Global Navigation Satellite System in the Civil Surveillance

Krishna Samalla[1] & P. Naveen Kumar[2]
[1]Professor, Department of ECE
Sreenidhi Institute of Science and Technology, Telangana, India
[2]Professor, Department of ECE
Osmanaia Univesrsity, Telangana, India

DOI: *https://doi.org/10.34293/acsjse.v4i1.100*

Received Date: 02.01.2024 **Accepted Date:** 20.02.2024 **Published Date:** 01.04.2024

Abstract - *In the contemporary landscape dominated by widespread Global Navigation Satellite Systems (GNSS) usage for various navigational applications across aerial and terrestrial domains, route determination efficiency is increasingly reliant on the accuracy of inputs derived from GNSS, primarily facilitated by GPS and associated modules. However, the rising occurrence of spoofing mechanisms has introduced distortions in this realm, necessitating thorough examination. The discernible impact of GNSS signals on seamless navigation underscores their pivotal role in precise path determination. Yet, sophisticated spoofing methodologies disrupt this, compromising the integrity of GNSS-derived information. Addressing these challenges requires closer scrutiny of vulnerabilities and the formulation of robust countermeasures to fortify the GNSS infrastructure. This research embarks on exploring adaptive filtering techniques tailored for detecting and eliminating spurious signals introduced by sophisticated spoofing mechanisms. The primary goal is to establish an uninterruptible and dependable GNSS system. The scientific foundation involves a rigorous examination of signal processing methodologies, with a focus on adaptive filtering algorithms adept at discerning original signals from falsifiedones. By delving into these intricacies of adaptive filtering, this research aims to enhance GNSS resilience against spoofing threats, considering the nuanced characteristics of spoofed signals, and developing strategies capable of distinguishing them from authentic GNSS signals. The scientific rigor extends to the formulation of algorithms attuned to dynamic signal variations, ensuring adaptability to evolving spoofing techniques. This scientific inquiry contributes substantively to GNSS security by advancing the theoretical foundations of adaptive filtering mechanisms. Through systematic experimentation and empirical validation, the research aims not only to detect but also to eliminate spoofed signals, fostering an environment where GNSS users can rely on an uninterrupted and resilient navigation system. The results obtained from this study carry the promise of guiding the advancement of advanced counter-spoofing technologies, safeguarding the enduring integrity and reliability of GNSS against continuously evolving adversarial tactics.*

I Introduction

GNSS (Global Navigation Satellite Systems) has become criticalin the currently well-established civil surveillance [1], playing a pivotal role in applications such as transportation, navigation, and communication. GNSS technologies, spearheaded by systems like GPS [2] (Global Positioning System), GLONASS has a short life design [3], and Galileo, provide accurate and real-time positioning information [4]. 24 of these satellites have been orbiting after the launch since 2001, and the plans prevalent aim to see a total of 24 operational satellites by 2010 [5]. However, the increasing reliance on GNSS in civil surveillance has also exposed vulnerabilities, with spoofing emerging as a notable threat. Spoofing involves the deliberate transmission [6] of false signals to deceive GNSS receivers, leading to errors in position determination and compromising the reliability of surveillance systems. This paper delves into the nuanced interplay between GNSS and civil surveillance, focusing on the challenges posed by spoofing and exploring potential mitigation strategies. (GNSS) in civil surveillance [7,8] has revolutionized applications such as navigation, transportation, and communication. Striving to identify strategies for safeguarding Protecting GNSS users and other civilian customers from potential spoofing hazards. [9-10]. GNSS enables accurate positioning through satellite signals, but the escalating threat of spoofing poses significant challenges to the reliability and security of GNSS-based civil surveillance systems [4].

