International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Investigation of Suitable Anti Spoofing Algorithm for GNSS Receivers

Krishna Samalla[1], **Dr.P.Naveen Kumar**[2]

Submitted:11/03/2024 **Revised**: 26/04/2024 **Accepted**: 03/05/2024

Abstract: In an era driven by transformative technologies like 5G and the Internet of things (IoT), the Global position system vulnerability)-based navigation systems to spoofing attacks has become a paramount concern. Various techniques have been proposed to enable detections .This paper explains about anti –spoofing algorithms such as adaptive Kalman filter for dynamic positions and in GPS navigation, situations may arise where GPS receivers lack a clear line of sight to enough satellites ,such as when they are inside buildings .tunnels ,or aircraft with limited sky view .To tackle this challenge ,there is a techniques for initializing GPS receivers' to rapidly and effectively track signals once they are regain access to a clear sky vie .Furthermore ,in the context of unmanned aerial vehicles (UAVs) vulnerable to deliberate interference like spoofing attacks ,we present a comprehensive solution for GPS Spoofing detection and mitigation. This approach involves distributed radar ground stations equipped with local trackers .connected to fusion node

Keywords: *Anti spoofing algorithms, GNS Spoofing, GPS receivers, Adaptive Kalaman Filter, Automaticgain control*

1. Introduction

In today's technologically driven world with technologies like 5G and IOT , Global Positioning System (GPS)-based navigation has become an integral part of our daily lives, providing us with essential information about our position, velocity, and time (PVT). However, the widespread use of GPS systems, especially in critical applications such as unmanned [1] aerial vehicles (UAVs), has exposed them to vulnerabilities, most notably spoofing attacks

Spoofing attacks involve the manipulation of GPS signals, giving a significant threat to the security of GPS-based systems. [8]There are mainly on three type of problems on which this review paper has addressed

This paper explores various techniques and strategies to combat spoofing attacks and enhance the robustness of GPS navigation.[2]GPS receivers, which rely on signals from multiple satellites to determine precise locations, can face challenges when operating in environments with limited sky view, such as within buildings, tunnels, or high-speed aircraft. To address these challenges, researchers have developed innovative methods, like GPS repeaters and GPS spoofers. But again it was misused as GPS fake signal generation. To address this issue we introduced concept of AGC Additionally, the paper delves into the critical issue of detecting and mitigating GPS spoofing attacks, especially in the context of UAVs.[4-18-21]The proposed approach involves theintegration of distributed radar ground stations equipped with local trackers, creating a robust network to monitor and protect UAVs. By leveraging advanced tracking algorithms, like the extended Kalman filter framework [22]and global nearest neighbour association tracker frameworks, the system can estimate UAV positions and kinematics, detect spoofing attacks, and respond effectively.

GPS systems are vulnerable to spoofing attacks due to the weak signal strength of GPS receivers Spoofing attacks can be challenging to detect, especially in high dynamic positioning scenarios where GPS receivers are in rapid motion like UAVs,self drive cars and while moving in aircrafts. This paper proposes an anti-spoofing algorithm based on an adaptive Kalman filter to address the issue.

1.1. Techniques to Combat The GNSS/GPS Spoofing

In Early Days of Use

Code and Anti-Spoofing,[10-15] GPS receiver suddenly reports a significant Unrealistic change in position or time estimate, it may indicate a spoofing attack. For instance, if a vehicle's GPS receiversuddenly shows it teleporting across a large distance RAIM can be used to identify situations where signals from multiple GPS satellites donot align properly, indicating a potential spoofing attack.(RAIM)instantly, it's likely a sign of spoofing. RAIM can be used to identify situations where signals from multiple GPS satellites do not align properly, indicating a potential spoofing attack.(RAIM). Adding inertial sensors (like accelerometers) to a GPS receiver can help cross- compare reported movement with GPS data.(GPS receiver with inertial sensors reports significant movement while the GPS signals indicate no movement, it may raise suspicion of a spoofing attempt. These methods involve monitoring the correlation peaks in GPS signals and looking for

