Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 8
August 2024

Spoofing Threats and Design of Anti Spoofing ALGOR ITHM for Signal Analysis

Krishna Samalla [1] & Dr P Naveen Kumar [2]
[1]Faculty, Sreenidhi Institute of Science and Technology
[2]Professor, Osmanaia University, Hyderabad, India

Abstract: Daily life is significantly impacted by GPS-dependent location, navigation, and temporal synchronization processes. Therefore, for a variety of criminal purposes, terrorists and hackers find it more and more appealing to exploit such a widely used technology. As a result, in the field of GPS research, spoofing and anti spoofing algorithms have gained significant attention. In the area of GPS spoofing and anti-spoofing, new research will be reviewed in this paper. After examining GPS's harmful signals to spoofing attacks, various methods for creating spoofs will be covered. Following the introduction of the model of the spoofing signal, a succinct analysis of newly suggested methods of counter-spoofing and its effectiveness in mitigating and detecting spoofing will be given. We'll talk about the limitations of anti-spoofing algorithms and present various solutions. Furthermore, because of the strict emission restrictions, evaluating the spoofing/anti-spoofing systems is a difficult problem with certain limits. Here we proposed and modeled Anti spoofing algorithm.

Keywords: Navigation System*, Spoofing Detection Algorithm, Authenticity, Network Spoofing, Imitation of Spoofing Signals*

1. Introduction

These days, GPS enabled devices will found in many of its positioning, navigation and its applications. Safe and secure GPS applications are becoming more and more important for things like tracking criminal offenders, police and rescue services, mobile phone locations, telecommunication networks, and air, maritime, and land transportation. These days, the majority of cars and cell phones have GPS-based positioning and navigation systems installed. Furthermore, GPS is the primary component of numerous time tagging and synchronization systems used in the telecom and electrical power grid industries. As a result, terrorists and hackers are finding it more and more appealing to disrupt a widely utilized system illegally, Because GPS transmissions are very weak broadcast signals through the channels of wireless, they are susceptible to bandwidth interferences. Thus, within a few kilometers, even low- power interference can jam or spoof GPS systems with ease. Furthermore, GPS has a public domain signal structure and is a backwards-compatible technology [1]. This increases the vulnerability of GPS technology In the future, spoofing and anti spoofing mechanisms emerging challenges in contemporary GPS applications will draw more and more academic attention [1]. The purpose of spoofing is to intentionally interfere with GNSS. be far more dangerous than jamming. Recent progress of software-defined radio (SDR) technology has made the implementation of sophisticated spoofers more practical, versatile, and affordable [3].

Research on mitigation and spoofing discrimination has been started recently [2–9]. First, a quick summary of the various spoofing generation methods is given in this document. In addition, three test scenarios that are helpful in evaluating the spoofing/ant spoofing algorithms in real- world circumstances will be examined

2. Spoofing Techniques and its Classifications

GPS Signal Simulator. In this category, real GPS signals are imitated by concatenating a GPS signal simulator with an RF front-end. This type of spoofer does not provide signals that are precisely timed to the actual GPS signals. Consequently, even when the spoofer power is larger than the real signals, the spoofing signals appear to be noise to areceiver that is in tracking mode. However, if the spoofing signal power is greater than the real signals, this kind of spoofer can successfully fool commercial GPS devices. The most basic type of GPS spoofer is a GPS signal simulator, which may be identified using various anti spoofing methods such as amplitude monitoring, consistency checks between measurements, and consistency checks using inertial measuring units (IMUs).