II GPS

G.P.S. (Short for Global Positioning System), originally developed by the USA, for a satellite-oriented navigation [2, 12] system which has transformed the way we determine and track locations on Earth. Operating through a constellation of satellites orbiting our planet, GPS [12] enables users to pinpoint their precise position through the triangulation of signals transmitted by these satellites. Originally developed for military applications, GPS has become an integral part of civilian life, finding widespread use in navigation systems for vehicles and smartphones, aviation, maritime activities, surveying, and various location-based services. The primary components of GPS include the Space Segment (satellites), Control Segment (ground-based control stations), and User Segment (GPS receivers) [13] work collaboratively to provide accurate and real-time positioning information. Augmentation systems like WAAS and EGNOS enhance GPS accuracy, mitigating factors such as signal obstructions and atmospheric conditions. With applications ranging from logistics and precision agriculture to search and rescue operations, GPS continues to play a crucial role in diverse industries. Ongoing developments, including multi-frequency signals and integration with other satellite navigation systems, promise further improvements in accuracy and functionality.

GPS currently provides two distinct services: the Standard Positioning Service (SPS) for civilian users and the Precise Positioning Service (PPS) exclusively available to authorized users, primarily the U.S. military and its allies [14]. The United States has committed to offering the GPS SPS for civil aviation globally, ensuring continuous availability without imposing direct user fees. This commitment, initially established by the Federal Aviation Administration (FAA) administrator in 1994 [15], was reaffirmed in 2007. Additionally, during this time, a pledge was made to provide GPS satellite-based augmentation system (SBAS) services in North America through the FAA's Wide Area Augmentation System (WAAS), again without imposing direct user charges. The commitment includes a provision for at least six years' advance notice in case of a decision to terminate the GPS SPS service [14]. This underscores the long-standing dedication to making GPS services accessible and reliable for civil aviation users while promoting the use of satellite-based augmentation systems to enhance navigation accuracy in North America.

At one-point, intentional degradation of the accuracy of the Standard Positioning Service (SPS) occurred through a method referred to as Selective Availability (SA).

This degradation involved applying pseudorandom dithering to the satellite clock, and only Precise Positioning Service (PPS) receivers possessing knowledge of the generation algorithm and cryptographic keys could counteract its impact. However, on May 1, 2000, the purposeful degradation of SPS performance due to SA was terminated [16]. In a more recent development, in September 2007, the United States declared its decision to eliminate the capability to implement selective availability from future GPS satellite procurements [17].

III GNSS OVERVIEW

Global Navigation Satellite Systems comprise constellations of satellites orbiting the Earth, emitting signals that can be received by ground-based receivers. These signals contain information about satellite positions and precise timing, allowing GNSS receivers to calculate their location accurately through trilateration shown in Figure 1. The most prominent GNSS is the GPS, operated by the United States, but other systems like GLONASS (Russia), Galileo (Europe), and BeiDou (China) contribute to the global coverage and redundancy of satellite signals.

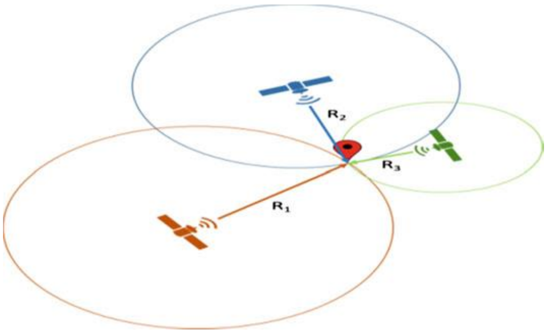

Figure 1 Trilateration of the Satellite

Applications of GNSS span across diverse sectors, encompassing navigation for vehicles, ships, and aircraft, precise timing for communication networks [4], disaster management, surveying, agriculture, and scientific research. GNSS has become an integral part of modern life, underpinning numerous technological advancements and improving efficiency across various industries.

While GNSS has brought unprecedented convenience and accuracy to location-based services, it is not without challenges. Threats such as signal interference, multipath reflections, and intentional spoofing pose risks to the reliability and security of GNSS data [11]. Researchers and engineers continually strive to develop advanced technologies, algorithms, and signal processing techniques to mitigate these challenges, ensuring the robustness and dependability of GNSS in an ever-evolving technological landscape. As the demand for precise positioning and timing information continues to grow, GNSS remains a cornerstone technology that shapes the way we navigate, communicate, and interact with the world around us.

