International Journal of
Technology and
Systems
(IJTS)

Global Positioning System Signal Verification through Correlation Function Distortion and Received Power Tracking

CARI
Journals

Journal of Technology and Systems
ISSN : 2788-6344 (Online)
Vol. 6, Issue No. 3, pp 34 – 51, 2024

www.carijournals.org

Global Positioning System Signal Verification through Correlation Function Distortion and Received Power Tracking

[1*] **Moses Michael Meitivyeki,** [2] **Associate Prof. Haiying Liu**

[1*] Post Graduate Student: College of Astronautics

Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China.

[2] Lecturer, College of Astronautics

Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China.

https://orcid.org/0009-0008-2805-5691

Abstract

Purpose*:* This study proposes a significantly improved method for detecting, classifying, and isolating Global Navigation Satellite System (GNSS) signals using the relationship between the measured power and the distortion of the correlation function to achieve the signal verification required for Global Positioning System (GPS) civil applications such as safe civil aircraft navigation.

Methodology*:* The suggested approach uses power and distortion measurements in the received signal to identify it as jammed, multipath, spoofing, or no-interference. By adding an isolator scaling factor to the detector, the signal patterns will be induced with a unique temporary factor that will set it apart from the rest and make it possible to easily position each signal in its own zone. The detector divides the four signal types into distinct zones for verification.

Findings*:* The sufficient signal data is analyzed and the extensive simulation conducted indicates that about 94% detection accuracy is achieved which is relatively high.

Unique contribution to theory, practice and policy: This study is implemented through the development of relevant detection software tools with a user-friendly interface for GNSS signal detection, validation and analysis.

Keywords: *Gps, Signal Verification, Signal Power, Correlation Distortion, Navigation Safety.*

1. INTODUCTION

The global navigation satellite system (GNSS) is integral to the Communications, Navigation, and Surveillance (CNS) infrastructure. Civil and military aviation are among numerous technical businesses that rely heavily on GNSS for Positioning, Navigation, and Timing (PNT). Such important industries require GNSS's most significant level of service to ensure safety and security. For example, the International Civil Aviation Organization (ICAO) specifies four high-quality requirements for a GNSS service: integrity, accuracy, availability, and continuity.

Signals broadcast via GNSS are inherently vulnerable since they are Radio Frequency (RF) waves that may be attenuated upon landing on the Earth's surface, making them more sensitive to various external attacks, both purposeful and unintended. GNSS signal vulnerabilities can be categorized into physical degradation, intentional and unintentional threats as discussed in (Zidan et al., 2021). Because GNSS signals travel over wireless channels, the ionosphere introduces frequency-dependent delays into the signals. This might result in signals being entirely obscured and unusable for navigation, or it can create Non-Line-of-Sight (NLoS), which occurs when signals are received through a reflected path owing to an obstacle in the Line of Sight (LoS). LoS and NLoS signals reach the receiver in other cases, causing multipath interference. However, deliberate and accidental threats, mostly jamming and spoofing, provide substantial difficulty. Because GNSS signals are below the background noise level at the earth's surface, a small quantity of interference is sufficient to jam the receiver. Aside from military jammers, tactics such as Personal Protection Devices (PPD) are routinely used to deliberately overpower the relatively weak GNSS signal receiver as investigated in (Gao et al., 2016; Karaim et al., 2017), since most commercial receivers nowadays still operate only in the L1 band. Unlike jamming, spoofing is purposeful, in which the spoofer alters the GNSS signal, amplifies it, and rebroadcasts it with minor but significant Position, Velocity, and Time (PVT) anomalies to fool a specific victim, as analyzed in (Ouyang et al., 2015; Wu et al., 2020).

Several ways have been developed to counteract these GNSS dangers utilizing various strategies, as explained, classified, and examined in (D. Fabio, 2015; Jafarnia-Jahromi et al., 2012; Meng et al., 2022). These include but are not limited to, GNSS receiver stand-alone techniques such as receiver measurement consistency checks and Signal quality monitoring (SQM), as well as hybrid positioning receiver techniques such as inertial system and communication system integration. One of the best hybrid strategies for GNSS signal authentication is a power and distortion monitoring methodology provided in (K. Wesson et al., 2016), which forces the spoofer to decide between balancing power and the influence on the distortion function. If the attacker transmits a weak signal, it will either be insufficient to execute the desired spoofing or cause a significant distortion in the correlation function, notifying the anti-spoofer. If the spoofer selects high power, the correlation function is unaffected; nevertheless, the anti-spoofer detects a significant rise in received power. This is a brilliant but flawed technology with a few drawbacks; one is that clean, multipath, jammed, and faked signals have similar power and distortion characteristics, leading to erroneous and missed detections. The overlapping features of the desired and undesirable signals allow accidental interference and hostile jammers and spoofers to trick receivers and detectors.

This research presents an enhanced approach that includes a step for signal isolation into separate zones after identification by applying appropriate scaling factors to signal patterns based on their unique properties in response to the power and distortion function. Adding an isolator scaling factor to the detector will induce the signal patterns with a unique temporary factor that will distinguish them from the others with various aspects and allow each signal to be readily located in its zone. After scaling, the detector will have four zones: clean, multipath, jammed, and faked signals. After gathering the appropriate zones, the scaling factor is reversed to send the original signal to the receiver end user. Since this is a signal detection and monitoring strategy rather than a mitigation technique, the four isolation zones can be utilized to notify the receiver of any dangerous impurities in the GNSS signals. This study uses GPS L1 C/A, the most widely utilized signal for civil aviation and nonmilitary applications.

The rest of the paper is organized as follows. The second section addresses the proposed approach. The third section presents the simulation and performance analysis. Lastly, the paper's conclusion is provided in Section IV.

2. PROPOSED APPROACH

2.1. Modified Signal Model

Prior to beginning the zone separation procedure, the suggested detector checks both the received power and the correlation function distortion.

2.1.1. Power monitoring

We use and adapt the methodology provided in (Wesson et al., 2018) to monitor incoming power. The Automatic Gain Control (AGC) setpoint evaluates power in receivers with AGC-equipped front ends. Receivers that do not require an AGC can directly determine received power by averaging the squared modulus of discrete samples formed from the mix of legitimate and interference signals,

$$P_{meas} \triangleq 10\, log_{10}\left(\frac{1}{T}\int_{t_{k-1}}^{t_k} |\tilde{r}_c(t)|^2\, dt\right) \tag{1}$$

The received power P_{meas} in dB is represented by (1) where $\tilde{r}_c(t)$ is combination of authentic and interference signals exiting the RF front end over the interval from t_{k-1} to t_k accumulated over T seconds

2.1.2. Distortion monitoring.

To monitor the correlation function distortion, we use and adapt the maximum likelihood estimation model introduced in (Gross et al., 2019) and summarized in this section. This approach uses more relevant distortion measurements instead of the symmetric difference metrics utilized in

(Wesson et al., 2018). The general correlation function (2) contains all the complex components, that is, authentic signal $\xi_{Ak}(\tau)$, the interference signal $\xi_{Ik}(\tau)$. and thermal noise $\xi_{Nk}(\tau)$,

$$\xi_k(\tau) = \beta_k[\xi_{Ak}(\tau) + \xi_{Ik}(\tau) + \xi_{Nk}(\tau)] \tag{2}$$

where β_k is the average value of the scaling factor for the received signal. The correlation function's thermal noise component $\xi_{Nk}(\tau)$ is treated as having independent in-phase and quadrature components. Using the maximum likelihood technique to model the correlation function $\xi_k(\tau)$ by considering the interference-free mode, that is, $\xi_{Ik}(\tau) = 0$, the authentic signal correlation function model is expressed as (3),

$$\xi_K(\delta_i) = \alpha_{Ak} \exp(j\phi_{Ak})\, R\, (\delta_i - \tau_{Ak}) + \beta_k \xi_{Nk}(\delta_i) \tag{3}$$

where δ_i is the signal location tap, j is the estimation cost, ϕ_{Ak} is the authentic signal's carrier phase, τ_{Ak} is its code phase and α_{Ak} its gain-controlled amplitude at time index k.

