УДК 621.396.669

GPS COMPLEX INTERFERENCE MODELS AND THE POSSIBLE ANTI-SPOOFING PROTECTIVE MEASURES

SAAD H. KH., STUPIN K. V.

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Беларусь)

E-mail: HusseinSaadTENG@outlook.com, stupin@bsuir.by

Аннотация. GPS приемники подвергаются различным типам преднамеренных и непреднамеренных помех. Из-за очень слабого сигнала, передаваемого спутником GPS, он больше уязвим для подавления и спуфинга, чем для других источников непреднамеренных помех. Спуфинг считается наиболее опасной и сложной атакой, связанной с GNSS (Спутниковая система навигации), способом, который приводит к неправильным решениям в PVT (позиция, скорость, время) в целевом GPS-приемнике. В этой статье будут описаны сложные модели помех GPS, рассмотрены часто наблюдаемые инциденты, математическое моделирование помех GPS, математические соотношения для закона временной задержки и управления доплеровским сдвигом частоты и другие параметры с результатами моделирования.

Abstract. GPS receivers are being exposed to different types of intentional and unintentional interference. Due to the very weak signal transmitted by the GPS satellite, it is very vulnerable to jamming and spoofing attacks rather than the other unintentional interference sources. Spoofing is considered the most dangerous and complex attack dealing with GNSSs, the way which lead to wrong PVT solutions in the targeted GPS receiver. Complex GPS interference models will be shown in this article, highlighting the most registered incidents, the mathematical modelling of GPS interference, mathematical relations for the law of time delay and Doppler frequency shift control and other parameters with the results of modelling.

Problem statement

Examining the success or the failure of a GPS spoofing act depends on many features and parameters related to the navigation process, taking in consideration the number of targeted receiver(s) (single or multi-receivers) in addition to the signal's strength transmitted power, the distance between the spoofer and the victim, the time offset, Doppler shift, delay locked loop bandwidth, etc. To sum up, mathematical compensation formulations will be done to study the possible ways in order to differentiate between the possible GPS spoofing success and failure, to attain at the end the best methodology that should be followed to meet our aim in GPS spoofing.

Many GPS spoofing incidents have been registered in the modern technological history. The most famous cases known either on the air or land or sea vehicles are shown in the following:

Regulus Tesla Spoofing Experiment; Regulus Cyber spoofed a Tesla Model 3 off the road during a test drive using Navigate on Autopilot (NOA) [1].

"Ghost ships" circle off San Francisco coast; data analyst Bjorn Bergman discovered nine ships broadcasting false GPS signals from Point Reyes, just north of San Francisco, California [2].

Iran-U.S. RQ-170 incident; on December 5, 2011, Iranian forces commandeered a U.S. Lockheed Martin RQ-170 Sentinel stealth drone flying about 140 miles from Iran's border with Afghanistan [3].

University of Texas researchers steer multimillion dollar yacht off its course; the experiment took place as the 213-foot yacht traveled across the Mediterranean Sea from Monaco to Greece [4].

On the other hand, GPS jamming cases are also recorded, some of which are: an intermittent GPS signal loss experienced by aircraft landing at Harbin airport in north-eastern China is traced to a jammer installed at a nearby pig farm [5]; Mexico passes an anti-jammer law, discovered that GPS jammers are being in 85% of cargo vehicle thefts in the country [6].

Note that another GPS spoofing and jamming attacks happened, but we just list the most famous registered ones focusing on the more complex (spoofing).

Mathematical Modelling for the Complex GPS Interference

In general, the consumer's navigation equipment will function in the presence of multipath, jamming, false navigation signals generated by one or more sources of spoofing, noise interference and internal noise of receiving channels. GPS spoofing can be defined as transmitting fake GPS navigation messages to the targeted receiver in order to interrupt the position, navigation, and time solutions of the desired receiver, thus wrong position. While GPS jamming is simple than spoofing, which is briefed in emitting the same frequency as that of the navigation satellite (NS) with a suitable level of power and estimated distance, the way which lead to interrupt the navigation signal leading to the nulling of the available signals from different satellites. Furthermore, multipath is an unintentional interference which results from the reflection of the GNSS signals when hitting an obstacle as a tower, building, etc. Noise either external or internal is considered as a normal case of unintentional interference due to the thermal noise, noise figure and others in the receiver's equipment and other cases related to the surroundings and AWGN. In our modeling, we will assume that the CNE antenna system includes $\ell = \overline{1, L}$ receiving channels with coordinate vectors of phase centers $\boldsymbol{\eta}_\ell(t) = (x_\ell(t), y_\ell(t), z_\ell(t))^{\mathrm{T}}$, where the dependence on time t reflects the law of motion of the center of mass of the consumer's equipment and the possible rotational movements of the antenna system of the equipment. The distances between the phase centers and the geometric center of the antenna system with $\boldsymbol{\eta}_0(t)$ coordinates are such that $|\boldsymbol{\eta}_\ell - \boldsymbol{\eta}_0| << c / \Delta f_0$, where Δf_0 - is the width of the navigation signal spectrum. The coordinate vector $\boldsymbol{\eta}_0(t)$ defines the phase center of the antenna system and is used to simplify the description of the navigation signals' time delays.

