ISSN 2277-2685
IJESR/April. 2026/ Vol-16/Issue-2s/127-132
Mr. MohdTekBurhanuddin *et. al.*, / International Journal of Engineering & Science Research
Full Length Article

GPS Threat Detection Using CG-Trained ANN Framework

Mr. MohdTekBurhanuddin[1], Mr. Syed Abdul Baqi[2], Mr. M. A. Majed[3], Dr. SyedaGauharFatima[4]
[1,2,]UG Students; Department of ECE, Deccan College Of Engineering And Technology, Hyderabad, India
[3]Associate Professor, Department of ECE, Deccan College Of Engineering And Technology, Hyderabad, India
[4]Prof & HOD; Department of ECE, Deccan College Of Engineering And Technology, Hyderabad, India
Mail Id; mohdtekburhanuddin@gmail.com, sabdulbaqi04@gmail.com, majed@deccancollege.ac.in, gauharfatima@deccancollage.ac.in
Accepted 27-04-2026

Abstract:
The widespread dependence on Global Navigation Satellite Systems (GNSS), particularly GPS, has significantly increased vulnerabilities to intentional threats such as spoofing and jamming attacks. While various machine learning techniques—including Convolutional Neural Networks (CNNs), ensemble methods, and deep learning architectures—have demonstrated promising results in threat detection, the exploration of advanced optimization algorithms for training Artificial Neural Networks (ANNs) remains limited. This paper provides a comprehensive review of GNSS security threats and existing machine learning-based detection approaches. It proposes a novel research framework that employs the Conjugate Gradient (CG) optimization algorithm for efficient ANN training. Furthermore, it details the integration of CG-trained ANN (CG-ANN) models to achieve accurate, low-latency, and real-time detection of spoofing and jamming in GPS signals, potentially enhancing GNSS resilience in critical applications.

Keywords: *GNSS, GPS spoofing, jamming, artificial neural networks, conjugate gradient optimization, machine learning.*

I. Introduction:

It is almost impossible to imagine navigating modern life without the use of Global Navigation Satellite Systems (GNSS). Applications for navigation and positioning have become unavoidable, whether travelling somewhere, looking for something, or doing our job as bus, truck, taxi, ship, or plane crew. Stable and precise synchronization is of key importance in mobile networks for the successful connection of base stations and real-time data transmission, as well as for navigation and positioning services. Mobile networks must be synchronized so that base stations whose coverage overlaps do not interfere with each other causing call drops or service degradation. Due to the loss of synchronization, there is a deterioration in the quality of mobile transmission, a drop in the number of successful calls, and a decrease in the number of users. One of the important sources of reference signals for synchronization and provision of navigation and positioning services is GNSS. Constant improvement of existing systems ensures better precision.Currently the system has 31 satellites in orbit supporting L1 (1575.42 MHz), L2 (1227.60 MHz) and L5 (1176.45 MHz) frequencies. However, due to the increasing use of satellite navigation systems, there are an increasing number of threats and risks such as malicious attacks targeting these systems [1].

GNSS underpins aviation, infrastructure, and telecommunications, but threats like jamming (noise overwhelm) and spoofing (counterfeit signals) have surged, with incidents increasing dramatically in contested regions [2].

Classification of GPS threat:

Threat detection identifies disruptions to Global Positioning System (GPS) signals, primarily jamming (which overwhelms signals to cause loss of lock) and spoofing (which transmits counterfeit signals mimicking authentic ones to deceive receivers). These threats compromise position, navigation, and timing (PNT) in critical systems like military vehicles, aviation, and infrastructure. Detection relies on analysing radio frequency (RF) environments, signal characteristics, and cross-verification methods as shown in the fig. 1.