These three important parameters for the correlation function, the gain-controlled amplitude α_{Ak}, the carrier phase ϕ_{Ak} and the code phase τ_{Ak}, are then estimated by maximum likelihood technique by implementing their linear relationship (4) which estimates the code phase from the estimation of the amplitude and carrier phase, where H is the function of the observation matrix,

$$\xi_K = H(\tau_{Ak}, \delta)\alpha_{Ak} \exp(j\phi_{Ak}) \tag{4}$$

Finally, the distortion is computed through the designer's estimates of the component $\tau_{Ak} \rightarrow \tau_{Ak}'$ which leads to the evaluation of the estimates $\alpha_{Ak} \rightarrow \alpha_{Ak}'$ and $\phi_{Ak} \rightarrow \phi_{Ak}'$. Here, the distortion measurement D_{meas} is taken as cost J_k of the estimates $\{\alpha_{Ak}' , \tau_{Ak}' , \phi_{Ak}' \}$ as (5) where Q is the Toeplitz matrix for the complex gaussian thermal noise.

$$D_{meas} = \| \xi_K - H(\tau_{Ak}', \delta)\alpha_{Ak}' \exp\left(j\phi_{Ak}'\right) \|_Q^2 \tag{5}$$

2.2. Signal classification

By monitoring the P_{meas} and D_{meas} , the received GNSS signal can be classified into clean, multipath, jamming or spoofing based on its characteristic reaction to power and distortion dynamic in the first part of the detector. For the first part of the detector, signal classification, the observation vector Z_{obs} in (6) is modeled as a random variable within the observation set based on the received power and the distortion metrics. Using the Bayesian M-ary hypothesis, the same hypothesis H_i, $i \in I_{CL}=\{0,1,2,3\}$ previously proposed in (Gross et al., 2019; Wesson et al., 2018) can be used to classify the signal.

$$Z_{obs} = [D_{meas}, P_{meas}]^T \tag{6}$$

2.2.1. Clean

Clean signal is classified as I_{CL}=0, to represent the desirable interference-free signal. Here the D_{meas} is low since the only the thermal noise is present and the interference power advantage over P_{meas} is zero since it has no effect on observation risk.

2.2.2. Multipath

Multipath is classified as I_{CL}=1, to represent an uncorrelated error which arises when a portion of the satellite signal reaches the receiver after reflections or scattering off the ground or an obstacle. The D_{meas} is low when the multipath is low and increases with its severity. The P_{meas} is lower in multipath since when the authentic signal is not obstructed, it has a higher power output than an echo, whose increased path length and interference with reflective surfaces reduces its output.

2.2.3. Spoofing

Spoofing is classified as I_{CL}=2, to represent the fake signal modified by the attacker. Since successful spoofing requires a spoofing signal to be at least as strong as the authentic signal, the interference power advantage over P_{meas} is taken as at least 1. The D_{meas} for spoofing has a wider range in comparison to multipath.

2.2.4. Jamming

Jamming is classified as I_{CL}=3, to represent interference on frequencies from external sources. Because weaker jamming is both harmless and common enough to be unnoticed, its power advantage over P_{meas} is estimated to be at least 1. Also, since the gain-controlled correlation function is barely affected by jamming, its D_{meas} nearly the same as in clean signal.

2.3. Signal zonal isolation

To improve the detection process and refine the analysis, we propose including a signal zone isolator in the detector's second component. To further comprehend the function of this detector's two primary sections, consider the following hospital example. The first component of the detector, the signal classifier, is similar to categorizing patients into distinct symptomatic groups based on lab test findings. The second component, the zone isolator, is similar to splitting patients into various medical wards based on their classification group to allow for more continuous study.

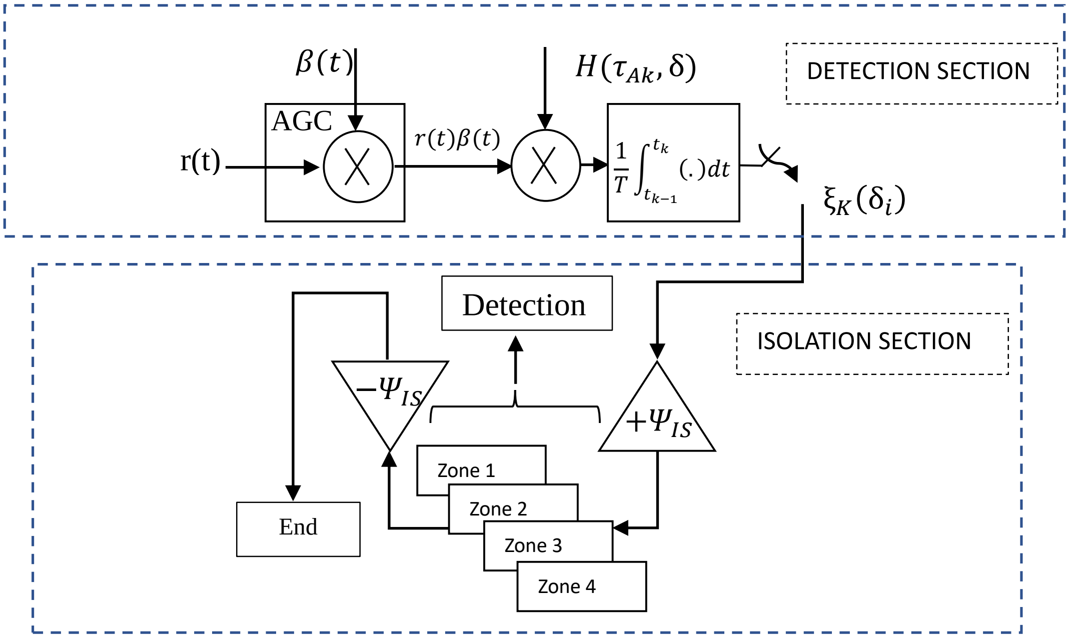


Fig. 1. The framework showing both the classifier and zonal isolator parts of the proposed detector

The $\xi_K(\delta_i)$ will go through the second part of the detector for zonal isolation. For better clarity of signal distribution and zonal isolation, we propose taking advantage of the multipath estimator in (Gross et al., 2017) as a third dimension of the signal distribution. In (7), the zonal isolator Ψ_{IS} is a 3-dimention observation vector with D_{IS}, P_{IS}, MPE_{IS} as distortion, power and their relative multipath estimator values respectively in the isolation state. D_{IS} and P_{IS} are directly passed from D_{meas} and P_{meas} from (6), and MPE_{IS} is from the multipath estimator value. IS_P, IS_D, and IS_{MPE} are the isolation scales for power advantage, distortion and multipath estimation. The isolation scale is decided based on the parameters used in the simulation to set different signals into different zones in 3-dimention space.

$$\Psi_{IS} = [\, P_{IS},\ D_{IS},\ MPE_{IS}\,]^T + [\, IS_P,\ IS_D,\ IS_{MPE}\,]^T \qquad (7)$$