[1] *Sreenidhi Institute Of Science & Technology, Yamnampet, Ghatkesar, Hyderabad, Telangana 501301.*
ORCID ID : 0000-0002-7006-4136,
krishna.s@sreenidhi.edu.in
[2] *University College of Eng,Osmanaia University Hyderabad*
ORCID ID : 0000-3343-7165-777X
drnaveenkumarp9@osmania.ac.in

anomalies that might indicate the presence of spoofing signals

1.2. Algorithms Provided For Different Types Of Spoofing

When GPS receivers do not have direct access to sky view**.** In GPS navigation, GPS receivers typically need to receive signals from multiple GPS satellites in order to accurately determine their location. However, in certain situations, such as when the GPS receiver is inside a building, a tunnel, or an aircraft with limited sky view, it may not have a clear line of sight to enough GPS satellites to perform accurate positioning.[9-17-19] The technique mentioned is designed to address this situation. It involves initializing the GPS receiver in a way that allows it to quickly and effectivelystart tracking GPS signals once it gains access to a clear view of the sky. Here's breakdown of what it means: GPS Receiver Initialization: When the GPS receiver is initially powered on or activated, it goes through an initialization process. During this phase, the receiver attempts to acquire signals from GPS satellites and calculate its position

To resolve above issue we go for AGC. A G C stands for Automatic Gain Control. It's a critical component in GNSS/GPS receivers that helps optimize the gain of the front end to match the input range of the analog-to-digital converter (ADC).

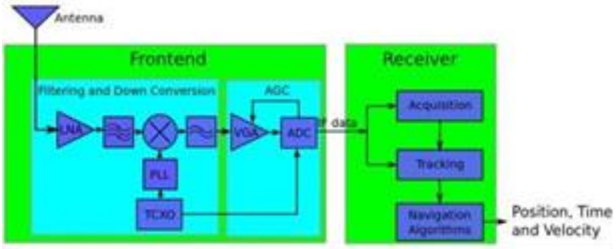

Fig1. Schematic Diagram Of An AGC Used in the Analog Telephone network.

AGC is essential for adapting the receiver to varying gain levels, such as those provided by different active antenna designs and early-stage front-end components. AGC adjusts the gain in the receiver's front end to achieve a specific distribution of incoming signal sample AGC for multibit ADC. [12-13]This distribution aims to minimize Multi-bit ADCs are commonly used in GPS receivers. AGC adjusts the gain to minimize quantization losses when converting analog signals to digital.AGC continuously monitorsthe distribution of samples and raises or decreases the gain if the distribution deviates from the expected Gaussian distribution

Sensitivity Of AGC Mechanism: Different GPS receivers may have varying levels of sensitivity within their AGC circuitry. A more sensitive AGC mechanism is desirable for better detection of Radio Frequency Interference (RFI) or spoofing signals An experiment was conducted **.**

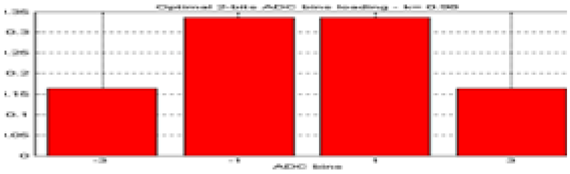

Fig.2. AGC Distribution for 4 optimal

to assess the ability of the AGC measurement to detect the presence of a spoofing signal generated by a GPS repeater. This experimentwas conducted with appropriate permissions at a test range with the support of the Swedish Defence Research Agency (FOI)