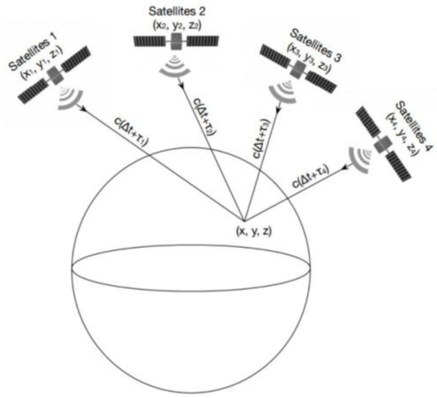

Figure 2 Topological of Satellite and GPS Signal Receiver (Four-Star Positioning)

The information provided describes the derivation of a formula for the satellite signal in the context of GPS timing characteristics, emphasizing the spatial coordinate system and the topological of satellite and GPS signal receiver is shown in Figure 2. The formula, expressed as

$$(\Delta t + \tau_i) \times c = Q(x_i, y_i, z_i) - Q(x, y, z)$$

It showcases the correlation between the temporal attributes that the received satellite signal and the spatial coordinates within the coordinate system possess. In the provided equation, Δt represents the time difference between the transmission time of the satellite signal (T_0) and the specified reference receiving Time (T). The variable $\tau_i$indicates the inherent time delay of the received signal from satellite i, and 'c' denotes the speed of light. The coordinates of satellite i are denoted by $Q(x_i, y_i, z_i)$, and those of the GPS receiver by Q(x, y, z). The subtraction of these two vectors yields the computation of distance, offering a fundamental insight into the GNSS concept. Figure 3 depicts a timing diagram illustrating the signals received by a GPS receiver module in a scenario involving four satellites for positioning.

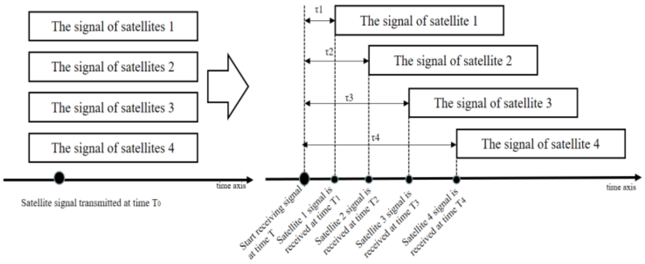
The signal of satellites 1
The signal of satellites 2
The signal of satellites 3
The signal of satellites 4
time axis
Satellite signal transmitted at time T_0
τ1
τ2
τ3
τ4
The signal of satellite 1
The signal of satellite 2
The signal of satellite 3
The signal of satellite 4
time axis
Start receiving signal at time T
Satellite 1 signal is received at time T_1
Satellite 2 signal is received at time T_2
Satellite 3 signal is received at time T_3
Satellite 4 signal is received at time T_4

Figure 3 Timing Diagram Illustrating the Signals Received by a GPS Receiver Module

For a system involving four satellite,

$$(\Delta t + \tau_1) \,.\, c = Q(x_1, y_2, z_3) - Q(x, y, z)$$
$$(\Delta t + \tau_2) \,.\, c = Q(x_1, y_2, z_3) - Q(x, y, z)$$
$$(\Delta t + \tau_3) \,.\, c = Q(x_1, y_2, z_3) - Q(x, y, z)$$
$$(\Delta t + \tau_4) \,.\, c = Q(x_1, y_2, z_3) - Q(x, y, z)$$

IV GNSS Spoofing

Spoofing in GNSS involves the transmission of counterfeit signals to deceive GNSS receivers, leading to erroneous position calculations. The impact of spoofing is particularly concerning in civil surveillance applications, where accurate positioning is crucial. Spoofing attacks can be categorized into various forms, such as signal replay, signal generation, or signal modification, each aiming to mislead the GNSS receiver. The consequences of successful spoofing attacks include compromised location accuracy, potential security threats, and risks to public safety.