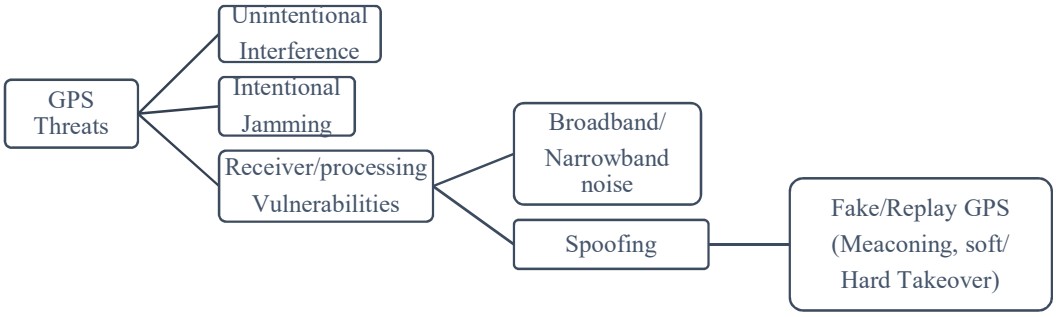

Fig. 1 Classification of GPS threat

GPS spoofing is an attack where a nearby radio transmitter sends fake GPS-like signals that overpower real satellite signals, tricking a receiver into computing a false position, time, or velocity as shown in Fig.3.

GPS Jamming floods receivers with noise, preventing satellite signal acquisition and disrupting mission-critical operations. Spoofing is subtler, starting with low-power fake signals synchronized to genuine ones, then overpowering them to report false positions or times.

Conjugate Gradient (CG) method is essentially correct and matches the standard mathematical treatment of CG for solving $Ax=b$ with A symmetric positive-definite (SPD), or equivalently for minimizing the quadratic as

$$f(x) = \frac{1}{2}x^T Ax - b^T x \quad (1)$$

The key idea is that CG generates a sequence of conjugate directions $\{P_k\}$ with respect to A, as per equation 2.

$$p_i^T Ap_j = 0, \text{ for } i \neq j, \quad (2)$$

which guarantees that the method converges in at most nn steps for an n-dimensional problem. **Problem setting and objective**

- When solving $Ax=b$ where $A \in R^{n\times n}$ is symmetric positive-definite.
- Equivalently, you are minimizing the convex quadratic as shown in equation.

whose gradient is $\nabla f(x)=Ax-b$. Residuals $r_k=b-Ax_k$ are then minus the gradient, $r_k=-\nabla f(x_k)2$.

II. Methodology

CG algorithm Framework

Starting from an initial guess x_0, the classical CG method proceeds as follows.

1. Initialize:
   - $r_0=b-Ax_0$ (residual)
   - $p_0=r_0$ (first search direction).
2. For k=0,1, 2:
   - Step size (optimal line search in direction p_k):

$$\alpha_k=\frac{r_k^T r_k}{p_k^T Ap_k} = \frac{p_k^T r_k}{p_k^T Ap_k}$$

(since $a_{rk}=Ap_{ke}$ only along the line) (3)

This makes x_{k+1} minimize f along the ray $X_u+\alpha p_k$.

   - Update solution and residual:

$x_{k+1}=X_u+\alpha_k p_k$,

$r_{k+1}=r_k-\alpha_k Ap_k$.

This is just the standard CG update in residual form.

   - Compute the next conjugate direction:
     - For the Fletcher–Reeves formula:

$$\beta_k=\frac{r_{k+1}^T r_{k+1}}{r_k^T r_k},$$

$$p_{k+1}=r_{k+1}+\beta_k p_k, \quad (4)$$

This β_k ensures that the new direction p_{k+1} is conjugate to all previous p_g. with respect to A.

GPS Threat Detection uses **CG-trained dynamic ANNs** (FTDNN/DTDNN) to identify spoofing/phishing attacks on user position (let/long/height) from input data, then predict lost signals.