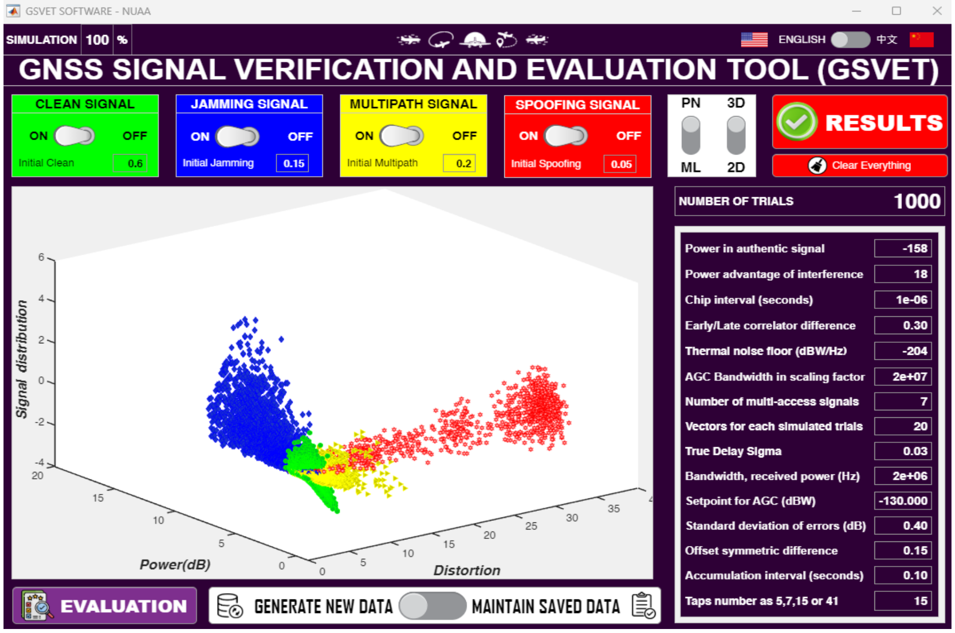
The isolation scale for I_{CL}=0 is [0 0 0] for the authentic signal to remain in the original unaltered zone. For I_{CL}= 1, the IS_D is increased to isolate multipath signal from clean signal zone since the severity of multipath increases with its distortion. For I_{CL}= 3, power scale is increased to cause more spike in the jamming since it's power advantage to the clean signal is at least 1 and unnoticeable for weaker signals. For I_{CL}= 2, all the three scales can be increased based on the pre-established zones in clean, multipath and jamming signals so as to avoid zonal interference. There is no set formula for producing isolation scales. Still, the designer should include a realistic trigger in the above directions for best results to maintain a distinct separation between the zones. Because the power and distortion levels in the isolated zones are triggered and scaled from the genuine signal measurements, all of the established zones are only briefly configured for signal authentication and analysis. After all of the zones have been formed and recorded, the detector negates the isolation scale values, reverting the signal to its unscaled condition before displaying it to the user.

3. SIMULATION AND ANALYSIS

3.1. Simulation setup

We implement the code given in (Gross et al., 2019; Wesson et al., 2018) and modify it per this study proposal. The modified code is then used to develop part of a relevant simulation software in Fig. 1 with a user-friendly interface for GNSS signal detection, validation and analysis.

This software is developed by the authors and has the official copyright. It is only available upon a reasonable request sent to the corresponding author or the institution.



Initial Clean	0.6
Initial Jamming	0.15
Initial Multipath	0.2
Initial Spoofing	0.05
NUMBER OF TRIALS	1000
Power in authentic signal	-158
Power advantage of interference	18
Chip interval (seconds)	1e-06
Early/Late correlator difference	0.30
Thermal noise floor (dBW/Hz)	-204
AGC Bandwidth in scaling factor	2e+07
Number of multi-access signals	7
Vectors for each simulated trials	20
True Delay Sigma	0.03
Bandwidth, received power (Hz)	2e+06
Setpoint for AGC (dBW)	-130.000
Standard deviation of errors (dB)	0.40
Offset symmetric difference	0.15
Accumulation interval (seconds)	0.10
Taps number as 5,7,15 or 41	15

Fig. 2. The interface of the relevant developed detection software tool (GSVET).

3.2. Data Generation

The GNSS receives for civil aviation applications have an acquisition threshold certification as described in (Eurocae, 2023; Novella et al., 2022; RTCA, 2018). To validate the quality of the GNSS signal at the receiver,   in this study, the standard GPS L1 C/A parameters are set and the signal data is generated, which will be used for classification and analysis.

The parameters are set to simulate data using the same configuration as used in the real data provided in TEXBAT dataset (Humphreys et al., 2012), and utilize it for spoofing detection performance analysis based on the proposed approach. TEXBAT is a battery of recorded spoofing scenarios has been compiled for evaluating civil Global Positioning System (GPS) signal authentication techniques. The battery can be considered the data component of an evolving standard meant to define the notion of spoof resistance for commercial GPS receivers. Signal data is simulated from the corresponding software in *Fig. 2,* and will be utilized for classification and analysis.

To generate this data, we run 6 extensive Monte-Carlo simulations of 100,000 trials each with the same parameters. Four simulations are of individual non scaled isolated signal outputs as clean, multipath, jamming and spoofing. The other two simulations are of all signals in their isolated zones after $+\Psi_{IS}$ and non-isolated zones after $-\Psi_{IS}$. Power in authentic signal is set to -158 dBW, power advantage of interference signal used is 18 dB, thermal noise floor of -204 dBW/Hz and the standard deviation of in-band power measurement of 0.4dB. Setpoint for AGC on which the incoming signal will be scaled is -130 dBW, bandwidth over which the received in-band power is measured is 2MHz and bandwidth over which the AGC operates is 20MHz. The number of non-authentic multi-access signals is set to 7, chip interval of 1µs with an accumulation interval of 0.1s and the number of taps is set to 15. Zone isolation parameters are in *Table 1*. Other parameters including the decision regions classification matrix are as in original code.

All the simulations were run on an 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz 2.80 GH 64-bit operating system, x64-based processor, 32.0 GB RAM machine for about 21 hours and recorded about 102GB of data. The visualization of the recorded data is presented in *Fig. 3 to Fig. 5.*

Table 1

Zone isolation scale parameters

Scenario	**Power advantage scale,** $\boldsymbol{IS_P}$ **(dB)**	**Distortion function scale,** $\boldsymbol{IS_D}$	**Multipath estimator scale,** $\boldsymbol{IS_{MPE}}$
Clean	0	0	0
Multipath	0	1,500	0
Jamming	3	0	0
Spoofing	5	100	10,000

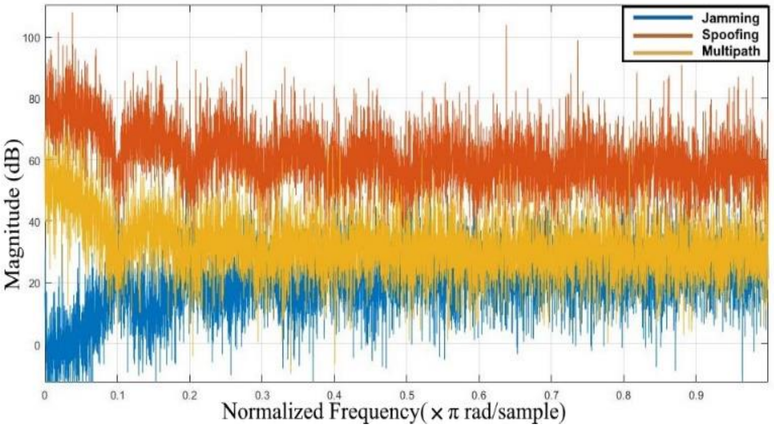


Fig. 3. Visualization of magnitude response for simulated jamming, spoofing and multipath signal in blue, red and yellow respectively.

