver acquires its correct position first and will be spoofed when its carrier enters the line-of-sight region. The observer at "A" calculates the propagation time of RDS's signals to reach the flying platform and starts to adjust the ΔT to drift it. For the proposed GNSS receiver the (3) can be expressed as

$$\Delta T = t_{\gamma} + t_{\delta} + t_{propagation} \qquad (9)$$

The $t_{propagation}$ is the required time for re-broadcasted signal to reach the GNSS receiver. Obviously $t_{propagation}$ decreases as the flying platform nears the spotted point. Also as the large values of adjusted t_{δ}, which produce considerable drifts, alerts the processing infrastructure of the flying platform, the observer tries to adjust or increase it progressively. Logically the amount of induced drift must be comparable to inherent drift of other onboard navigational systems such as Inertial Navigation System. Typically when the R_{LoS} is small, the larger values of t_{δ} were suggested to produce desired drift. But as long as the R_{LoS} is long enough, the progressive change of t_{δ} results in desired effects.

In "Best" case of conditions, the GNSS receiver receives the deceptive signals of RDS when it enters the line-of-sight perimeter. Assuming the GNSS receiver to be spoofed and drifted when it enters the R_{min} circle, the RDS transponder cannot compensate the propagation time of signals, as the final minimum value of delay will be t_{γ}. A simple comparison of output of auxiliary navigational systems such as INS[1], TERCOM[2] or DSMAC[3] and of GNSS receiver will alerts the processing infrastructure of the flying platform which will discard its spoofed navigational results.

5.3. Deception of Outbound Flying GPS Receiver

The "Outbound" flying platform, starts to fly from a location within R_{min} range of spotted point and moves outward. As the initial operational status of RDS is influencing the reasoning, it will be investigated separately:

- If the RDS has been turned off initially, the onboard GNSS receiver acquires its location precisely. But when the observer at "A" turns the RDS on, he can not adjust the proper value of t_{δ} to compensate the inherent and propagation delays. This will cause considerable change in GNSS receiver navigational output, which can be used to invalidate them.
- The RDS has been turned on long ago and the GNSS receiver start its location acquisition using spoofed signals. As the observer at "A" can not adjust proper t_{δ} while the GPS receiver is within the R_{min} range of the spotted point, the flying platform's navigation systems has constant drift equal to R_{min} till it passes R_{min} kilometers off the spotted point. So the initial electronic warfare against it is successful, but detectable.

As summery, Tab. 3 listed the electronic warfare operation described in 5.1 and 5.2.

Tab. 3. Final results of spoofing a flying GNSS receiver using an RDS in "Best" attainable conditions.

The Scenario	Electronic Warfare Status
Inbound flying GNSS receiver.	Fails if flying platform enters the R_{min} circle to hit the spotted point or to cross over the area.
Outbound flying GNSS receiver - RDS has been turned off initially.	Fails upon EW operation starts.
Outbound flying GNSS receiver - RDS is fully operational prior to platform flight.	Successful unconditionally but detectable while the flying platform range form RDS is less than R_{min}.

5.4. Suggestions

Due to the established "Best Case" conditions, the real situation is worse than what have been described and, for example, the R_{min} is much less than what is calculated here. But there are some practical suggestion for observer at "A" which can help him to succeed in EW operation against flying platform.

First of all, installation of RDS far away off the spotted point is highly suggested. By defining the distance of RDS form spotted point to be equal to

$$D_{RDS} = R_{\min} + \frac{R_{\max} - R_{\min}}{2} (\text{Km}) \qquad (10)$$

And naming the area between the R_{min} and R_{max} as the RDS Operational Ring, the location of spotted point should

[1] Inertial Navigation System

[2] Terrain Contour Matching

[3] Scene-Mapping Area Correlator

be selected near the center of this ring, as far as possible. Obviously the RDS can be installed far from threat-side for safe operation. But to obtain more operational efficacy it is suggested to install the RDS near the threat front[1]. Also due to (5), to maximize the R_{LoS} and subsequently the R_{max}, the RDS should be installed at altitudes as high as possible. Figure. 4 illustrate the suggested arrangement.