Core Steps:

GPS Jamming and Spoofing

Data: Estimate position via Bancroft algorithm; label normal vs. phished

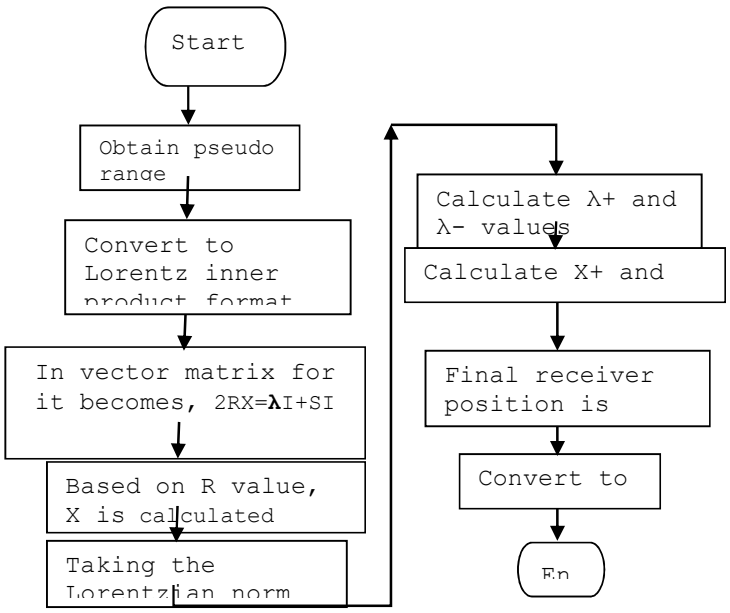

Fig.2Bancroft algorithm

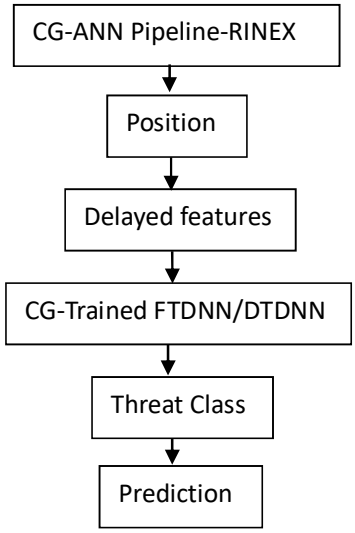

Fig. 3 CG-trained dynamic ANNs (FTDNN/DTDNN)

Features: Time-delayed inputs (order 2–10: input/hidden delays).
ANN: 4 hidden neurons (sigmoid), 1outputs (linear); train via **SCG/CGP/CGF** (CG variants).
Output: Detect threats; predict via past values;

Tab 1,2,3 shows the Root Mean Squared Error (RMSE) for different orders of FTDNN NN trained with SCG, CGF and CGP algorithms. With the increase in order (that is the number of input and output delays) MSE decreases.

Result and Discussions

Table 1: RMSE (dig) of latitude for various orders of FTDNN trained with SCG, CGF and CGF algorithms

RMSE (Dig)	**2**	**4**	**6**	**8**	**10**
SCG	1.2913	1.2792	1.2702	1.2593	1.2444
CGF	1.2842	1.2681	1.2576	1.2463	1.2493
CGP	1.3046	1.2913	1.2813	1.2701	1.2500

Table 3: RMSE (m) of height for various orders of FTDNN trained with SCG, CGF and CGP algorithms

RMSE(m)	2	4	6	8	10
SCG	54.9821	54.7393	54.5977	54.2806	54.2361
CGF	60.9976	56.8635	55.1765	55.0708	54.1212
CGP	60.9812	57.8341	56.7612	55.9821	54.0843

FTDNN trained with SCG has good performance over CGF and CGP algorithms as the RMSE for SCG algorithm of order 10 is minimum for latitude, longitude and height (1.2493, 0.9340 and 54.2361) when compared to that of CGF and CGP algorithms. The RMSE of order 10 trained with CGP algorithm is less for longitude and height (0.4121 and 54.0843) and for latitude it is less for CGF algorithm (1.2444).