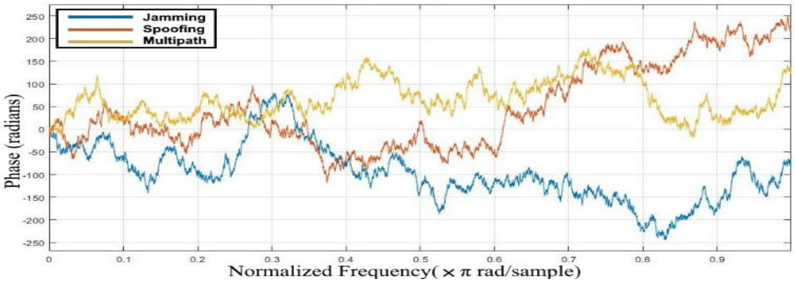


Fig. 4. Visualization of phase response for simulated jamming, spoofing and multipath signal in blue, red and yellow respectively.

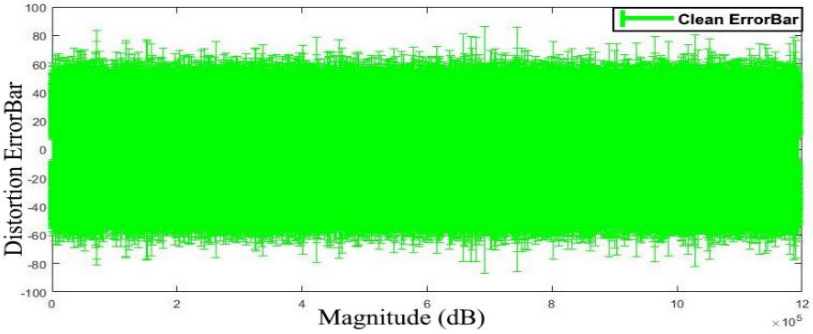


Fig. 5. Visualization of error bar of the simulated clean signal data.

3.3: Results analysis

The output from the detection software for the isolated zones after the application of $+\Psi_{IS}$ is presented in *Fig. 6* showing the signal distribution in their isolated zones in relation to the power, distortion and multipath estimator. *Fig. 7* shows the non-isolated signal distribution after the application of $-\Psi_{IS}$. Since the clean signal zone is not scaled, that is $[IS_P,\ IS_D,\ IS_{MPE}]^T$ = [0 0 0], the green zone is with exact measurements of the power and distortion for the no-interference signal.

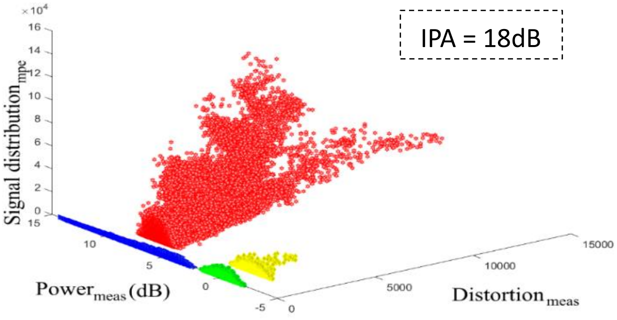


Fig. 6. GPS signal isolated to clean, jamming, spoofing and multipath zones in green, blue, red and yellow colors

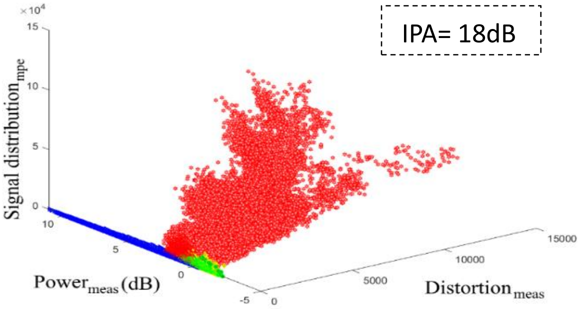


Fig. 7. GPS signal in non-isolated state as clean, jamming, spoofing and multipath in green, blue, red and

Further simulation is conducted by adjusting the Interference Power Advantage (IPA) from as low as 10dB to as high as 20dB while other parameters are set as mentioned earlier. The results presented in *Fig. 8* shows the isolation of interfered and clean signal is successful at all tested power advantages.

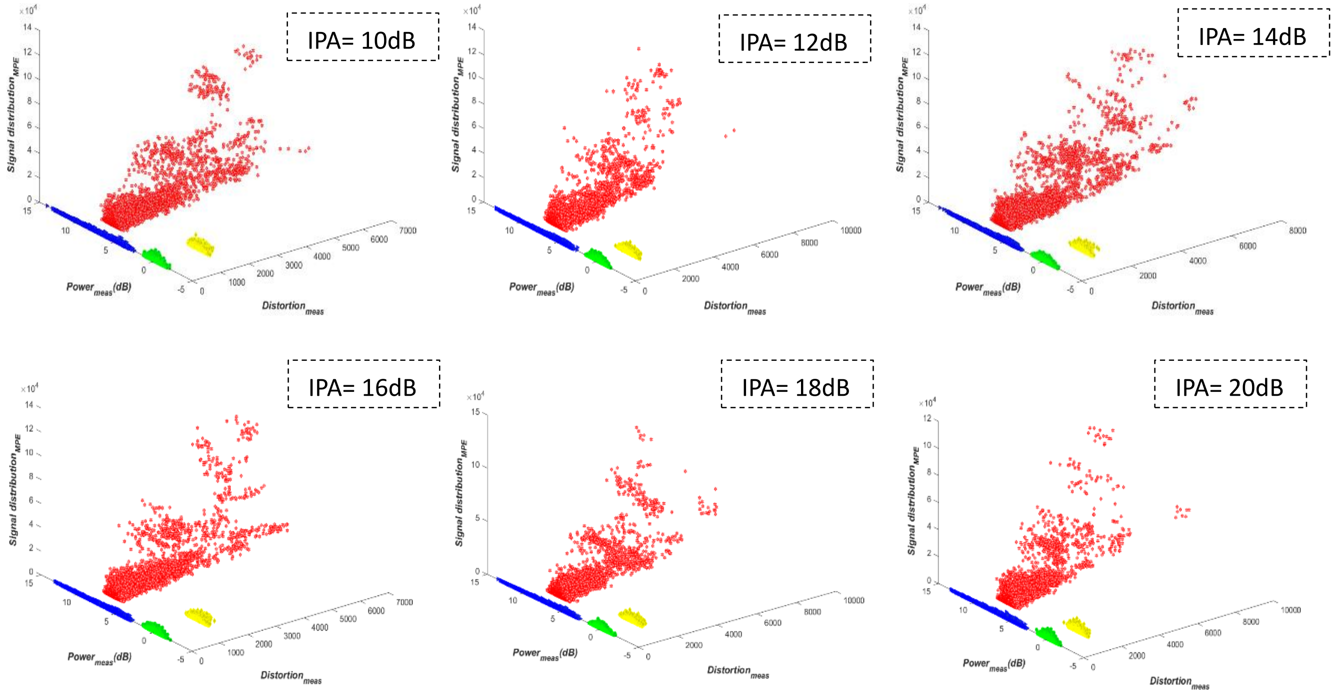


Fig. 8. GPS signal distribution in individual zones classified as clean, multipath, jamming and spoofing from left right, top down. X = Power, Y =Distortion and Z = Distribution(MPE)