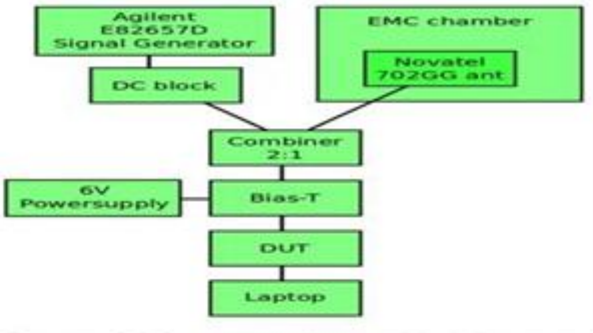

Fig 3.GPS /GNSS Spoofing Spoofing Scheme

Techniques for addressing the spoofing problem in Unmanned Aerial Vehicles (UAV)s. In following we can be solved

Deployment of Radar Ground Stations: Establish a network of radar ground stations equipped with local trackers in theoperational area where UAVs are deployed.

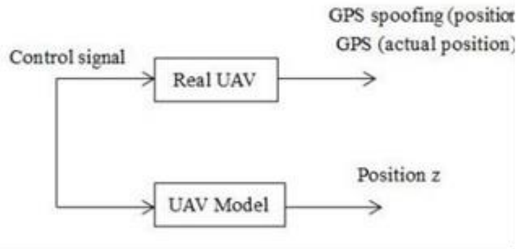

Fig 3.GPS /GNSS Spoofing Spoofing Scheme

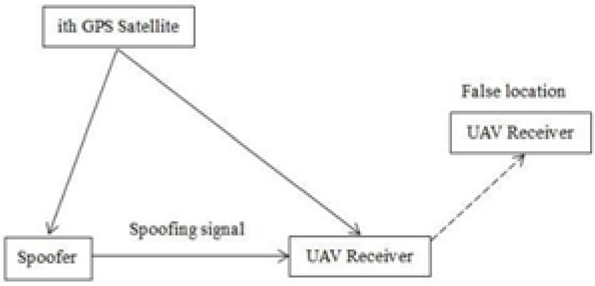

Fig 4. AGC Detection of Live Repeater Spoofing

Data Collection and Fusion:UAVs continuously estimate their position and velocity using extended Kalman filters and share this primary data with a central fusion node. Additionally, the UAVs estimate their time-varying kinematics and transmit this secondary data to the fusion node.

$$\sum_{i=1}^{n} h_{ij} e_i D(e_i) = 0 \quad j = 1, 2, \ldots$$

Track-to-Track Association: Implement a track-to-track association algorithm that compares the primary and secondary data to detect discrepancies or inconsistencies that may indicate a spoofingattack

Spoofing Detection: Use the track-to-track association results to detect spoofing attacks wheninconsistencies are detected

Correlation-Free Fusion.If a spoofing attack is detected, apply a correlation-free fusion technique to combine the primary and secondary data, providing a more accurate estimate of the UAV's truestate.

Spoofing Mitigation.Utilize the fused state obtained from the correlation-free fusion as a control input tothe UAVs to counteract the effects of the spoofing attack and ensure safe navigation.

Fig 5. Decision rule for Detecting the GPS Spoofing

2. Adaptive Kalaman Filter For High Dynamic Positioning

In High-Dynamic GPS navigation scenarios, observations during filtering can experience significant jumps, especially in the presence of spoofing interference.

These abrupt changes can lead to filtering process disruptions and even divergence, making it difficult to obtain accurate navigation results. An anti-spoofing algorithm based on an adaptive Kalman filter to address the issue. It leverages the orthogonality of innovation in Kalman filtering, which essentially means that the innovation (the difference between predicted and measured values) should be uncorrelated. Orthogonality in mathematics and signal processing means that two things are perpendicular or uncorrelated to each other. In this context, it means that the innovation at one time step should ideally be uncorrelated with the innovation atother time steps. Orthogonality means the error in one prediction should not besystematically related to the error in the next prediction.