Receiver-Based Spoolers. A GPS receiver coupled with a spoofing transmitter makes up a more sophisticated kind of spoofer. This system generates a spoofing signal knowing the 3D pointing vector of its transmit antenna toward the target reception antenna after first synchronizing to the current GPS signals and extracting the position, time, and satellite ephemeris. This type of

spoofer is more complex than the previous category and is harder to distinguish from the real signals. The primary obstacle in implementingthis type of spoofer is delivering the spoofing signals to the designated victim receiver at the proper signal strength and delay. Keep in mind that in order to successfully trick the target receiver, the spoofing power needs to be only a little bit greater than the real signal power—not much higher than the power of regular GPS signals. Other restrictions that a receiver-based spoofer should address include matching the carrier frequency and phase to the real GPS signals, reducing the self-jamming effect, and increasing relative data bit latencies. Understanding the 3D pointing vector from the spoofer transmit antenna phase center to the target receiver antenna phase center at the centimeter level is necessary for carrier phase alignment to the legitimate signals. Therefore, having the spoofer antenna very close to the target receiver antenna would be quite advantageous for this type of spoofers.

Sophisticated Receiver-Based Spoofers: The most intricate and potent kind of parody category is this one. In order to precisely synchronize the spoofing signal coding and carrier phase to those of genuine signals at the receiver, it is expected that this kind is aware of the centimeter-level location of the target receiver antenna phase center [7]. This kind of spooler can overcome direction of arrival antispoofing strategies by utilizing several broadcast antennas. In this instance, in order to fool an angle of arrival (AOA) discriminating GPS receiver, the spoofer must create an array manifold that is compatible with the array manifold of the genuine signal.

Building a spoofer of this kind is far more complicated than building any of the two previously mentioned categories. This type of spoofer has a significantly narrower effectiveness region than the preceding spoofing categories. The rationale is that only a very tiny region containing the target reception antennas may be able to achieve array manifold synchronization and carrier phase alignment .Due to the geometry and movement of the target reception antenna(s), it is therefore exceedingly difficult, and in many cases impossible, to realize this form of spooler

3. GPSVulnerability the against Spoofing Attack

The signal processing, data bit, and position/navigation solution levels of GPS receivers are the three operational layers where the vulnerability of GPS to spoofing can be examined

3.1. GPS Vulnerability in Signal Processing Level.

The modulation type, pseudo-random noise (PRN) signals, transmit frequency, and signal bandwidth, Doppler range, and signal strength of GPS signals are all publicly known. Additionally, GPS is a backwards-compatible technology, meaning that the characteristics of the L1 signal remain mostly unchanged between GPS satellite generations. The automatic gain control (AGC) block used in the majority of commercial GPS receivers is designed to correct for fluctuations in the received GPS signal's power. However, because AGC automatically modifies the receiver. Input gain in response to stronger spoofing signals, it may make GPS devices more susceptible to these signals [8].

Consequently, a spoofing module can create fake signals that are arbitrary similar to the real GPS signals in order to successfully fool GPS receivers, provided it is aware of the general layout and functional principles of a civilian GPS receiver.

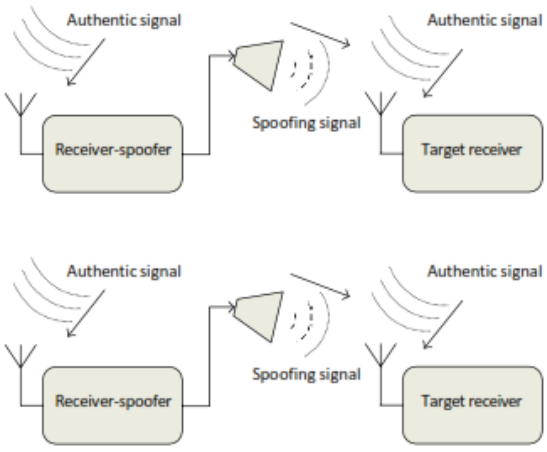


Fig1: Block Diagram of Repeater spoofer

4. Classification of Anti spoofing Techniques

Numerous anti spoofing methods have been put forth in the public domain and can be broadly categorized into two primary groups: spoofing detection and spoofing where Mitigation. While[m] spoofing mitigation techniques primarily focus on neutralizing the detected spoofing signals and assist the victim receiver in regaining its positioning and navigational capabilities, spoofing detection algorithms.

