International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

SOFTKILL: An AI Assisted Framework for GNSS Signal Analysis and Interference Simulation

Vishnukanth Kulkarni, P Jignesh, R Tafazul Khan, Samartha P, Shravan K Kodidhala
Department of Artificial Intelligence and Machine Learning
AMC Engineering College, Bengaluru 560083, India

Abstract - GNSS quality monitoring is difficult to demonstrate in a small student laboratory because receiver measurements reveal only part of the underlying signal environment. We propose SOFT KILL, a low-cost framework that combines live GPS observations with software-generated degradation scenarios and AI-based condition inference. A u-blox NEO-6M receiver and Arduino Uno provide navigation messages to a host computer. The host retains the measured baseline and creates separately labeled copies for controlled changes in signal-quality indicators, satellite availability, position and time. Random Forest serves as the primary classifier, while a Long Short-Term Memory model is proposed for temporal analysis. The design includes explicit data provenance, an uncertainty-aware decision layer and a browser dashboard. Its central contribution is a reproducible evaluation workflow that distinguishes simulated measurement anomalies from actual radio-frequency interference. The paper specifies feature extraction, session-based dataset partitioning, benign confounders and performance measures. It presents a proposed architecture rather than a validated detection system, and therefore reports no experimental accuracy or field performance. The framework is intended for education and preliminary research, with independent recorded-data validation required before operational use.

Index Terms: GNSS, GPS, interference simulation, receiver observables, Random Forest, LSTM, anomaly detection.

I INTRODUCTION

A navigation display can continue to show a plausible position even when the observations supporting that position are becoming unreliable. For a student studying satellite navigation, this creates a useful question: what evidence can an inexpensive receiver provide about the quality of its solution, and how should an inference model interpret that evidence? GNSS interference research addresses reception loss, deceptive positioning and the difficulty of separating these conditions from ordinary environmental degradation [1]. An educational prototype should make those distinctions visible rather than reduce every weak-signal event to an attack label.

The proposed SOFT KILL platform addresses this problem at the measurement level. Its hardware records GPS navigation messages, while its software constructs controlled scenarios from copies of those records. This arrangement lets the user compare the measured baseline with an altered data stream and examine how features and model predictions change. The project name refers to the study of navigation disruption. The prototype itself has no interference transmitter and makes no attempt to deny service to another receiver.

The hardware choice sets an important boundary. The NEO-6M is a GPS L1 C/A receiver [2]. Its navigation interface does not supply the multi-band RF observations needed to identify unknown L1, L2 and L5 signals. The proposed system consequently identifies the signal band from receiver metadata and investigates observable quality changes. Automatic RF-band classification remains a separate extension requiring compatible recordings or upgraded acquisition hardware. The u-blox protocol documentation provides the basis for selecting navigation fields, including signal-strength values and fix-related messages [3].

We make three design contributions. First, we separate the original measurements from simulated copies and retain their provenance through inference. Second, we specify a feature-based classifier with an optional temporal

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

extension and an explicit abstention state. Third, we define an evaluation protocol that tests benign degradation, limits leakage between recording sessions and separates simulated performance from real-interference evidence. These contributions describe a research workflow to be implemented and tested. They do not establish a new state-of-the-art detector.

II RELATED WORK

Radoš, Brkić and Begušić review GNSS jamming and spoofing detection methods and organize the literature around the measurements and techniques available to a detector [1]. Their survey helps explain why one method cannot be assumed to transfer directly between receivers. A navigation-message stream, a calibrated power monitor and raw RF samples provide different evidence. Our design uses this distinction to constrain the feature set and to avoid claiming signal-level capabilities from a basic serial interface.

Kriezis et al. examine automatic gain control, satellite availability and carrier-to-noise density ratio under laboratory and open-sky conditions [4]. Their work motivates using several observables together and accounting for their natural variation. A related COTS-receiver study combines C/N_0 with calibrated received power to distinguish nominal, jammed, spoofed and blocked conditions [5]. That study has controlled-test and deployment evidence. Our prototype does not have an equivalent calibrated power channel, so its detection space is narrower and its class labels need more cautious interpretation.

Raichur et al. study machine-learning-assisted interference monitoring using smartphone GNSS features collected through a distributed platform [6]. Their measurement campaign includes conditions such as multipath and receiver motion. The work supports the use of receiver features for learning, but its data sources, spatial coverage and validation differ from a single NEO-6M setup. We therefore use it as a methodological reference rather than a performance benchmark that the proposed hardware can immediately reproduce.