$[Zk = HX + sk]$ (1)

$$\sum_{i=1}^{n} \psi(Z_{ki} - h_i X_k) h_{ij} = \sum_{i=1}^{n} \psi(e_{ki}) h_{ij} = 0 \quad j = 1, 2, \ldots \tag{2}$$

$$\sum_{i=1}^{n} f(Z_{ki} - h_i X_k) = \sum_{i=1}^{n} f(e_{ki})$$

(3)

(4)

This is the M-estimation, ψ( ) is the derivative function

of f( ) for the unknown vector

Make D(ei) = ψ(ei) /ei

Then the above equation becomes the weighted matrix of M-estimation is proposed

Threshold Detection: The algorithm starts by using a threshold determination technique to identify whether spoofing jamming is occurring during the GPS positioning process.

The Extended Kalman Filter Combined with M-estimation: If spoofing jamming is detected, the algorithm modifies the gain coefficient using M-estimation in statistics. This modification aims to counteract the effects of spoofing and improve the

accuracyof the filter's estimate. In the GPS anti-spoofing system, spoofing interference will have a great impact on the observed values in the Kalman filter process. These effects will be superimposedon the state estimation by the multiple of the Kalman gain K, resulting in a large deviation. Therefore, improved M-estimation theory is used to correct the gain coefficient in the Kalman filtering process by using the weighted estimation matrix ofthe innovation, so as to achieve the purpose of resisting spoofing jamming. According to GPS positioning calculation model, it can be seen that the observation equation ofreceiver positioning calculation system model is. The nonlinear function of the observation equation is expanded by Taylor series and the first order approximation is used to obtain the linear zed observation equation Among them, sk is the amount of error caused by

spoofing interference. H is the Jacobean matrix of vector function h[ ], also known as observation matrix. Thus for the linear zed observation equation, the residual function f( ) can be written as where f( ) is a properly selected scalar function, n represents the observed vector dimension, Zki represents the number i element in the observation vector at time k, hi represents the number i row of the observation matrix. Therefore, the residuals are derived and make it equal to zero, to minimize the residual

$$D(e_i) = \begin{cases} 1 & |e_i| < 1 \\ 1/|e_i| & 1 \leqslant |e_i| < m \\ 1/n\,|e_i| & |e_i| \geqslant m \end{cases} \tag{5}$$

Error Variance Reduction: The algorithm also works on reducing the error variance toensure that the Kalman filter's estimate is as close as possible to the true state of the system. This step contributes to filtering accuracy

A fading factor is introduced to reduce the reliance on previous state information and to emphasize current measurement information.

This approach enhances the convergence of the filter and improves stability, particularly in highdynamic scenarios. fading factor to restrict the memory length of Kalman filter, thus the application efficiency of historical status information is reduced, so as to achieve the purpose of reusing the current measurement information where λk is called fading factor, or forgotten factor

3. Conclusion

In the rapidly evolving technological landscape driven by innovations like 5G and theInternet of Things (IoT), the integrity and reliability of Global Positioning System (GPS)- based navigation systems are paramount. These systems are integral to numerous This analyzed paper has provided insights into several challenges and anti-spoofing algorithms for GNSS receivers applications, including unmanned aerial vehicles (UAVs), and are susceptible to spoofingattacks that can compromise their accuracy and security

Challenges Addressed: Limited Sky View: The paper has addressed situations where GPS receivers lack a clear line of sight to enough satellites due to obstacles like buildings, tunnels, or aircraft withlimited sky view

$$\sum_{i=1}^{n} f(Z_{ki} - h_i X_k) = \sum_{i=1}^{n} f(e_{ki})$$

$$\sum_{i=1}^{n} f(Z_{ki} - h_i X_k) = \sum_{i=1}^{n} f(e_{ki})$$

UAV Vulnerability: The paper emphasizes the vulnerability of UAVs to deliberateinterference through spoofing attacks, which can have serious consequences

Techniques and Solutions: GPS Receiver Initialization: A technique is introduced to efficiently initialize GPS receivers to rapidly track signals when they regain a clear sky view, especially in obstructed environments Automatic Gain Control (AGC): AGC is highlighted as a crucial component in GPS receivers to optimize signal reception, adapt to varying gain levels, and detect spoofingsignals