4.1 Spoofing Attack Scenarios:

Spoofing attacks on Global Navigation Satellite Systems (GNSS) unfold through various scenarios, each capitalizing on unique vulnerabilities to manipulate location-based data. One prevalent tactic involves signal replay attacks, where adversaries illicitly rebroadcast previously captured authentic GNSS signals. By replaying these signals, attackers mislead receivers into computing inaccurate positions based on outdated

information. In contrast, signal generation attacks entail the creation of entirely fabricated signals that mimic legitimate GNSS transmissions. Crafted by malicious entities, these counterfeit signals can lead receivers astray by furnishing false positioning data. Real-world instances of GNSS spoofing incidents underscore the tangible

Consequences of such attack scenarios. Examples include the disruption of drone navigation during critical operations, the manipulation of vessel tracking systems to deceive maritime navigation, and potential compromises to location-based applications in autonomous vehicles. Some instances of spoofing attacks have even been orchestrated for geopolitical motives, underscoring the far-reaching implications of this malicious activity on a global scale. A comprehensive understanding of the diverse tactics employed in these scenarios is imperative for the development of effective anti-spoofing strategies. These strategies play a crucial role in mitigating the ramifications of spoofing attacks and fortifying the resilience of GNSS systems against an ever-evolving landscape of threats.

The real and fake SNR values are shown in Figure 3. in contrast to the TSP for the scenarios of 10, 20, and 30 equal power spoofing signals and 10 equal power genuine signals. The Eachgenuine signal has a power of -158 dBW, and the coherent Tc =NTs = 1 ms is the integration time. Typical identification TheSNR threshold is shown in this picture. It’s noticed when theTSP increases, the SNR of the real signals drops conversely, when the SNR of the spoofing grows signals rise to a specific point when the TSP rises. The highest level of spoofing SNR isdetermined by the number of fake PRN signals that were sentand the distribution among them is TSP. The estimated receiver noise floorat the10 ms.

(a) Absolute Power Monitoring. It is challenging for a spoofer to determine the transmit power needed to impose sufficient signal strength at the target receiver without unduly surpassing the typical power level of the legitimate GPS signals since the route loss between the spoofer and target receiver is very variable [8]. At earth terminals, the maximum GPS signal received power is approximately 153 dBW.As a result, as Figure 4 illustrates, the vulnerability region of the C/N0 monitoring receiver is significantly larger than that of the absolute power monitoring receiver. Additionally, in the event of a spoofing attack, the receiver's vulnerability window can be significantly reduced if it can detect the absolute receiver power with greater accuracy [12].In order to use this power monitoring technique, the receiver must be able to measure the received signal's absolute amplitude with a certain degree of accuracy. As a result, hardware complexity goes up a little. Furthermore, the amplitude discrimination techniques are limited in their performance by the relatively high dynamic range of the GPS signal strength.

(b) Received Power Variations versus Receiver Movement A free space propagating signal's received power is proportional to the inverse of the squared propagationdistance, according to the free space square law of propagation. Because GPS satellites are located about 20,000 kilometers from Earth, if a receiver is moved on Earth in low multipath open sky conditions, it should not significantly alter the received power from genuine satellites, except from deterministic losses at lower altitudes. In contrast to the GPS satellites, the spoofing signal is typically transmitted from a single directional antenna that is situated much closer to the receiver, as was previously discussed. The receiver's movement in relation to the spoofer antenna can therefore significantly alter

*(c) L1/L2 Power Level Comparison. N*o difference is made by receiver movement or multipath effects [11]. The spoofer is assumed to not differentially modulate the C/N0 of the various PRN signals in this scenario. This is a low-complexity spoofing nation technique that doesn't require the GPS receiver to undergo significant hardware or software changes.

There is no assurance that the receiver movement will significantly alter the received C/N0 of the spoofer generated signals, though, as the receiver is not always aware of the spoofer antenna's position or variations in distance from the receiver antenna. For instance, when the GPS receiver and spoofing transmitter are housed in the same car, the movement of the car does not affect the spoofing signals' C/N0 measure. An additional drawback of this. *Spoofing Discrimination Using Spatial Processing.* Spatial Processing for Spoofing Discrimination.