A replay spoofing attack [18-21] is asecurity threat whereinthe attacker tries to get in and records legitimate communication between two parties and later replays that communication to misguide the system or toachieve a prohibited access. In the view of Global Navigation Satellite Systems (GNSS), replay spoofing attacks can occur when adversary records authentic signals sent from satellites to a receiver and subsequently replays those signals to the receiver at a later time.

A. GNSS Spoofing Signal

In essence, for successful satellite signal spoofing, the fake signal must share specific data characteristics with the authentic signal to deceive the target [22]. The mathematical representation of a typical GNSS signal is given by the following expression [23].

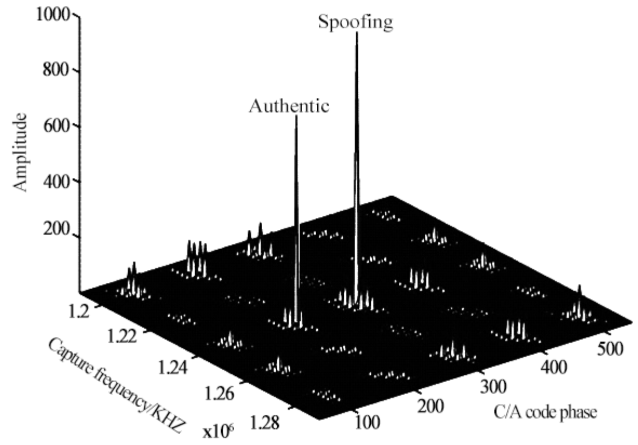

Figure 4 Spoofing Attacks in the Stage of Captured

$$y(t) = Re \sum_{i=1}^{N} AiDi(t - \lambda i(t))Ci(t - \lambda i(t))ej(\omega c\ t - \varphi i(t))$$

Figure 4 presents spoofing attacks in the stage of captured. In the realm of Global Navigation Satellite Systems (GNSS), let's delve into the parameters defining the signals. Here, we have 'N,' denoting the count of signals in the spreading code. Each signal is characterized by its amplitude 'Ai,' accompanied by the data bit stream 'Di(t)' and an extension code 'Ci(t).' This extension code could take various forms, such as binary phase-shift keying (BPSK), pseudo-random noise (PRN) code, or bindery offset carrier (BOC)/PRN code. The coding phase of the signal is represented by 'λi(t),' and the nominal carrier frequency is denoted by 'ωc.' Additionally, 'φi(t)' corresponds to the beat carrier phase of the ith signal. Figure 5 presents GNSS Spoofing Attack.

$$ys(t) = Re\sum_{i=1}^{N_s} A_{si}D_i(t - \lambda_{si}(t))C_i(t - \lambda_{si}(t))e_j(\omega c\ t - \varphi_{si}(t))$$

In general, the count of spoofed signals (Ns) matches the count of authentic signals (N). The strategy for deceiving the receiver involves ensuring that each spoofed signal shares an identical spreading code (Ci(t)) with its corresponding genuine signal, and its broadcasted data bit stream (Di(t)) typically mirrors the best estimate of the authentic data. For each spoofed signal indexed from 1 to Ns, the parameters including spoofing amplitude (Asi), coding phase (λsi), and carrier phase (φSi) may exhibit variations depending on the nature of the initiated attack. Throughout a spoofing attack [24], the receiver's reception is influenced, and the maximum total signal received is a crucial metric in evaluating the effectiveness of the deception. And given by:

$$y_{total}(t) = y(t) + y_s(t) + \mathrm{l}(t)$$

Here, l(t) denotes additional noise signals that could be present.