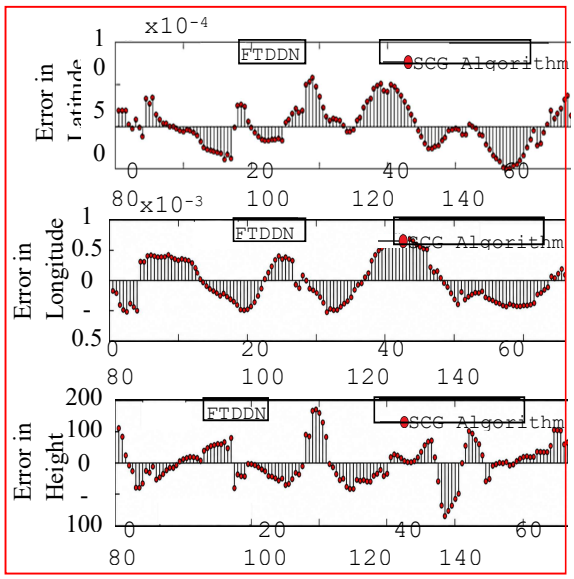

Fig.4Amount of error in prediction of GPS user position using FTDNN trained with SCG algorithm a) Latitudeusing FTDNN trained with CGF algorithm a) Latitude
b) Longitude c) Heightb) Longitude c) Height

Fig 4,5,6 shows Amount of error in prediction of GPS user position using FTDNN trained with SCG, CGF and CGP algorithmsa) Latitude b) Longitude c) Height shows the amount of error in predicted values over the 144 epochs for the FTDNN of 2nd order trained with SCG, CGF and CGP algorithms.

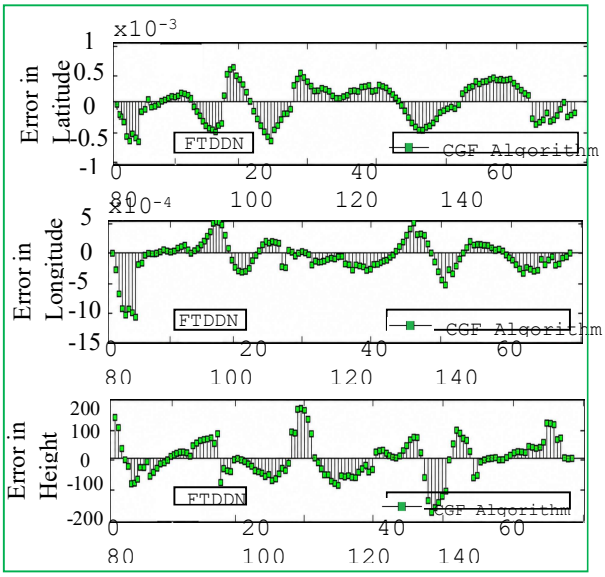

Fig.5 Amount of error in prediction of GPS User Position The amount of deviation from the zero line indicates the amount of error made at that instance by the neural network in its prediction. It can be observed from the graph that the error fluctuates to and from the zero-value mark till the last epoch. The amount of error is minimum for FTDNN of order 10 trained with SCG algorithm for latitude, longitude and height when compared to that of CGF and CGP algorithms.

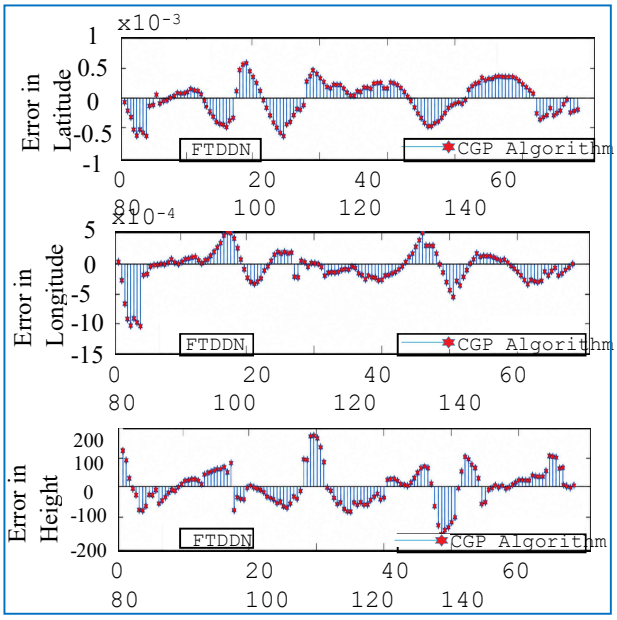

Fig.6Amount of error in prediction of GPS user position using FTDNN trained with CGalgorithma) Latitude
b) Longitude c) Heigh