Owing to practical constraints, spoofing transmitters typically transmit multiple fake signals from a single antenna, whereas the real signals originate from distinct satellites in different directions. In order to distinguish between signals that are spatially correlated and estimate the spatial signature of received signals, a spatial processingtechnique can be used.

(d)Multi antenna Spoofing Discrimination. In

Discrimination by Multi antenna Spoofing (a). A spoofing detection method is presented in [2] that monitor the phase difference between two fixed antennas for approximately an hour.

To distinguish between the spoofing threat and real phase difference observed by the antenna array, theoretical phase differences can be computed and compared to the satellite movement trajectory and array bearing.

The algorithm's primary flaw is that it takes a long time (roughly an hour) to distinguish between spoofing signals. Furthermore, for this technique to function correctly, the antenna array needs to be calibrated and have a known array orientation.

According to [14], spoofing signals are identified and reduced using an antenna array structure based on their spatial correlation. In order to distinguish signals received from the same spatial sector, the correlator output phase measurements for various PRN signals are mutually compared.

This method works well for spoofing signal detection and doesn't require array calibration or orientation information. When using a single transmit antenna, this technique can effectively discriminate between different spoofing scenarios. Furthermore, since every spoofing signal experiences the same propagation channel characteristics, multipath propagation does not impair the effect.

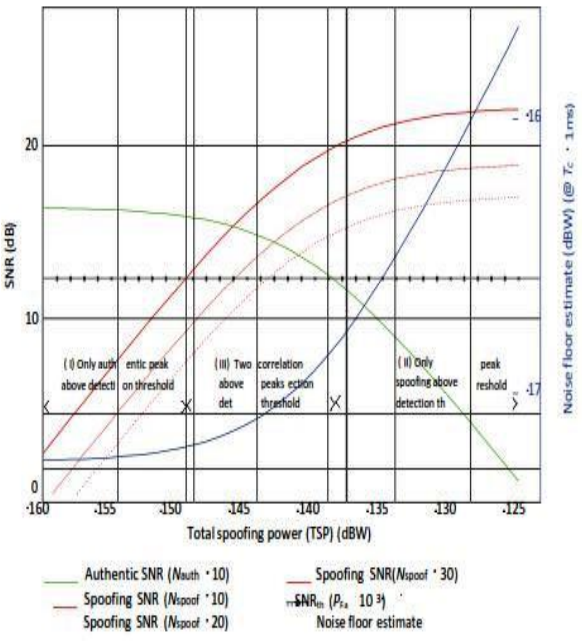


Fig 2: Received SNR versus TSP for authentic and spoofing correlation peaks

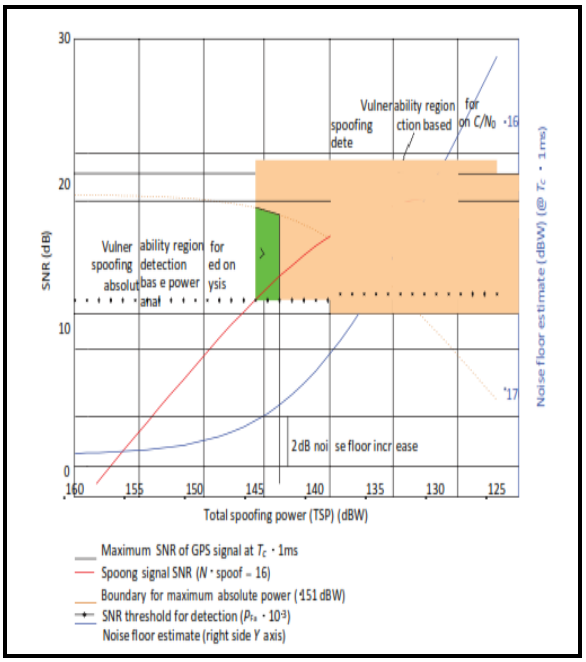
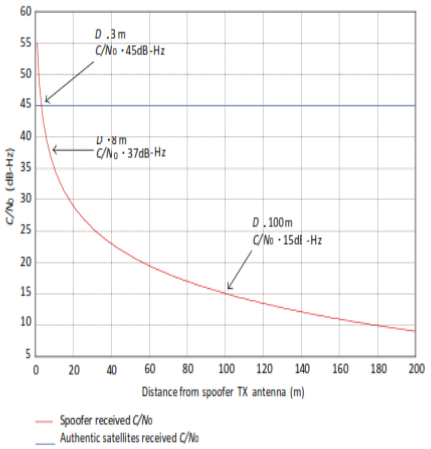