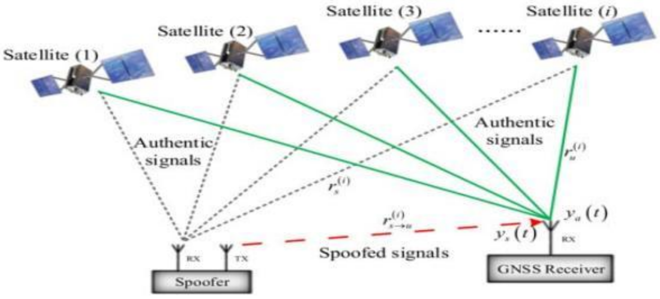

Figure 5 GNSS Spoofing Attack

B. GNSS Vulnerabilities and Threats

GNSS play in particularthe pivotal role for various aspects of trending life, providing accurate positioning and timing information for a wide range of applications. However, the widespread reliance on GNSS also exposes it to vulnerabilities and potential threats. One significant concern is the susceptibility to signal interference, where malicious actors can employ techniques such as jamming or spoofing to disrupt or manipulate GNSS signals. Jamming involves broadcasting radio frequency signals to overpower legitimate GNSS signals, leading to signal loss and inaccurate positioning. Spoofing, on the other hand, entails generating counterfeit GNSS signals to deceive receivers, resulting in misleading location information. These vulnerabilities pose risks to critical infrastructure, transportation systems, emergency services, and other sectors heavily dependent on GNSS accuracy. As GNSS continues to be integral to our interconnected world, addressing these vulnerabilities and developing robust security measures are imperative to ensure the reliability and resilience of GNSS services. This includes advancements in anti-spoofing technologies[25], signal processing methods, and international collaboration to mitigate the impact of potential threats and safeguard the integrity of GNSS for users worldwide.

Vulnerabilities because of The adoption of a broadcast communication mode in Global Navigation Satellite Systems (GNSS) is designed for user convenience, where navigation signals are directly broadcast to the majority of users [26]. However, this approach exposes the communication channel to potential vulnerabilities due to its direct exposure in the social space. The unprotected broadcast channel becomes susceptible to interference, monitoring, and tampering, posing security risks to the integrity of GNSS signals. Moreover, the GPS signal's inherent weakness upon reaching the ground, with an average signal power ranging from -150 dB to -160 dB [27], makes it particularly vulnerable to interference. The low directional power required to disrupt and suppress legal GNSS signals further contributes to the fragility of the GNSS signal in practical scenarios [28]. These challenges highlight the need for enhanced security measures to protect the broadcast channel and ensure the reliability and resilience of GNSS in the face of potential threats.

C. Spoofing Error Detection in GNSS

The Realm of contemporary navigation systems lays heavily reliant on GNSS, a burgeoning threat, wherein malicious entities manipulate GNSS signals to induce misguidance, necessitates the deployment of robust countermeasures for the preservation of navigational integrity. An efficacious strategy in this domain involves the meticulous scrutiny of received GNSS signals [29], with a particular emphasis on discerning alterations in critical signal attributes. Figure 6 gives tracking stage of spoofing attack.

TheSNR (Signal to Noise Ratio), one of the fundamental metric delineating strength of the signal, relative by thenoise that is ambient, emerges as a pivotal parameter for such analyses. The formula

$SNR_{genuine}=\mathbf{P}noise/\mathbf{P}signal$

Continuous monitoring of Doppler shifts enables the identification of irregularities indicative of spoofing, particularly when observed shifts deviate conspicuously from anticipated values predicated upon the kinematics of authentic signals.