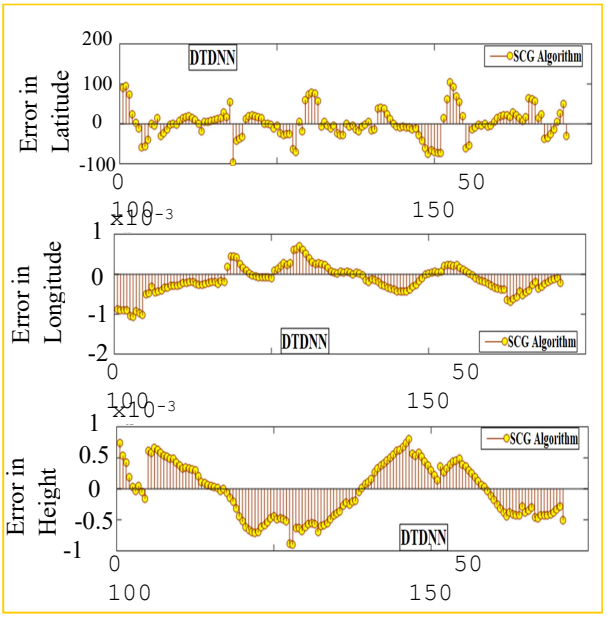

Fig.7 Amount of error in prediction of GPS User Position using DTDNN trained with SCG algorithm a) Latitude
b) Longitude c) Heigh

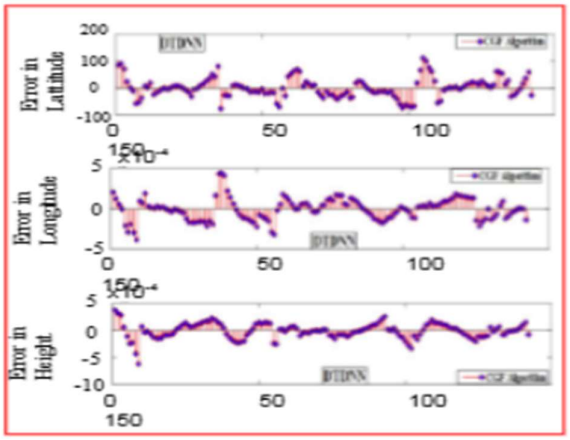

Fig.8Amount of error in prediction of GPS User Position using DTDNN trained with CGF algorithm

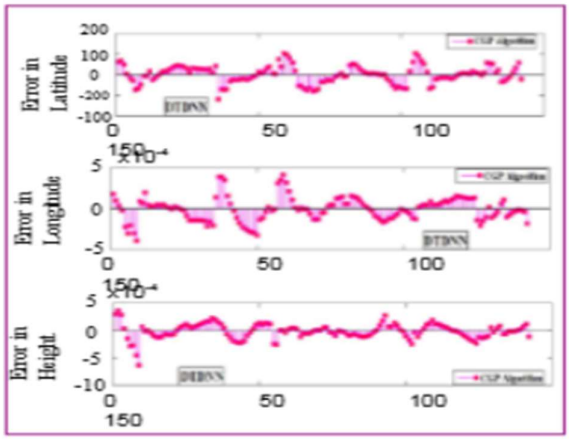

Fig.9Amount of error in prediction of GPS User Position using DTDNN trained with CGP algorithm

Fig 7,8,9shows the amount of error in predicted values over 144 epochs for DTDNN of order 2 trained with SCG, CGF and CGP algorithms. The amount of deviation from the zero line indicates the amount of error made at that instance by

the neural network in its prediction. It can be observed that the error in prediction oscillates to and from the zero-value mark till the last epoch and DTDNN when trained with SCG shows better performance than CGF and CGP algorithms. For latitude, longitude, and height, RMSE of DTDNN of order 10 trained with SCG algorithm is the lowest possible (0.6392, 1.2373 and 79.3131). SCG outperforms CGF and CGP algorithms in terms of performance. In comparison to CGP algorithm, the RMSE of order 10 trained with CGF algorithm is lower for latitude, longitude, and height (0.6897, 1.3387, and 80.9888).