Fig 3: Vulnerability region comparison of C/N0 Versus absolute power monitoring techniques



4. Variations of Spoofing and authentic received C/N0 versus receiver distance from spoofer transmitting antenna

However, because it requires the use of multiple antenna branches, this technique increases the hardware complexity of the GPS receiver. Additionally, using this method makes the GPS receiver more computationally complex because it musttrack and acquire both real and spoofing signals in order to distinguish between spoofing PRNs. Depending on the number of transmit antennas, the number of receiver antennas, and the geometry of the spoofer antennas in relation to the target receiver antennas, a multiple-antenna spoofer may be able to overcome the multiple-antenna spoofing discrimination techniques. Nevertheless, putting such a complex spoofing scenario into practice is severely constrained.

(b)Synthetic Array Spoofing Discrimination. A

synthetic antenna array-based spoof-ing detection method has been proposed in [6]. In this instance, a handheld GPS receiver with a single antenna is moved in an arbitrary manner to create a synthetic antenna array structure. In Figure 6, this scenario is depicted. Using the correlation coefficient metric (ρij), the received signals' phase and amplitude corresponding to various PRN signals are continuously compared to one another. Consequently, the following normalized correlation coefficient is used to distinguish between spoofing signals and authentic signals once different PRN signals have been acquired for the received signal set:

Signal Quality Monitoring (SQM). In multipath fading conditions, the GPS correlation peak quality has been observed using SQM approaches in the past [17]. Similar to how multipath components alter the correlation result, spoofing attempts on a tracking receiver can do the same [18]. In order to detect receiver can do the same [18]. In order to detect spoofing attacks on tracking receivers operating in line receiver can do the same [18]. In order to detect of-sight conditions, the authors of [4, 5, 7] have expanded the SQM approaches. To find any unusual asymmetry or flatness of GPS correlation peaks induced by the spoofing attack, they used the ratio and delta SQM tests. Presumably, the receiver has the goal of a spoofing assault is to trick the receiver into following its fictitious correlation peaks.

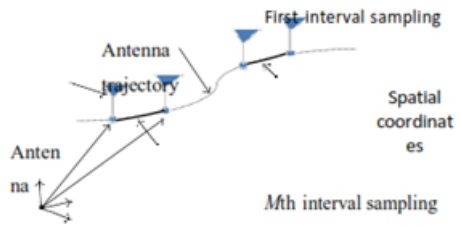


Fig5: Spatial Sampling for moving Receivers

SQM anti spoofing techniques are effective means of identifying spoofing attacks, particularly in contexts where propagation occurs line-of-sight. Nevertheless, the SQM approach might not be able to distinguish between multipaths

Reflections and spoofing signals in the context of multipath However, the genuine signals do not exhibit this correlation (that is, PRN-22 and PRN-24 amplitudes do not overlap). The reason this method is effective, in multipath environments is that all of the spoofing signals follow the same fading path. Furthermore, compared to the methods suggested in [2, 14], this method's hardware complexity is significantly lower because it doesn't use multiple receive antennas. To successfully discriminate the counterfeit signals, this method should be modified in the event that spoofer differentially modulates the amplitude and phase of distinct PRN signals. In this instance, the spoofing transmission can occur indoors, where it is not prohibited by laws governing radio transmission. Despite not accurately representing actual outdoor spoofing scenarios, this setup appears appropriate, particularly when considering multi-antenna anti spoofing techniques. In this instance, the single antenna also retransmits all genuine signals other considerations for indoor retransmission include multipath propagation, relative spoofing, and authentic signal powers.