The individual interference-free zone, depicted in *Fig. 9 (top left)*, is our target region for a good GNSS signal. In the isolation state, there is no misclassification of multipath and interference-free zones, independent of the error cost, even though the two zones have almost identical shapes in all three dimensions in their isolated zones. *Figure 9 (top right)* shows the individual zone for multipath in the non-isolated condition. Compared to the multipath estimator, the interference-free zone begins low, rises, and falls as more power is applied. However, the jamming zone maintains its existence to a more significant power advantage of roughly 14 dB, including the scaled value, before fading away. *Figure 9 (bottom left)* shows the unscaled jamming signal distribution in the non-isolated state. Spoofing and clean signals are separated in the isolated state, unlike in the non-isolated state. *Figure 9 (bottom right)* depicts the spoofing signal zone in its non-isolated form. It has been noticed that when the spoofer utilizes less power advantage, the spoofed signal, although interfering with the clean signal zone, has substantially more significant distortion than the detector detects. In the instance where the spoofer employs a more considerable power advantage, even while the signal distortion interferes with the clean signal, the power is substantially higher and more noticeable.

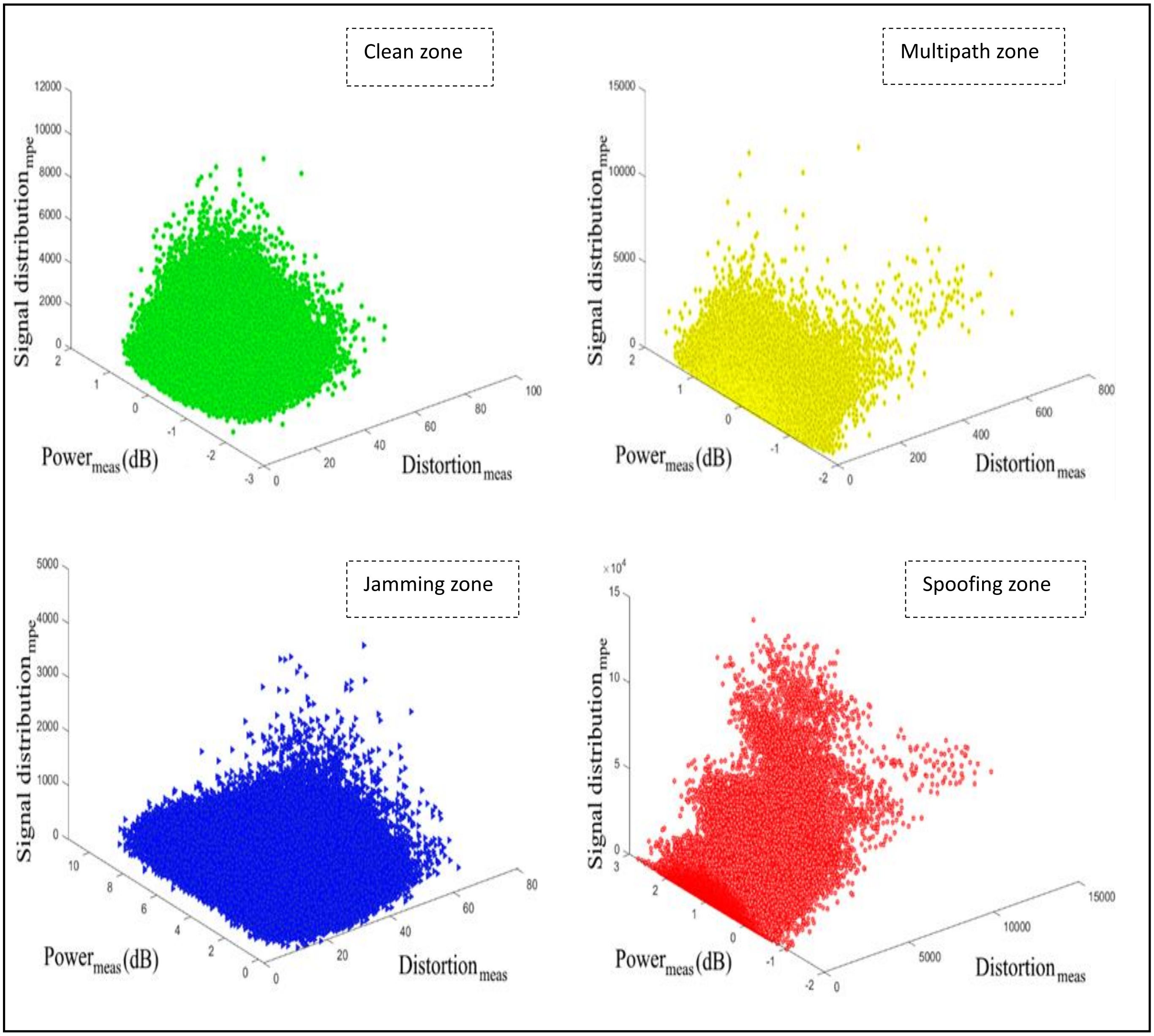


Fig. 9. GPS signal distribution in individual zones classified as clean, multipath, jamming and spoofing from left right, top down.

For interference free or clean signal zone alone, simulation is conducted by adjusting the Interference Power Advantage (IPA) from as low as 10dB to as high as 20dB while other parameters are set as mentioned earlier. The results presented in *Fig. 10* shows the isolation of interfered and clean signal is successful at all tested power advantages.