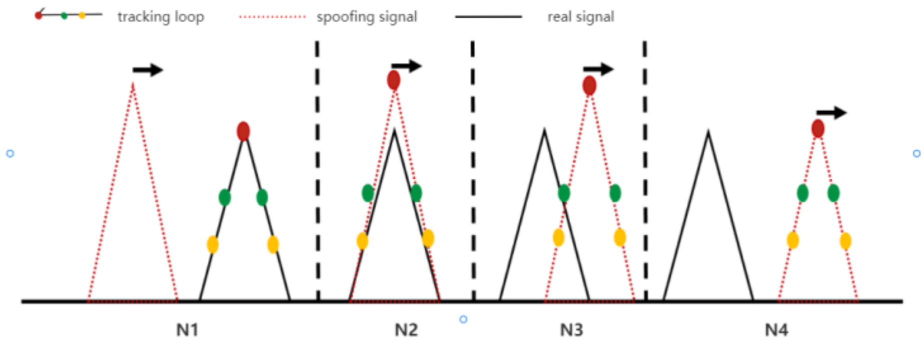

Figure 6 Tracking Stage of Spoofing Attack

Operationalizing these concepts necessitates sophisticated algorithms, continuous monitoring, and the integration of statistical methodologies and machine learning paradigms. Such an integrative approach augments the resilience of spoofing detection mechanisms, addressing the dynamic and intricate nature of the GNSS environment. As technological advancements continue, the imperative to fortify counter-spoofing measures remains paramount to preclude exploitations of emerging techniques and to uphold the dependability and trustworthiness of GNSS-based navigation systems.

V SUMMARY AND CONCLUSION

The summation or culmination of GNSS in civil surveillance projects has revolutionized the field, providing unprecedented accuracy, reliability, and efficiency. In conclusion, this technology has proven to be an invaluable asset for civil surveillance applications, offering a wide range of benefits and capabilities.

One of the key advantages of GNSS in civil surveillance is its ability to provide precise and real-time location information. This enables authorities to monitor and track assets, vehicles, and personnel with a high level of accuracy, enhancing overall situational awareness. Whether in urban environments or remote areas, GNSS ensures that surveillance operations can be conducted with precision, allowing for quick response times and improved decision-making.

In terms of security, GNSS enhances the integrity of surveillance systems by providing tamper-resistant location data. This ensures the authenticity and reliability of the information gathered, reducing the risk of unauthorized access or manipulation. The use of GNSS technology adds a layer of trust to the surveillance infrastructure, making it more resilient and capable of withstanding potential threats.

The cost-effectiveness of GNSS implementation in civil surveillance projects cannot be overstated. The technology reduces the need for extensive physical infrastructure, such as fixed surveillance cameras and sensors, by leveraging satellite-based positioning. This not only minimizes installation and maintenance costs but also allows for greater flexibility in deploying surveillance systems across diverse environments.

Moreover, GNSS enhances interoperability in civil surveillance by providing a standardized platform for location-based information. This facilitates seamless integration with other technologies and systems, such as Geographic Information Systems (GIS) and communication networks. The synergy between GNSS and these complementary technologies results in a more comprehensive and efficient surveillance ecosystem.

In conclusion, the incorporation of GNSS technology in civil surveillance projects represents a paradigm shift in how we approach monitoring and security. The benefits, including precise location information, enhanced geospatial data collection, improved security, cost-effectiveness, and interoperability, collectively contribute to the success of civil surveillance initiatives. While challenges exist, ongoing research and development efforts continue to strengthen the resilience and reliability of GNSS systems, ensuring their continued significance in shaping the future of civil surveillance.

VI REFERENCES

[1] Ledvina, B. M., Humphreys, T. E., O'Hanlon, B. W., Psiaki, M. L., & Kintner, P. M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Preprint of the 2008 ION GNSS Conference.*

[2] Parkinson, B. W., & Gilbert, S. W. (1983). NAVSTAR: Global positioning system-Ten years later. *Proceedings of the IEEE, 71*(10), 1177-1186.

[3] Kaplan, E. D., & Hegarty, C. J. (2006). *Understanding GPS: Principles and Applications*. Library of Congress Cataloging-in-Publication Data.

[4] Shi, R., Xu, J., & Yan, J. (2017). Detection on navigation deception signals based on direction finding by nulling antenna and angle contrast. *Mod. Navig, 8*(3), 193-198.