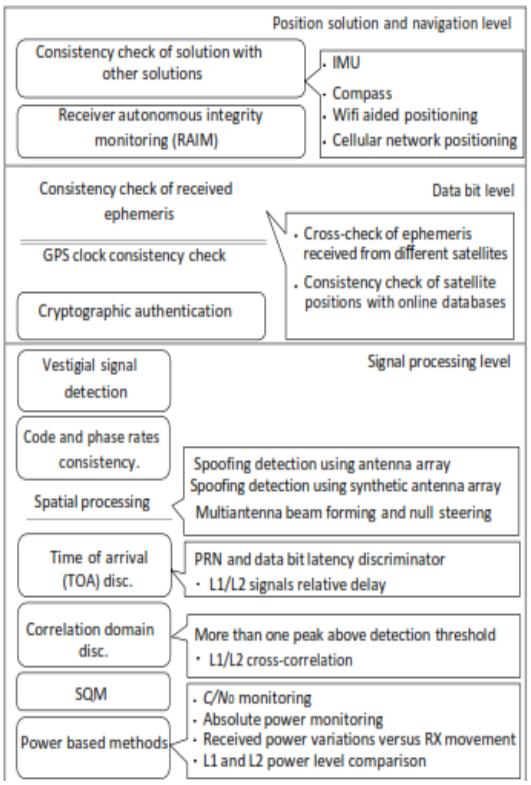


Fig6: A Multilayer approach to anti spoofing techniques

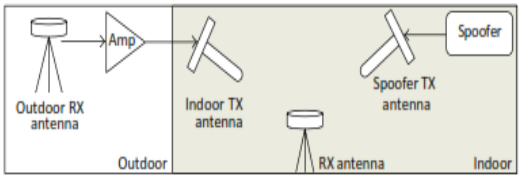


Fig 7: Spoofing test using GPS indoor signal retransmission

Spoofing Using Recorded Data with No RF Transmission. The intermediate frequency (IF) authentic GPS L1 signal is digitalized and stored on a hard drive in this scenario, instead of a real spoofer RF transmission. The recorded

data is then fed to the GPS receiver-spoofer, which tracks current GPS signals and generates corresponding spoofing signals. An output bit stream that is quantized is created by combining these signals. The target receiver receives the result of this process after the output bit stream has been interleaved with the original data [3]. A block diagram of this test scenario is shown in fig 7. *Employing RF Combiners to Combine Authentic and Spoofing Signals.* RF power combiners can be used to combine locally produced spoofing signals with real GPS signals. The power of the spoofing signal can be changed with Amplifier and variable attenuator in a cascaded configuration. The block diagram for this test setup, which verifies that a multi antenna anti spoofing technique is operating correctly, is displayed in Figure8
Strengthen GPS receiver security against jamming and spoofing attempts. This paper outlined various spoofing and anti spoofing scenarios as well as GPS vulnerabilities that may be exploited.

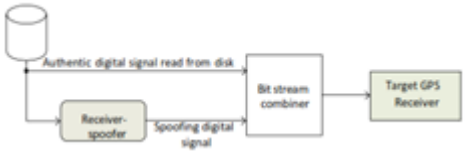


Fig 8: Spoofing test using recorded GPS data

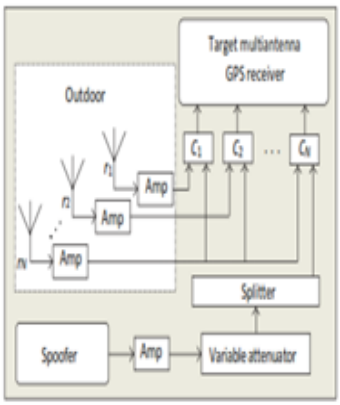


Fig 9: Spoofing test set pusing RF combiners for a multi antenna receiver

Hear we were examined in a multilayer GPS processing approach by a spoofer. It was demonstrated that spoofing attacks produced by various spoofing scenarios can easily compromise commercial GPS receivers. However, low-complexity spoofing detection and mitigation techniques can be used with minor modifications to make commercial GPS receivers more resilient to spoofing attacks. It is possible to implement countermeasures against spoofing signals at any or all of a GPS receiver's processing levels. Ideally, a potent anti spoofing method should have a low computational complexity and work well in general spoofing situations. According to this paper, since the majority of real-world spoofing scenarios use a single antenna to send fake signals, Consequently general and highly successful countermeasure against the majority of spoofing signals currently anticipated is the use of spatial processing-based anti spoofing techniques.