The coordinates of the $k = \overline{1, K}$ NSs are $\boldsymbol{\mu}_k(t) = (X_k(t), X_k(t), Z_k(t))^{\mathrm{T}}$. Signs of visibility of NSs $V_k^{ns} = 0$, if the satellite is below the horizon line (not visible) and $V_k^{ns} = 1$ if the satellite is above the horizon line (visible). The time index is omitted in this case, since it is assumed that the visibility conditions of the satellites do not change during the analysis.

To describe multipath propagation when the signal of the k -th NS is reflected from some object (area), we assume that the reflected signal comes to the receiving channel from some point in space $\boldsymbol{\mu}_k^{\mathrm{mul}}(t)$ with a time delay τ_k relative to the true signal. The scale factor for the amplitude of the reflected signal is $\dot{\Gamma}_k$, where the argument $\varphi_k = \arg(\dot{\Gamma}_k)$ takes into account both the reflection from the object and the delay during multipath propagation.

Destructive effects are created by $m = \overline{1, M_{jam}}$ sources of jamming with $\boldsymbol{\nu}_m(t) = (X_m^{jam}(t), Y_m^{jam}(t), Z_m^{jam}(t))^{\mathrm{T}}$ coordinate vectors and $n = \overline{1, N_{sp}}$ sources of false navigation signals (spoofing) with $\boldsymbol{\upsilon}_n(t) = (X_n^{sp}(t), Y_n^{sp}(t), Z_n^{sp}(t))^{\mathrm{T}}$ coordinates. Each of the sources of false navigation signals can create $V_{n,k}^{sp}(t) = 1$ or not create $V_{n,k}^{sp}(t) = 0$ false navigation signal from the k -th NS, and these conditions may change during observation.

The received implementation at the output of the ℓ -th receiving channel can be represented as:

$$\dot{Y}_\ell(t) = \underbrace{\sum_{k=1}^{K} V_k^{ns}\dot{S}_k(t)\dot{F}_\ell(\boldsymbol{\mu}_k)}_{\text{true signals}} + \underbrace{\sum_{k=1}^{K} V_k^{ns}\dot{\Gamma}_k\dot{S}_k(t-\tau_k)\dot{F}_\ell(\boldsymbol{\mu}_k^{\mathrm{mul}}(t))}_{\text{multipath}}$$

$$+ \underbrace{\sum_{n=1}^{N_{sp}}\sum_{k=1}^{K} V_{n,k}^{sp}(t)\dot{W}_n(t,k)\dot{F}_\ell(\boldsymbol{\upsilon}_n)}_{\text{spoofing}} + \underbrace{\sum_{m=1}^{M_{jam}} \dot{U}_m(t)\dot{F}_\ell(\boldsymbol{\nu}_m)}_{\text{jamming}} + \underbrace{\dot{N}_\ell(t)}_{noise}, \qquad (1)$$

where $\dot{S}_k(t)$ is the true navigation signal from the k -th NS at the output of the isotropic receiving antenna; $\dot{F}_\ell(\mathbf{v})$ is the radiation pattern of the ℓ -th receiving channel in the direction of a point with Cartesian coordinates $\mathbf{v}$, and the phase of the radiation patterns is counted from the common phase center for all elements of the antenna system; $\dot{W}_n(t,k)$ is the false signal of the k -th NS generated by the source of spoofing at the output of the isotropic receiving antenna; $\dot{U}_m(t)$ - interference from the m -th source of jamming at the input of an isotropic receiving antenna; and $\dot{N}_\ell(t)$ - intrinsic noise of the ℓ -th receiving channel with a power of $\sigma_\ell^2 = \overline{|\dot{N}_\ell(t)|^2} = \sigma_0^2$.

The model (1) is universal and allows reproducing a large number of situations characterized by different conditions of multipath propagation, the presence of one or more sources of spoofing and jamming, in addition to external and internal noise interference. Further complication of the model is achieved by: increasing the number of beams for multipath propagation of true signals and introducing multipath propagation for false navigation signals; introduction of polarization parameters of true and false navigation signals (including multipath) and jamming and the use of vector radiation patterns of receiving channels in a given polarization basis.