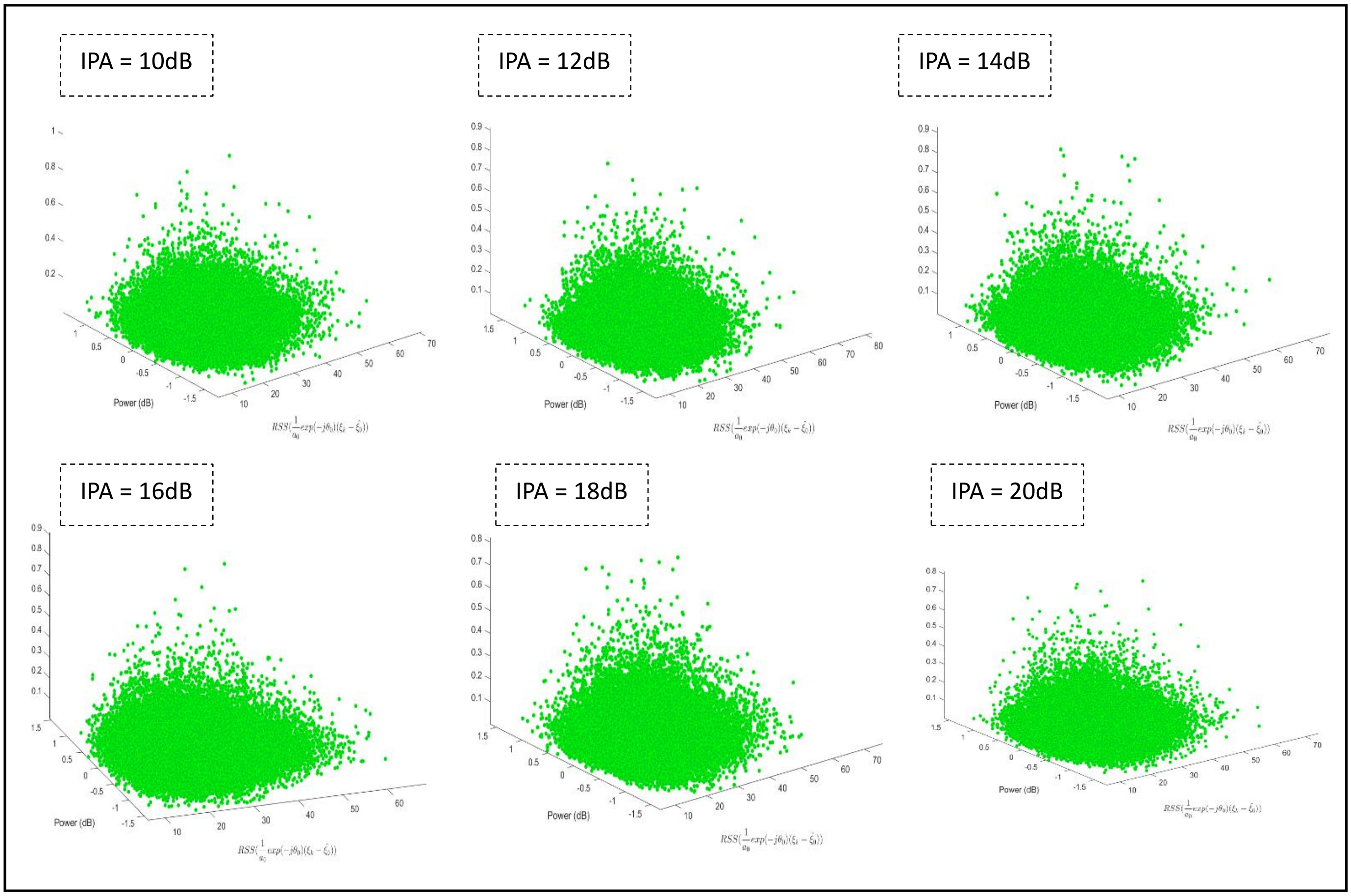


Fig. 10. Interference free GPS signal distribution with Interference Power Advantages from 10dB to 20dB, from left right, top down. ***X = Power, Y =Distortion and Z = MPE Distribution***

Regardless of the power advantages from the attacker being changed, the detector is successful at isolating the clean signal in every scenario. This simulation is repeated for different parameters, including even lower power advantages from 1dB to 9dB and the detection and isolation of the clean zone from the rest is obtained at high rate.

For multipath signal zone alone, again, the simulation is conducted by adjusting the Interference Power Advantage (IPA) from as low as 10dB to as high as 20dB while other parameters are set as mentioned earlier. The results presented in *Fig. 11* shows the isolation of the multipath signal from the rest is successful at all tested power advantages.

For jammed signal zone alone, also the simulation is conducted by adjusting the Interference Power Advantage (IPA) from as low as 10dB to as high as 20dB while other parameters are set as mentioned earlier. The results presented in *Fig. 12* shows the isolation of the jammed signal from the rest is successful at all tested power advantages.

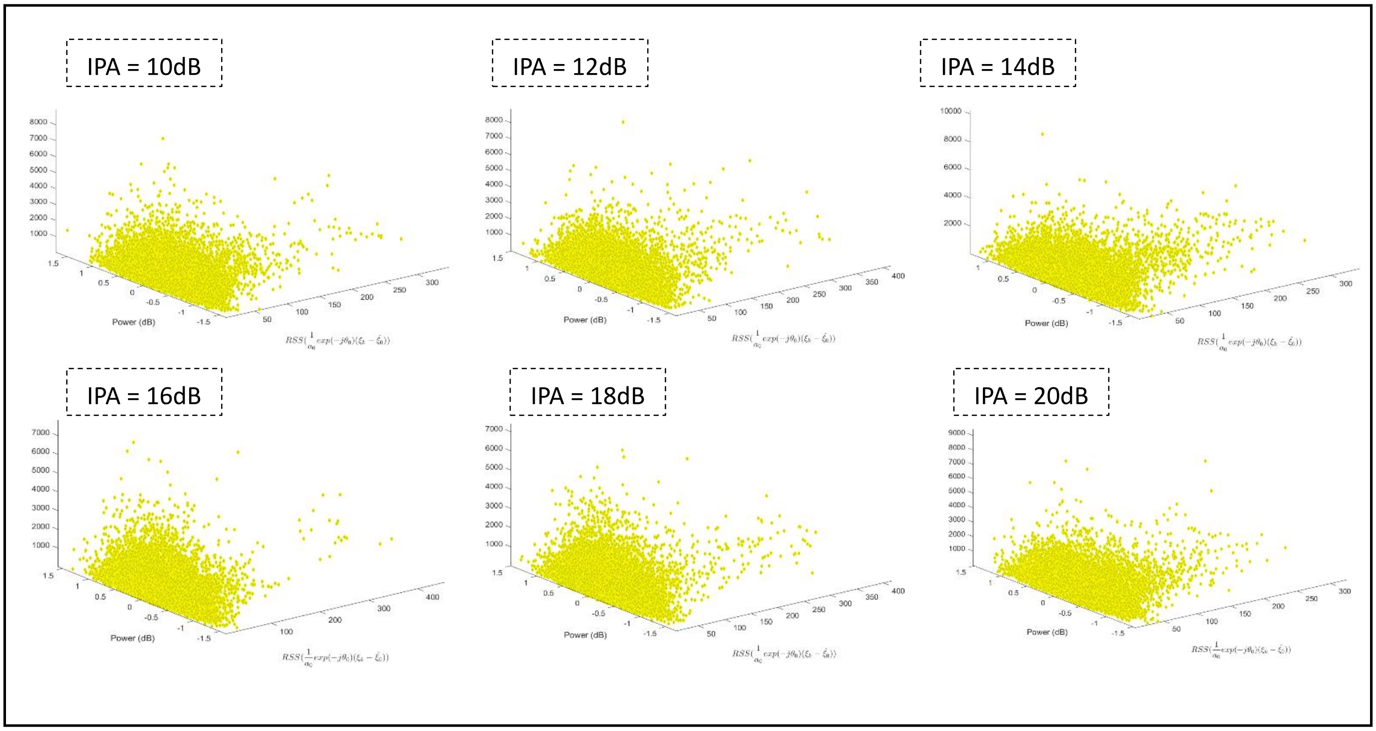


Fig. 11. Multipath GPS signal distribution with Interference Power Advantages from 10dB to 20dB, from left right, top down. ***X = Power, Y =Distortion and Z = MPE Distribution***