TABLE I. RELATED WORK AND ITS RELEVANCE TO THE PROPOSED FRAMEWORK

Study	Evidence or approach	Design implication
Radoš et al. [1]	Review of GNSS detection methods	Match claims to the available observables.
Kriezis et al. [4]	AGC, satellite and C/N_0 monitoring	Include natural variation and combined features.
Kriezis et al. [5]	C/N_0 with calibrated received power	Basic NMEA does not reproduce this detection space.
Raichur et al. [6]	Learning from distributed smartphone features	Include benign confounders and independent sessions.

The gap addressed here is practical rather than algorithmic: an inexpensive laboratory platform needs a traceable way to connect receiver observations, controlled perturbations and model evaluation. The proposed novelty lies in that constrained workflow. It does not depend on asserting that low signal strength alone identifies jamming, or that a position jump alone proves spoofing.

III PROPOSED SYSTEM ARCHITECTURE

Figure 1 summarizes the proposed data flow. The receiver and microcontroller form the acquisition stage. A host service parses the serial stream and writes an immutable baseline record. Both a measured-data path and a scenario path can then supply the feature extractor. The inference stage receives observation-derived features, while scenario labels remain in the evaluation store. A decision layer attaches quality information to predictions before the dashboard displays them.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

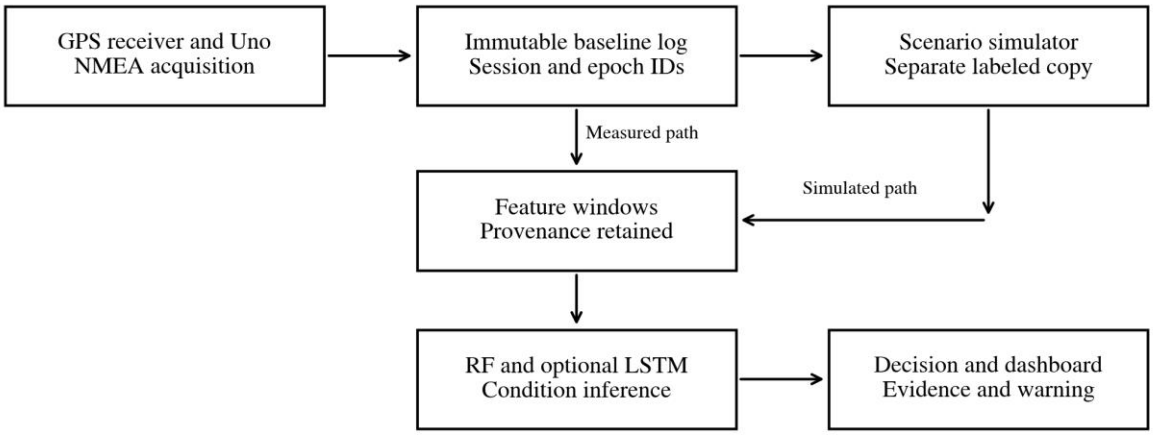

Fig. 1. Proposed architecture with separate measured and simulated data paths.

A Acquisition and Hardware Boundary

The NEO-6M sends NMEA messages over UART to a configured serial input on the Arduino Uno. The Uno forwards the stream to the host over USB. A common ground is necessary, and the receiver supply must follow the actual board specification. The bare NEO-6M supply range is 2.7–3.6 V [2]. A breakout board may include a regulator, but its presence does not establish that every serial pin accepts 5 V. If the Uno sends configuration commands to the receiver, the connection requires verified voltage compatibility or suitable level shifting. The acquisition sketch performs forwarding and basic integrity checks. Model inference runs on the host.

B Observation Records and Provenance

Each stored epoch includes a recording-session identifier, a host timestamp, the receiver timestamp when available, fix-related fields and the associated satellite observations. The parser verifies NMEA checksums, assembles multipart GSV messages and records missing or incomplete fields. It distinguishes satellites in view from satellites used in the position solution. A blank signal-strength field remains missing rather than becoming a zero-quality observation. These rules prevent communication errors from silently appearing as meaningful physical events.

Measured records and scenario records use different mode identifiers. Every scenario record points back to its baseline session and records the transformation settings, event onset and random seed. The system excludes these identifiers and generator settings from model inputs. Keeping labels outside the feature stream prevents an apparently accurate classifier from learning the scenario generator’s metadata rather than the observations themselves.