Comparative Analysis of the performance of designed neural networks and the algorithms

The performance of FTDNN and DTDNN neural networks trained with the three conjugate gradient methods (SCG, CGP, and CGF) is compared in this section. It is observed from the graph that FTDNN shows best performance when trained with SCG algorithm

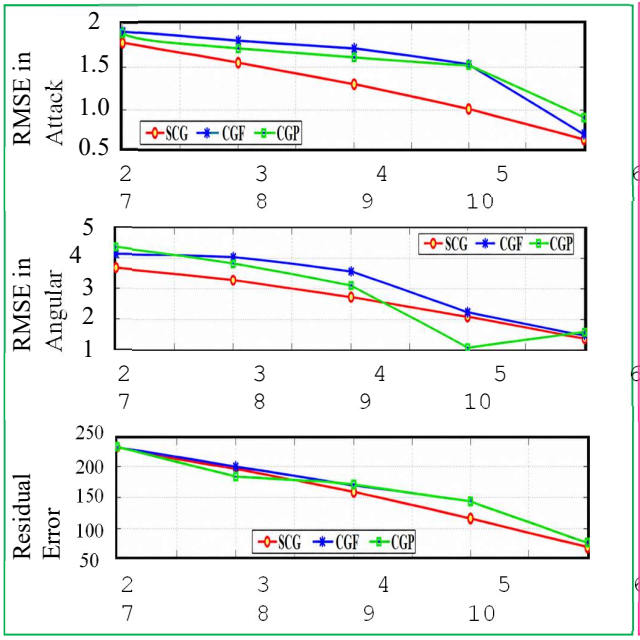

Fig.10 RMSE Vs order of NN for FTDNNalgorithm
Fig.11 RMSE Vs order of NN for DTDNN algorithm

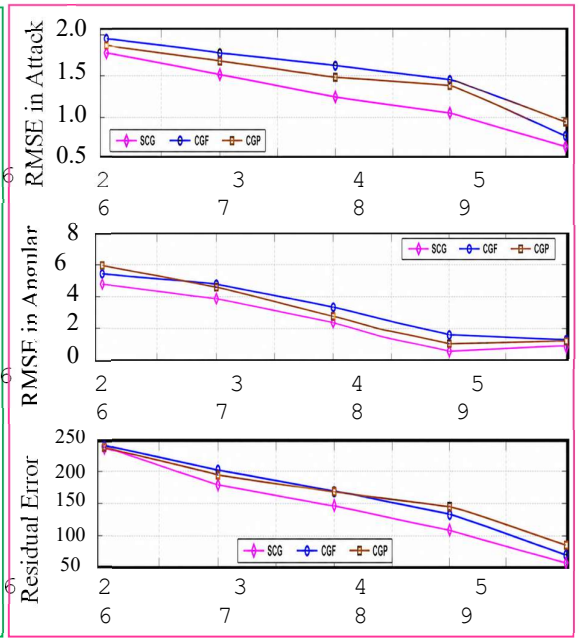

Fig. 10 shows the detection of GPS security threat and prediction of the user position with FTDNN of 2nd order

trained with SCG, CGF and CGP algorithms and shows the proximity of the neural network outputs with the targeted value of the user position. Fig.11 shows the amount of error in predicted values over 144 epochs for DTDNN of order 2 trained with SCG, CGF and CGP algorithms. The amount of deviation from the zero line indicates the amount of error made at that instance by the neural network in its prediction. It can be observed that the error in prediction oscillates to and from the zero-value mark till the last epoch and DTDNN when trained with SCG shows better performance than CGF and CGP algorithms. For latitude, longitude, and height, RMSE of DTDNN of order 10 trained with SCG algorithm is the lowest possible (0.6392, 1.2373 and 79.3131). SCG outperforms CGF and CGP algorithms in terms of performance. In comparison to CGP algorithm, the RMSE of order 10 trained with CGF algorithm is lower for latitude, longitude, and height (0.6897, 1.3387, and 80.9888).