5. Conclusions

Major threat to applications related to safety of life; however, since there is sufficient incentive for the un authorized use of spoofers, their realization is not unreasonably expensive. As a result, it is expected that a lot of research will be done to strengthen GPS receiver security against jamming and spoofing attempts. This paper outlined various spoofing and anti spoofing scenarios as well as GPS vulnerabilities that may be exploited.

References

[1] X. J. Cheng, K. J. Cao, J. N. Xu, and B. Li, "Analysis on forgery patterns for GPS civil spoofing signals," in *Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09)*, pp. 353–356, Seoul, Korea, November 20092nd ed., vol. 3, J . Peters, E d . New Y o r k , NY, USA: McGraw-Hill,1964,pp.15–64.

[2] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledv- ina, "Receiver-autonomous spoofing detection: experimen-tal results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the Institute of Navigation—International Technical Meeting (ITM '09)*, pp. 124–130, Anaheim, Calif, USA, January 2009.

[3] H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS '05)*, pp. 1285–1290, Long Beach, Calif, USA, September 2005.

[4] S. Savasta, L. Lo Presti, F. Dovis, and D. Margaria, "Trustwor- thiness GNSS signal validation by a time-frequency approach," in *Proceedings of the 22nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '09)*, pp. 66–75, Savannah, Ga, USA, September 2009.

[5] C. E. McDowell, "GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling—US Patent 7250903 B1," 2007.

[6] S. C. Lo and P. K. Enge, "Authenticating aviation augmen- tation system broadcasts," in *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS '10)*, pp. 708–717, Indian Wells, Calif, USA, May 2010.

[7] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal Authentication, a secure civil GNSS for today," *GNSS magazine*, pp. 30–39, 2009.

[8] R. E. Phelts, Multicorrelator techniques for robust mitigation of threats to GPS signal quality [Ph.D. thesis], Standford University, Palo Alto, Calif, USA, 2001

[9] P. Kopyt*et al., "*Electric properties of graphene-based conductive layers from DC up to terahertz range," *IEEE THz Sci. Technol.,* to be published. DOI: 10.1109/TTHZ.2016.2544142.

[10] PROCESS Corporation, Boston, MA, USA. Intranets: Internet technologies deployedbehindthefirewall forcorporateproductivity. Presented at INET96AnnualMeeting.[Online]. Available: http://home.process.com/Intranets/wp2.htp

[11] R. J. Hijmans and J. van Etten, "Raster: Geographic analysis and modeling with raster data," R Package Version 2.0-12, Jan. 12, 2012. [Online]. Available: http://CRAN.R-project.org/package=raster

[12] Teralyzer. Lytera UG, Kirchhain, Germany [Online]. Available: http://www.lytera.de/Terahertz_THz_Spectroscopy.php?id=home, Accessed on: Jun. 5, 2014

[13] U.S. House. 102nd Congress, 1st Session. (1991, Jan. 11). *H. Con. Res. 1, Sense of the Congress on Approval of Military Action*. [Online]. Available: LEXIS Library: GENFED File: BILLS

[14] Musical toothbrush with mirror, by L.M.R. Brooks. (1992, May 19). Patent D 326 189 [Online]. Available: NEXIS Library: LEXPATFile: DES

[15] D. B. Payne and J. R. Stern, "Wavelength-switched pas- sivelycoupledsingle-mode opticalnetwork,"in *Proc. IOOC-ECOC,* Boston, MA, USA,1985, pp.585–590.

[16] D.EbehardandE.Voges,"Digitalsinglesidebanddetectionforinterferometricsensors,"presentedat the*2ndInt. Conf.OpticalFiberSensors,*Stuttgart,Germany,Jan.2-5, 1984.