Track-to-Track Association: In the context of UAVs, the paper proposes a comprehensive solution involving distributed radar ground stations with local trackers. Track-to-track association is a key component to link and monitor UAV tracks, detect spoofing attacks, and apply countermeasures .Adaptive Kalman Filter: For high-dynamic GPS navigation, the paper suggests an adaptive Kalman filter-based anti-spoofing algorithm that addresses abrupt changes caused by spoofing interference The algorithm incorporates threshold detection, M-estimation, error variance reduction, and a fading factor to enhance filtering accuracyand stability

What still remains a requirement of further investigation in the research area: While various detection methods exist, there is no single, readily available methodology that is applicable to all GPS receivers. The choice of detection methoddepends on factors like receiver type, computational complexity, and infrastructure requirements. In conclusion, the review paper emphasizes the evolving challenges posed by spoofing attacks on GNSS receivers and provides valuable insights into various techniques and solutions to address these challenges. These efforts are crucial to ensure the continued reliability and security of GPS-based navigation systems in our technologically advanced world. As technology evolves, ongoing research and development in anti- spoofing algorithms will be essential to stay ahead of emerging threats and protect critical application.

$$P_{k,k-1} = \lambda_k \Phi_{k,k-1} P_{k-1} \Phi_{k,k-1}^{T} + Q_{k-1}$$

References

[1] [1].Ding, W. R. And L. Yun, “A Gps Receiver Adaptive Digital Beamforming Interference Suppres?Sion Algorithm Based On Kalman Filter,” Chinese Journal Of Electronics, Vol. 22, No. 2, 433–436, 2013

[2] Chan, Z. And M. L. Wei, “Application Of Extended Kalman Filter For Tracking High Dynamic Gps Signal,” 2016 Ieee International Conference On Signal And Image Processing (Icsip), 503–507, 2016

[3] Singh, A., “An Improvement Over Kalman Filter For Gps Tracking,” 2016 3rdInternational Conference On Computing For Sustainable Global Development (Indiacom), Ieee, 923–927, 2016

[4] Wang, Y., “Position Estimation Using Extended Kalman Filter And Rts-Smoother In AGps Receiver,” 2012 5th International Congress On Image And Signal Processing (Cisp),Ieee, 1718–1721, 2012

[5] Humphreys Te, Ledvina Bm, Psiaki Ml, O’hanlon Bw, Kintner Pm (2009) Assessing The Spoofing Threat. Gps World 20(1):28–39

[6] [6].Akos Dm (2012) Who’s Afraid Of The Spoofer? Gps/Gnss Spoofing Detection Via Automatic Gain Control (Agc). J Inst Navig 59(4)

[7] Caparra G, Ceccato S, Sturaro S, Laurenti N (2017) A key management architecture forGNSS open service navigation message authentication. In: Proceedings of European navigation conference (ENC), Lausanne, Switzerland, pp 287–297

[8] Humphreys TE (2013) UT Austin researchers spoof supery-acht at Sea. The University of Texas at Austin. [Online]. Available: http://www.engr.utexas.edu/features/superyacht-gps-spo ofing

[9] Shi, Chen S, Liu Z (2017) Analysis and optimizing of time-delay in GPS repeater deception.J Chongqing Univ Posts Telecommun (Natural Sci. Edition) 29(1):56–61

[10] Lo S, Lorenzo DD, Enge P, Akos D, Bradley P (2009) Signal authentication, a secure civil GNSS for today. Inside GNSS 4(5):30–39

[11] Psiaki ML,Humphreys TE (2016) GNSS spoofing and detection. Proc IEEE 104(6):1258–1270 Gao Z, Meng F (2011) Principle and simulation research of GPS repeater deception jamming.J Telemetry Tracking Command 32(6):44–47