Let's write down the components of the model (1). For the true signal from the k -th NS:

$$\dot{S}_k(t) = \sqrt{P_k}\, C_k(t + \tau_k^{ns} - t_{r_k}) D_k(t)\, \mathrm{e}^{j((\omega_0+\Omega_k(t))t+\varphi_k)} , \qquad (2)$$

where P_k is the signal power from the k -th NS at the output of the isotropic receiving antenna, determined by the distance to the satellite and the conditions of propagation of electromagnetic waves; $C_k(t) = -1;1$ is the rangefinder code of the k -th NS; τ_k^{ns} is the offset of the time scale of the k -th NS relative to the time scale of the navigation system; $t_{r_k} = |\,\boldsymbol{\mu}_k(t) - \boldsymbol{\eta}_0(t)\,| / c$ is the signal delay from the NS to the CNE's antenna; c - is the speed of propagation of electromagnetic waves; $D_k(t) = -1;1$ is a true navigation message, the spectrum width of which is much smaller than the spectrum width of the rangefinder code; ω_0 - is the carrier frequency, for the GPS system $f_0 = \dfrac{\omega_0}{2\pi} = 1575,42$ MHz; $\Omega_k(t) = 2\pi \dfrac{d}{dt} |\,\boldsymbol{\mu}_k(t) - \boldsymbol{\eta}_0(t)\,|$ - is the Doppler frequency shift of the signal from the k -th NS; φ_k - is a random but constant phase shift of NS signal during the observation interval.

For the false navigation signal of the k -th NS created by the n -th source of spoofing, we write:

$$\dot{W}_n(t,k) = \sqrt{P_{n,k}^{sp}}\, C_k(t + \tau_n^{sp} - t_{n,k}^{sp}) D_{n,k}^{sp}(t)\, \mathrm{e}^{j((\omega_0+\Omega_{n,k}^{sp}(t))t+\varphi_{n,k}^{sp})} , \qquad (3)$$

where $P_{n,k}^{sp}$ is the power of the false signal of the k -th NS created by the n -th source of spoofing at the output of the isotropic receiving antenna; τ_n^{sp} - the time scale offset of the n -th source of suffixing relative to the time scale of the navigation system; $t_{n,k}^{sp}$ - is the delay of the false signal of the k -th NS created by the n -th spoofing source; $D_k^{sp}(t)$ is a complex navigation message created by the k -th NS; $\Omega_{n,k}^{sp}(t)$ is the law of change of the Doppler frequency shift; and $\varphi_{n,k}^{sp}$ - the initial phase.

Noise interference $\dot{U}_m(t)$ is a Gaussian random process with a uniform (within the bandwidth of the receiving channels) spectral power density $N_m = P_m^{jam} / \Delta f_0$, where $P_m^{jam} = \overline{|\dot{U}_m(t)|^2}$ is the power of the m -th source of jamming at the output of an isotropic receiving antenna. Interference from various sources and internal noise are uncorrelated $\overline{\dot{U}_m(t)\overset{*}{U}_n(t)} = \delta(m-n)P_m^{jam}$, $\overline{\dot{U}_m(t)\overset{*}{N}_\ell(t)} = 0$, where $\delta(m)$ - the Kronecker symbol.

Note that the model (1) taking into account (2), (3) is universal. By controlling the parameters $P_{n,k}^{sp}$, $t_{n,k}^{sp}$, $\Omega_{n,k}^{sp}$ in (3) in terms of spoofing, the parameters $\dot{\Gamma}_k, \tau_k, \boldsymbol{\mu}_k^{mul}$ in (1) in terms of multipath propagation, as well as the parameters $P_m^{jam}, \mathbf{v}_m$ in terms of jamming, situations of any complexity can be reproduced.

General Anti-Spoofing Measures

The results of the analysis of well-known and universal works on countering GPS spoofing in CNE shows that the general principle of constructing protection methods is to perform four operations which are summarized in figure 1.

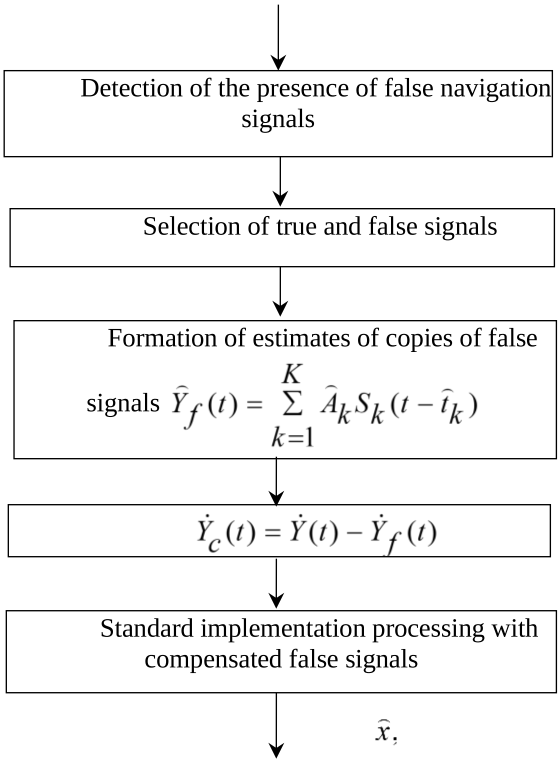
Detection of the presence of false navigation signals
Selection of true and false signals
Formation of estimates of copies of false signals $\hat{\dot{Y}}_f(t) = \sum_{k=1}^{K} \hat{A}_k S_k(t - \hat{t}_k)$
$\dot{Y}_c(t) = \dot{Y}(t) - \dot{Y}_f(t)$
Standard implementation processing with compensated false signals
$\hat{x}$,