[17] G. Brandli and M. Dick, "Alternatingcurrent fed power supply,"U.S.Patent 4 084 217,Nov.4,1978.

[18] J. O. Williams, "Narrow-band analyzer," Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, USA, 1993.

[19] N. Kawasaki, "Parametric study of thermal and chemical nonequilibrium nozzle flow," M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.

[20] Luo, Z.; Deng, Z. Positioning Method without GNSS for Unmanned Systems Based on Fusion of IMU, TOA and AOA; Springer:Singapore, 2022.

[21] Hu, Y.; Bian, S.; Cao, K.; Feng, G. Spoofing power control strategy for GNSS receive. J. Chin. Inertial Technol. 2015, 23, 5.

[22] Vervischpicois, A.; Samama, N.; Taillandierloize, T. Influence of GNSS Spoofing on Drone in Automatic Flight Mode. In Proceedingsof the ITSNT 2017: 4th International Symposium of Navigation and Timing, Toulouse, France, 14–17 November 2017;pp. 1–9.Qi, Z.; Li, H.; Qian, L. GPS spoofing attack on time synchronization in wireless networks and detection scheme design.In Proceedings of the MILCOM 2012—2012 IEEE Military Communications Conference, Orlando, FL, USA, 1 November 2012.

[23] Pardhasaradhi, B.; Cenkeramaddi, L.R. GPS Spoofing Detection and Mitigation for Drones using Distributed Radar Tracking andFusion. IEEE Sens. J. 2022, 22, 11122–11134. [CrossRef]

[24] F. N. O, A. D. A, T. D. A and K. M. A, "Detecting GPS Spoofing on Different Devices Using RaspberryPi with LimeSDR", *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 14-16, 2020.

[25] What are Global Navigation Satellite Systems?, November 2022, [online] Available: https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss

[26] M. L. Psiaki, T. E. Humphreys and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. here's how to fight back GPS lies", *IEEE Spectrum*, vol. 53, no. 8, pp. 26-53, 2016

[27] J. Li, X. Zhu, M. Ouyang, W. Li, Z. Chen and Q. Fu, "GNSS Spoofing Jamming Detection Based on Generative Adversarial Network", *IEEE Sensors Journal*, vol. 21, no. 20, pp. 22823-22832, Oct.15 2021

[28] K. K. Songala, S. R. Ammana, H. C. Ramachandruni and D. S. Achanta, "Simplistic Spoofing of GPS Enabled Smartphone", *2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)*, pp. 460-463, 2020.

[29] A. Rustamov, A. Minetto and F. Dovis, "Improving GNSS Spoofing Awareness in Smartphones via Statistical Processing of Raw Measurements", *in*

IEEE Open Journal of the Communications Society, vol. 4, pp. 873-891, 2023

[30] T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing", *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073-1090, APRIL 2013.

[31] L. Huang and Q. Yang, "Low-cost GPS simulator GPS spoofing by SDR", *Proceedings of DEFCON*, 2015.

[32] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer", *2008 ION GNSS Conference*, 2008

[33] B. Pardhasaradhi, Y. R. Reddy and L. R. Cenkeramaddi, "Machine Learning based Screening and Measurement to Measurement Association for Navigation in GNSS Spoofing Environment", *in IEEE Sensors Journal*, 2022

[34] D. Dardari, E. Falletti, M. Luise, *Satellite and Terrestrial Radio Positioning Techniques: A Signal Processing Perspective* (Academic Press, Boston, 2011)

[35] M.G. Amin, P. Closas, A. Broumandan, J.L. Volakis, Vulnerabilities, threats, and authentication in satellite-based navigation systems [scanning the issue]. Proc. IEEE **104**(6), 1169–1173 (2016)

[36] H. Sathaye, G. LaMountain, P. Closas, A. Ranganathan, SemperFi: anti-spoofing GPS receiver for UAVs, in Network and Distributed Systems Security (NDSS) Symposium 2022 (2022)