[12] Jiang, Chen S, Chen Y, Bo Y, Xia Q, Zhang B (2018) Analysis of the baseline data basedGPS spoofing detection algorithm. In: Proceedings of IEEE/ION position, location navigation symposium (PLANS), Monterey, CA, USA, pp 397–403

[13] Scott L (2003) Anti-spoofing & authenticated signal architectures for civil navigation systems.In: Proceedings of the 16th international technical meeting of the satellite division of the institute of navigation (ION GPS/GNSS), Portland, OR, USA, pp 1543–1552 97

[14] Humphreys TE (2013) Detection strategy for cryptographic GNSS anti-spoofing. IEEE Trans Aerosp Electron Syst 49(2):1073–1090

[15] Humphreys TE, Ledvina BM, Psiaki ML, O’Hanlon BW, Kintner PM (2009) Assessing the spoofing threat. GPS World 20(1):28–39

[16] Dai, Xiao M, Huang S (2017) GPS spoofing and inducing model of UAV. Commun Technol 50(3):496–501

[17] He L, Li W, Guo C (2016) Study on GPS generated spoofing attacks. Appl Res Comput 33(8):2405–2408

[18] Shi M, Chen S, Wu H, Mao H (2015) A GPS spoofing pattern based on denial environment. JAir Force Eng Univ (Natural Sci. Edition) 16(6):27–31

[19] Broumandan A, Jafarnia-Jahromi A, Dehghanian V, Nielsen J, Lachapelle G (2012) ‘GNSSspoofing detection in handheld receivers based on signal spatial correlation. In: Proceedingsof IEEE/ION position, location navigation symposium, Myrtle Beach, SC, USA, pp 479–487

[20] Curran JT, O’Driscoll C (2016) Message authentication, channel coding & anti-spoofing. In 29th International technical meeting

[21] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch,I. Fernández-Hernández, and M. Paonni, ``Signal structure-basedauthentication for civil GNSSs: Recent solutions and perspectives,"IEEE Signal Process. Mag., vol. 34, no. 5, pp. 2737, Sep. 2017.

[22] L. Huang, Z. Lv, and F. Wang, ``Spoong pattern research on GNSS Receivers," J. Astronaut., vol. 33, no. 7, pp. 884890, Jul. 2012

[23] M. Sun, L. Zhang, J. Bao, and Y. Yan, ``RF ngerprint extraction forGNSS anti-spoong using axial integrated wigner bispectrum," J. Inf. Secur. Appl., vol. 35, pp. 5154, Aug. 2017.

[24] L. Zhao, Z. Miao, B. Zhang, B. Liu, G. Li, and X. Zhou, ``A novel spoong attack detection method in satellite navigation tracking phase,"J. Astronaut., vol. 36, no. 10, pp. 11721177, Oct. 2015

[25] M. Yuan, Z. Lv, H. Chen, J. Li, and G. Ou, ``An implementation ofnavigation message authentication with reserved bits for civil BDS antispoofng," in Proc. China Satell. Navigat. Conf. (CSNC), vol. 2, 2017,pp. 6980

[26] X. Liu and L. Zhang, ``Research and implementation of GNSS antispoong interference positioning algorithm based on multiple antennas,"in Proc. 12th Signal Intell. Inf. Process. Appl. Nat. Academic Conf., Hangzhou, China, Apr. 2018, pp. 14.

[27] A. Khalajmehrabadi, N. Gatsis, D. Akopian, and A. F. Taha, Real time rejection and mitigation of time synchronization attacks on the global positioning system," IEEE Trans. Ind. Electron., vol. 65, no. 8, pp. 64256435, Aug. 2018.

[28] M. Sun, L. Zhang, J. Bao, and Y. Yan, ``RF ngerprint extraction forGNSS anti-spoong using axial integrated wigner bispectrum," J. Inf.Secur. Appl., vol. 35, pp. 5154, Aug. 2017.