Fig. 1. General structure of the GPS-spoofing protection algorithm

The basis of this sequence is evaluation and compensation processing, which allows using the well-proven structure of consumer navigation equipment in the coherent reception of navigation signals.

When selecting true and false signals, two situations must be taken into account:

- before the appearance of spoofing or jamming, the consumer equipment functioned normally and the time scales of the navigation system and equipment were aligned; sufficiently high accuracy of the alignment of the time scales will be maintained during the time interval determined by the stability of the frequency of the master generator of the navigation equipment; an increase in the mismatch of the time scales can be taken into account in (2) if the parameter τ_k^{ns} is made dependent on the current time t;
- navigation equipment begins to function in conditions of spoofing or jamming and the coordination of time scales has not been completed.

For the first of these situations, estimates $(\hat{x}, \hat{y}, \hat{z})$ will be determined, for the second- $(\hat{x}, \hat{y}, \hat{z}, \hat{t})$.

As we have said previously, some countermeasures should be followed in order to minimize the risk of the illegal use of GPS spoofing. Table 1 indicates a list of proposed protective measures against GPS spoofing, either by using a single channel or multi-channel antenna, knowing that the last may be rotational beamforming array antenna or adaptive array antenna (adaptive beamforming).

Table 1: Protection measures against GPS spoofing

Type of navigation equipment	Possible options
Single channel receiver	1. The detection of the presence of two (or more) of signals from one navigation satellite, selection of false signals on the level (amplitude), estimation of time delay, the complex amplitude and phase signals about their subtraction (estimated-compensation processing) of the accepted implementation with the subsequent processing of the implementation in the traditional way. 2. Breeding of false signals in the residual rate of change of time delay and Doppler frequency shift. 3. Selection of false signals based on the content of the navigation message (taking into account the available a priori data). 4. Selection of false signals based on the synchronicity of amplitude changes for different navigation satellites when the antenna is rotated.
Multi-channel receiver	1- Measurement of bearings, thus the phase difference of receiving channels, for detected navigation signals, selection of false signals based on the same set of phase differences and evaluation and compensation processing (estimation of arrival time, complex amplitude and frequency, subtraction of a scale copy of the signal from the received implementation in the selected receiving channel without spatial processing). 2- Measurement of bearings for detected navigation signals, selection of false signals and their spatial compensation (nulling or zeros' formation towards the direction of the GPS spoofing source). 3- Combination of methods 1 and 2 with methods of the first group.

Conclusion

At the end, the general concept of the GPS interference is shown, listing the main incidents registered, showing the main principle of it in addition to the mathematical modeling and formulation, ending with the conclusion including the protection countermeasures. Although GPS spoofing is considered nowadays as the most complex type of intentional interference, but protective measures should be followed mainly against the illegal use of such attack.

References

1. Yonatan Zur, Yoav Zangvil, Jana Wagner, Adi Kremer Hyatt, Stas Gutliansky, Avner Zangvil, David Ramati, Igor Zarivach, Alon Shani, and Yury Ben-Sheer. REGULUS. Ed. REGULUS. 4 August 2019. Regulus Cyber. 4 August 2019 https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-navigation-system-hack-causes-car-to-turn-on-its-own.
2. Jacobs, Frank. BIG THINK. Ed. HARD SCIENCE. 18 March 2021. BIG THINK. 18 March 2021 https://bigthink.com/hard-science/circle-spoofing/.
3. Scott, Peterson. Iran–U.S. RQ-170 incident. Ed. encyclopedia. 5 December 2011. encyclopedia. December 2011 https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident.
4. Zumalt, Erik. UT NEWS. Ed. The University of Texas at Austin. 30 July 2013. SCIENCE & TECHNOLOGY. 30 September 2021 https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/.
5. Dutton, Julian. Gigazine. Ed. Pascal Debrunner. 23 December 2019. December 2019 https://gigazine.net/gsc_news/en/20191223-flight-systems-jammed-pig-farm/
6. Goward, Dana A. "Linked in." 5 December 2020. https://www.linkedin.com. Ed. Guy Buesnel. December 2020 https://www.linkedin.com/pulse/gps-jamming-spoofing-2020-year-review-spirents-guy-buesnel-goward