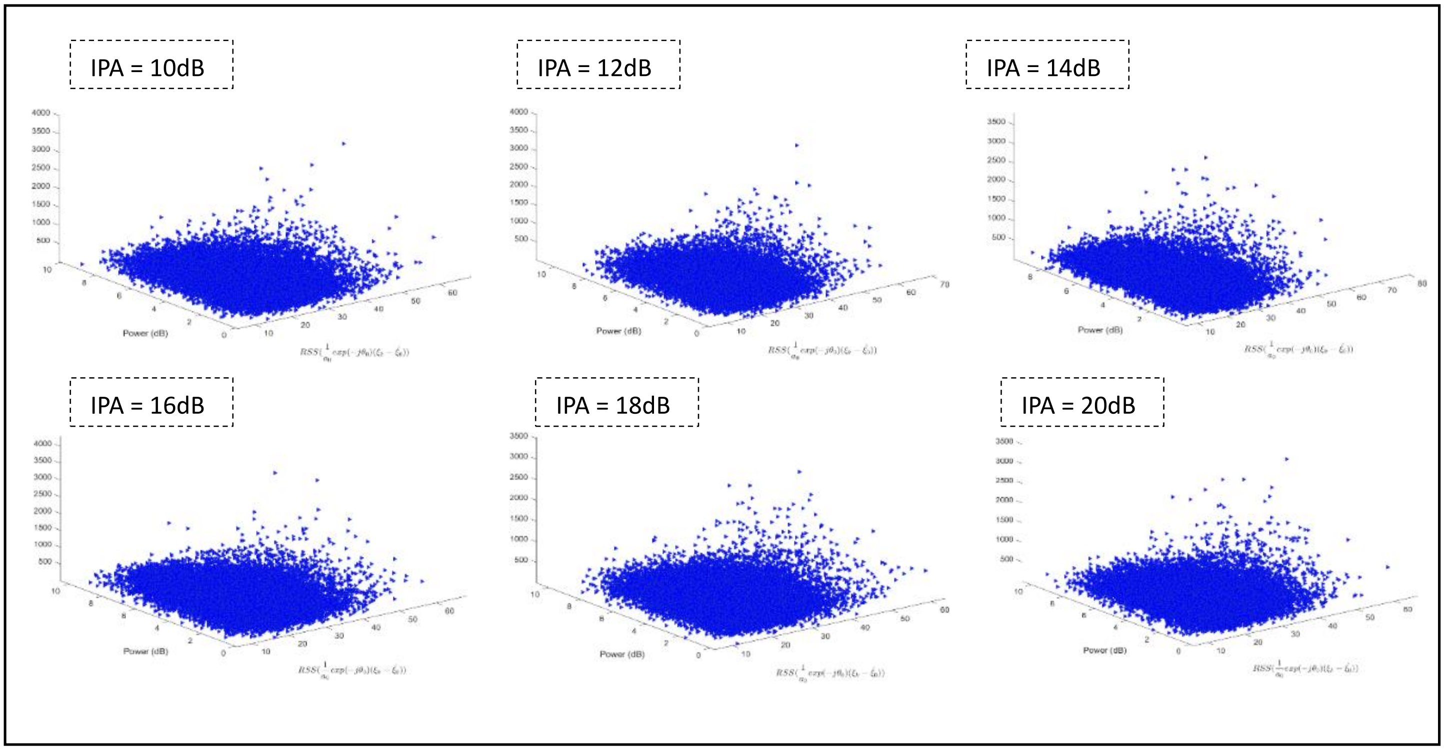


Fig. 12. Spoofed GPS signal distribution with Interference Power Advantages from 10dB to 20dB, from left right, top down. ***X = Power, Y =Distortion and Z = MPE Distribution***

Finally, for spoofed signal zone alone, the simulation is also conducted by adjusting the Interference Power Advantage (IPA) from as low as 10dB to as high as 20dB while other parameters are set as mentioned earlier. The results presented in *Fig. 13* shows the isolation of the spoofed signal from the rest is successful at all tested power advantages.

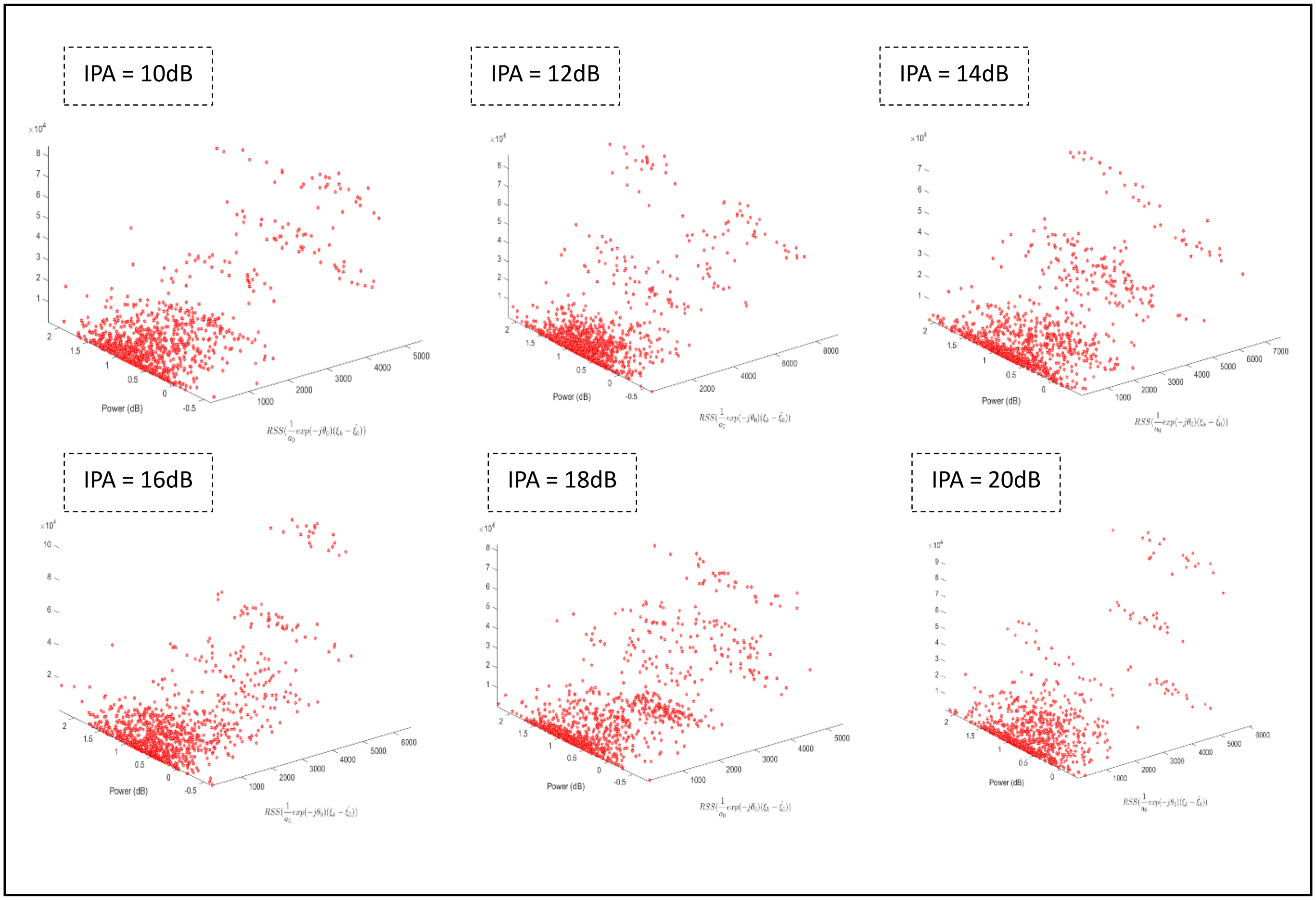


Fig. 13. Multipath GPS signal distribution with Interference Power Advantages from 10dB to 20dB, from left right, top down. ***X = Power, Y =Distortion and Z = MPE Distribution***