Conclusion

This detail addresses GPS vulnerability to phishing by implementing Focused (FTDNN) and Distributed (DTDNN) Time Delay Neural Networks to detect spoofing and predict location during signal loss. Performance evaluations across Scaled Conjugate Gradient (SCG), Polak-Ribiero (CGP), and Fletcher-Reeves (CGF) training algorithms confirm the 10th-order FTDNN with SCG as the optimal configuration, yielding the lowest overall RMSE of 0.9340. While CGP demonstrates high accuracy for latitude (1.2444), CGF provides superior precision for longitude (0.4121) and altitude (54.0843) metrics. These results demonstrate that dynamic neural networks effectively enhance GPS signal resilience against sophisticated interference.

References

[1] SUSAN BERTRAM, LUCA EISENTRAUT, AND RICARDO BUETTNER, “A Systematic Literature Review
of Current Machine Learning Approaches for Detecting GNSS Spoofing Attacks”, IEEE ACCESS, Pg. no. 108898,
Volume 13,2025. DOI 10.1109/ACCESS.2025.3582435.

[2] A. Ghanbarzadeh et al., "GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep L
earning," arXiv:2501.02352, 2025.

[3] J. Tian et al., "Conjugate-Gradient-like Based Adaptive Moment Estimation Optimization Algorithm for Deep Learning," arXiv:2404.01714, 2025.

[4]Aireon Inc., "GPS Anomaly Trends," White Paper, 2025.

[5] S. A. Khan and M. A. Khan, "Dimensionality reduction and transformer-enhanced CNN for GPS spoofing
detection using CAF images," *Int. J. Electra. Electron. Eng.*, vol. 12, no. 3, pp. 45–58, 2024.

[6] KatarinaRado, Marta Brkić andDinkoBegušić “Recent Advances on Jamming and Spoofing Detection in GNSS”
sensors, MDPI, volume 24, issue 13, *Sensors* 2024, *24*(13), 4210; **https://doi.org/10.3390/s24134210**

[7] P. Borhani-Darian et al., "Detecting GNSS spoofing using deep learning," EURASIP J. Adv. Signal Process., vol.
2024, no. 14, 2024.

[8] J. Smith et al., "Crowdsourced ML for GNSS jammer detection: Random forests and Gaussian processes," *SSRN*
Electron. J., preprint, 2024. [Online]. Available: https://ssrn.com/abstract=5119211

[9] K. Radoš et al., "Recent Advances on Jamming and Spoofing Detection in GNSS," Sensors, vol. 24, no. 13, p.
4210, 2024.

[10] N. Sato et al., "Scaled Conjugate Gradient Method for Nonconvex Optimization in Deep Neural Networks,"
arXiv:2412.11400, 2024.

[11] Sathyabama Inst. Sci. Technol., "AI-SIEM for cyber threat detection using deep neural networks," Dept. Inf.
Technol. Rep., 2024.

[12] SandboxAQ, "The growing threat to GPS: Policy imperatives for resilient navigation," Blog Post, 2024. [Online].
Available: https://www.sandboxaq.com/post/the-growing-threat-to-gps-that-policymakers-cant-ignore

[13] Space Security Project, "Threats to GPS Reliability," Johns Hopkins Univ., 2024.

[14] Novatel. What Are Global Navigation Satellite Systems? Available online: https://novatel.com/tech-talk/an-
introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss (accessed on 15 October 2023).

[15] Additional conceptual placeholders for CG variants and datasets.

[16]Conjugate gradient method - Wikipedia