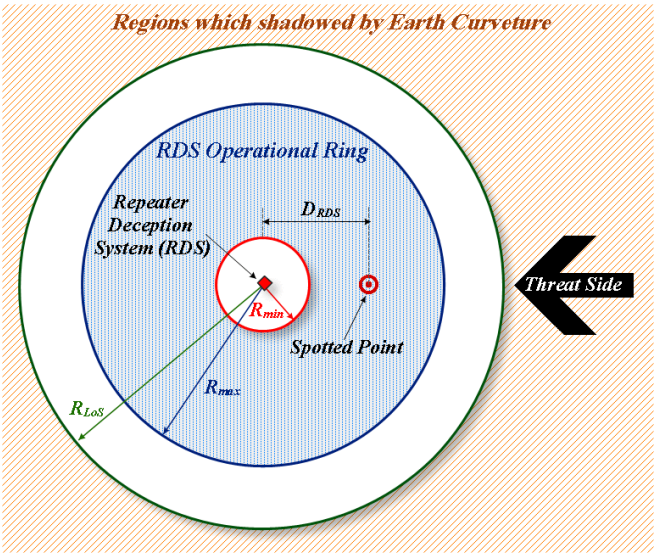

Figure. 4. The suggested arrangement of RDS in respect with targeted spot and threat side

6. Conclusion

To investigate the inherent limitations of spoofing the GNSS-based navigational subsystem of a client, the issue was investigated in "Best Case" conditions while the selected assumptions were chosen as the generality of study retained. First of all the geometrical model of a hypothetical GNSS system was extracted parametrically. The resulted data were used to develop the mathematical model of described spoofing method using a simple but precisely arranged scenario. The inherent delay of Repeater Deception System introduces a lower limit to its Operational Range, the R_{min}, while its upper limit governs by the line-of-sight range, the R_{LoS}. The R_{min} were calculated for five international and 2 local space-based navigation systems and were presented figuratively. Finally, the selected scenarios of inbound and outbound flying platform were investigated. The results were shown the installation of RDS over the spotted point reduce the efficacy of electronic warfare operation. Finally some suggestions were provided to conclude the article.

References

[1] Giles. Sun Tzu on the Art of War, *Abingdon, Oxon: Routledge, 2013.*

[2] Homer, The Iliad, *Edited by: R. Lattimore, R. A. Lattimore, ISNB: 0226469409, University of Chicago Press, 1961*

[3] Ch. F. Bond, M. Robinson, The evolution of deception, *Journal of Nonverbal Behavior 12(4):295-30, DOI10.1007/BF00987597, December 1988*

[4] Y. Bassil, Steganography & the Art of Deception: A Comprehensive Survey, *Int. Journal on Latest Trends Computing, Vol ‐ 4 No. 3: 128-138, September 2013*

[5] M. A. Peters, The History and Practice of Lying in Public Life, *Review of Contemporary Philosophy, Vol. 14:47-61, 2015, ISSN 1841-5261*

[6] T. E. Humphreys, et al. "Assessing the spoofing threat: Development of a portable GPS civilian spoofer." *Proceedings of the ION GNSS international technical meeting of the satellite division. Vol. 55. 2008.*

[7] T. E. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing." *University of Texas at Austin, 2012*

[8] Kerns, Andrew J., et al. "Unmanned aircraft capture and control via GPS spoofing." *Journal of Field Robotics vol. 31, no.4, pp. 617-636, 2014.*

[9] A. Jafarnia-Jahromi, et al., "GPS Vulnerability to Spoofing Threats and a Review of Anti spoofing Techniques," *International Journal of Navigation and Observation, vol. 2012, Article ID 127072, 2012.*

[10] *W.L. Garfield, TACAN: a navigation system for aircraft, Proceedings of the IEE - Part B: Radio and Electronic Engineering, Volume: 105, Issue: 9, 1958*

[11] W. Zhang, K Zhang, B. Wu and H. Suh, "Simulation and Analysis Acquisition of GPS C/A Code Signals in GPS System", *International Symposium on Computer Network and Multimedia Technology,. CNMT 2009,, Wuhan, China, 2009.*

[12] D. Hambling, "Ships fooled in GPS spoofing attack suggest Russian cyber weapon", *New Scientists, vol. 3139, 19 August 2017.*

[13] J. Bao, Y. Tsui, "GPS C/A Code Signal Structure, Fundamentals of Global Positioning System Receivers: A Software Approach*", Ch. 5, John Wiley & Sons, Inc. ISBN 0-471-38154-3, 2000.*

[14] G. Blewitt, "Basics of the GPS Technique: Observation Equations", *Geodetic Applications of GPS, the Swedish Land Survey, 1997.*

[15] Y.B. LIU, et al. "Efficiency Analysis of Repeater Deception Jamming GPS Repeater [J]." *Journal of Air Force Radar Academy 4,* 2004.

[16] M. E. Johnson, et al. "Comparison of measured data with IF-77 propagation model predictions". *National Telecommunications and Information Administration Boulder Co Institute for Telecommunication Sciences, 1979.*

[17] A. Esmaeilkhah and N. Lavasani, "Jamming Efficacy of Variable Altitude GPS Jammer against Airborne GPS Receiver, Theoretical Study and Parametric Simulation", *AEM*, vol. 7, no. 1, pp. 57-64, Feb. 2018.

[1] Threat front could be defined as the direction in which the penetration of opponent's flying systems is predictable and more probable.