The detector in *Fig. 1.* is used to analyze the signal data collected in between $+\Psi_{IS}$ and $-\Psi_{IS}$. The patterns for the zone isolations are presented in the 3-dimetion model in *Fig. 14.* The four-color patterns represent signal detection regions in relation to power-distortion dynamic. The areas without color overlap represent correct detection while areas where color overlap occurred represent false detection. The areas with color overlap and with no overlap were calculated and showed an approximately 94% of correct detection was achieved using (8),

$$\frac{Area\ of\ zones\ without\ colors\ overlap}{Areas\ With\ color\ overlap + \ Without\ colors\ overlap} \times\ 100\%\ \approx 94.17\% \qquad (8)$$

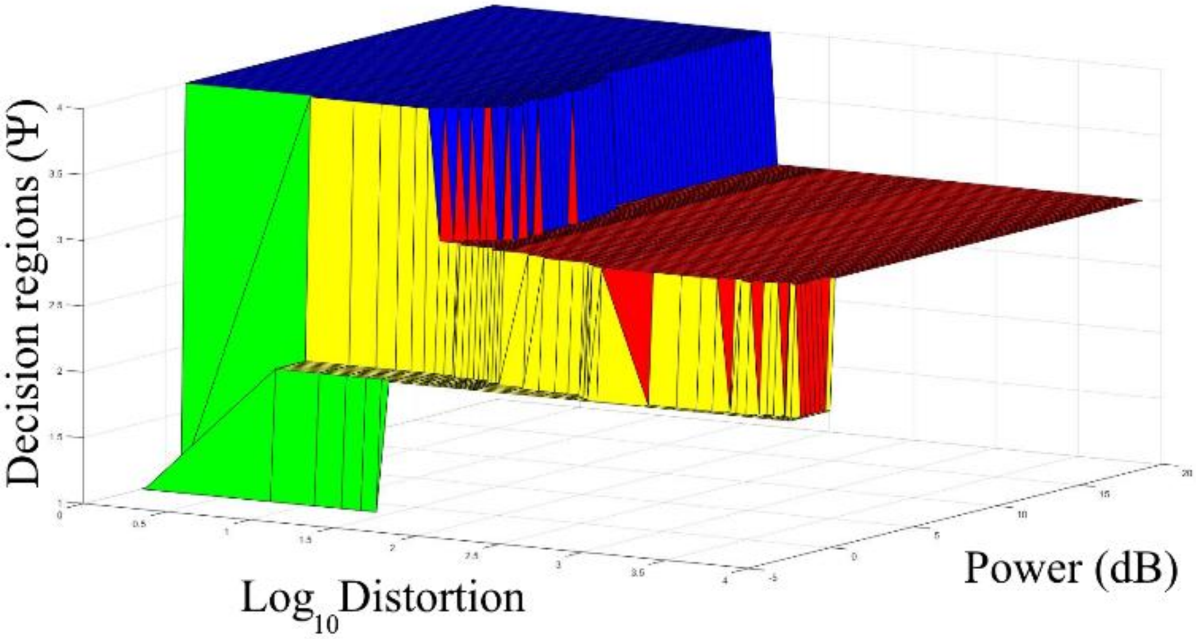


Fig. 14. Detector's output zones for GNSS signal authentication.

4. Conclusion

This study presents an improved technique for GNSS signal detection and validation through the power-distortion dynamic. Though the relevant detection and analysis software tool developed, we showed how the isolation of signal into different zones reduces the chances for interference of the clean signal with the multipath, jammed and spoofed signals. The simulation results support this detection technique with great detection results of the GNSS signal data tested. The isolation of signal into separate zones also made significant simplification and clarity to the analysis procedure of the GNSS signal. The simulation and data used are based on civil GPS L1 C/A signal which is still used in many areas of aircraft navigation, however, in order to increase accuracy through ionospheric correction and resilience by signal redundancy, future aircraft will employ L5 in conjunction with L1 C/A. The future direction for this research is on GPS L5 which is currently pre-operational in civil aircraft navigation.

Acknowledgement

Research for this paper is supported in part by the aviation science foundation of China (201908052002).

References

D. Fabio. (2015). *GNSS interference threats and countermeasures*. Boston ed: Artech House.

Eurocae. (2023). Minimum operational performance standard for galileo/global positioning system/satellite-based augmentation system airborne equipment . *The European Organization for Civil Aviation Equipment, ED259*.

Gao, G. X., Sgammini, M., Lu, M., & Kubo, N. (2016). Protecting GNSS Receivers From Jamming and Interference. *Proceedings of the IEEE*, *104*(6), 1327–1338. doi: 10.1109/JPROC.2016.2525938

Gross, J. N., & Humphreys, T. E. (2017). GNSS Spoofing, Jamming, and Multipath Interference Classification using a Maximum-Likelihood Multi-Tap Multipath Estimator. *Proceedings of the 2017 International Technical Meeting of The Institute of Navigation, ITM 2017*, 662–670. doi: 10.33012/2017.14919

Gross, J. N., Kilic, C., & Humphreys, T. E. (2019). Maximum-Likelihood Power-Distortion Monitoring for GNSS-Signal Authentication. *IEEE Transactions on Aerospace and Electronic Systems*, *55*(1), 469–475. doi: 10.1109/TAES.2018.2848318

Humphreys, T., Bhatti, J., Shepard, D., & Wesson, K. (2012). *The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques* (pp. 3569–3583). Retrieved from http://www.ion.org/publications/abstract.cfm?jp=p&articleID=10532

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation*, *2012*, 127072. doi: 10.1155/2012/127072

K. Wesson, J. N. Gross, B. L. Evans, & T. E. Humphreys. (2016). GNSS signal authentication via joint detection of correlation function distortion and anomalous received power. *IEEE Transactions on Aerospace and Electronic Systems*.

Karaim, M., Elghamrawy, H., Tamazin, M., & Noureldin, A. (2017). Investigation of the effects of White Gaussian Noise jamming on commercial GNSS receivers. *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, 468–472. doi: 10.1109/ICCES.2017.8275353

Meng, L., Yang, L., Yang, W., & Zhang, L. (2022). A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sensing*, *14*(19). doi: 10.3390/rs14194826

Novella, G., -Pena, A. J. G., Macabiau, C., Martineau, A., Ladoux, P., Estival, P., & Troubet-Lacoste, O. (2022). GNSS Acquisition Thresholds for Civil Aviation GNSS Receivers. *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*. Retrieved from https://enac.hal.science/hal-04088236

Ouyang, X., Zeng, F., Hou, P., & Guo, R. (2015). Analysis and Evaluation of Spoofing Effect on GNSS Receiver. *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-*

ScalCom), 1388–1392. doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.250

RTCA. (2018). Minimum operational performance standards (MOPS) for GNSS airborne active antenna equipment for the L1/E1 and L5/E5a frequency bands [MOPS]. *Radio Technical Commission for Aeronautics, DO 373*.

Wesson, K. D., Gross, J. N., Humphreys, T. E., & Evans, B. L. (2018). GNSS Signal Authentication Via Power and Distortion Monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, *54*(2), 739–754. doi: 10.1109/TAES.2017.2765258

Wu, Z., Zhang, Y., Yang, Y., Liang, C., & Liu, R. (2020). Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. *IEEE Access*, *8*, 165444–165496. doi: 10.1109/ACCESS.2020.3022294

Zidan, J., Adegoke, E. I., Kampert, E., Birrell, S. A., Ford, C. R., & Higgins, M. D. (2021). GNSS Vulnerabilities and Existing Solutions: A Review of the Literature. In IEEE Access (Vol. 9, pp. 153960–153976). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ACCESS.2020.2973759