[5] ICG. (2007). *Second Meeting of the International Committee on Global Navigation Satellite Systems (ICG).*

[6] Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, *31*(4), 617-636.

[7] Key, E. (1995). *Techniques to counter GPS spoofing*. MITRE Corporation.

[8] Kerns, A. J., Wesson, K. D., & Humphreys, T. E. (2014). A blueprint for civil GPS navigation message authentication*. Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS).*

[9] Lo. S., Lorenzo, D. D., Enge, P., Akos, D., & Bradley, P. (2009). Signal authentication - A secure civil GNSS for today. *Inside GNSS*, 30-39.

[10] Margaria, D., Motella, B., Anghileri, M., Floch, J. J., Fernández-Hernández, I., & Paonni M. (2017). Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives. *IEEE Signal Processing Magazine*, *34*(5), 27-37.

[11] Broumandan, A., Jafarnia-Jahromi, A., & Lachapelle, G. (2015). Spoofing detection, classifiification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solutions*, *19*, 475-487.

[12] GPSP Team. (2014). *Global Positioning System (GPS) Standard Positioning Service (SPS) Performance Analysis Report*. William J. Hughes Technical Center.

[13] Misra, P., & Enge, P. (2006). *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press.

[14] Blakey, M. C. (2007). Letter to Dr. R. Kobeh, Federal Aviation Administration.

[15] Hinson, D. R. (1994). Letter to Dr. A. Kotaite, Federal Aviation Administration.

[16] Clinton, W. J. (2000). *Statement by the President regarding the United States' Decision to Stop Degrading Global Positioning System Accuracy*. Office of the Press Secretary.

[17] Perino, D. (2007). *Statement by the Press Secretary*. Office of the Press Secretary.

[18] Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE, 104*(6), 1258-1270.

[19] Gao, Z., & Meng, F. (2011). Principle and simulation research of GPS repeater deception jamming. *Journal of Telemetry, Tracking and Command*, 44–47.

[20] Scott, L. (2003). Anti-spoofing & authenticated signal architectures for civil navigation systems. *ION GPS/GNSS*.

[21] Humphreys, T. E. (2013). Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronics Systems*, *49*(2).

[22] Khanafseh, S., Roshan, N., Langel, S., Chan, F. C., Joerger, M., & Pervan, B. (2014). GPS spoofing detection using RAIM with INS coupling. *Position, Location and Navigation Symposium-Plans*.

[23] Huang, L., Gong, H., Zhu, X., & Wang, F. (2013). Research of re-radiating spoofing technique to GNSS timing receiver. *Journal of National University of Defense Technology*, (4), 93-96.

[24] Jahan, F. (2015). *Implementation of GNSS/GPS Navigation and its Attacks in UAVSim Testbed*. The University of Toledo.

[25] Zhang, L., Sun, C., Zhao, H., Feng, W., & Liu, H. (2020). The derivation and evaluation of algorithm of anti-spoofing attack on loosely/tightly coupled GNSS/INS integration system. *China Satellite Navigation Conference (CSNC) 2020 Proceedings*.

[26] Namie, H., Nishikawa, K., Sasano, K., Fan, C., & Yasuda, A. (2008). Development of network-based RTK-GPS positioning system using FKP via a TV broadcast in Japan. *IEEE Transactions on Broadcasting, 54*(1), 106-111.

[27] Sun, M. T., Feng, W. C., Lai, T. H., Yamada, K., & Fujimura, K. (2000). GPS-based message broadcast for adaptive inter-vehicle communications. *52nd Vehicular Technology Conference*.

[28] Langley, R. B., Jannasch, H., Peeters, B., & Bisnath, S. (2000). The GPS broadcast orbits: An accuracy analysis. *Proceedings of the 33rd COSPAR Scientific Assembly*.

[29] Xu, G., Feng, S., Amin, M., & Wang, C. (2018). DOA classification and CCPM-PC based GNSS spoofing detection technique. *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*.