C Host Software and Dashboard

The host implementation is planned in Python, using serial acquisition and NMEA parsing with NumPy and Pandas for processing. Scikit-learn supports the Random Forest baseline. TensorFlow or PyTorch can support the temporal extension. A browser interface displays per-satellite C/N_0 histories, visible and used satellite counts, fix validity and position changes. It also shows the active data mode, the predicted condition and the evidence supporting a warning. The dashboard is a monitoring interface, not an autonomous navigation controller.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

IV MEASUREMENT SCENARIOS AND FEATURE EXTRACTION

A Scenario Definitions

The scenario generator creates observation-level perturbations. A jamming-like scenario reduces recorded C/N₀ indicators, removes selected tracked observations or introduces fix-loss intervals. A spoofing-like scenario adds controlled offsets or gradual drift to position and time fields. These transformations represent symptoms that an inference system might encounter. They do not recreate receiver tracking-loop behavior, propagation effects or authentic counterfeit satellite signals. Changing a displayed fix flag also does not cause the physical module to lose its fix.

Benign degradation is part of the scenario set. Satellite geometry changes, antenna obstruction, gaps in serial data and multipath-like position variation can resemble the effects used in interference examples. Including such cases makes the learning task harder, but gives the evaluation a more useful interpretation. The planned labels are normal, benign degradation, jamming-like anomaly and spoofing-like anomaly. Labels describe the generator's known scenario, not a confirmed cause for an unlabeled live event.

B Feature Windows

TABLE II. PLANNED RECEIVER OBSERVABLES AND FEATURES

Observable	NMEA source	Planned summary
Satellite C/N₀	GSV	Median, spread and change across a window
Satellite availability	GSV and GGA	Visible count, used count and count changes
Fix quality or validity	GGA and RMC	Invalid-fix fraction and transition duration
Position and time	GGA and RMC	Position increments and timestamp consistency
Geometry and DOP	GSV and GSA	Elevation context and dilution changes

For each window, the extractor summarizes the median C/N₀ of available satellites, its variation, changes in visible and used satellite counts, the fraction of invalid fixes and the duration of missing data. Position increments and timestamp consistency add motion and timing context. Elevation and dilution-of-precision fields help describe the geometry of the observation period. Table II lists the principal inputs. C/N₀ is a carrier-to-noise density ratio expressed in dB-Hz; it is not a direct measurement of RF power [3].

Window length, sample rate and minimum observation coverage are experimental parameters rather than settled design constants. They will be selected on validation sessions and reported with the results. Training-set statistics will determine imputation and any normalization. Those same transformations will then be applied unchanged to validation, test and live data. A window with inadequate coverage will produce an insufficient-evidence state instead of a forced class assignment.

V AI INFERENCE AND DECISION LOGIC

A Random Forest Baseline

Random Forest is selected as the initial model because the planned inputs are tabular summaries rather than RF images or raw waveforms. Breiman's formulation combines randomized tree predictors [7]. In this project, the forest will learn relationships between the observation-derived features and scenario labels. The implementation will compare its predictions with a threshold baseline that uses signal-quality change, satellite loss and fix validity. Tree count, depth limits and class weighting will be tuned using validation sessions.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Feature importance will support error analysis, but it will not establish the physical cause of an event. Correlated variables can share importance, and a useful predictor may reflect the simulator rather than a receiver mechanism. Permutation tests on held-out sessions and removal of feature groups will therefore be used to investigate which measurements actually influence the classifier. The final report will include feature definitions, the preprocessing configuration and the model seed.

B Temporal Extension

A Long Short-Term Memory network is proposed for sequences of feature vectors. The original LSTM formulation addresses learning over time through recurrent memory mechanisms [8]. Here, its intended role is to investigate slow drift and persistent degradation that short statistical windows may summarize poorly. Sequences will stay within a recording session and preserve their observation order. Missing epochs will be represented explicitly or handled through a documented mask rather than hidden by interpolation.

The hybrid design remains a hypothesis. We will compare Random Forest alone, LSTM alone and a validation-tuned combination. One candidate is to consult the temporal model when the baseline produces sustained uncertainty; another is to combine model scores after evaluating calibration. Neither policy will be selected using the final test set. The LSTM will be retained only if it offers a useful reduction in false alarms or detection delay relative to its computational cost.

C Uncertainty and Risk Interpretation

A predicted class must be accompanied by observation coverage and model confidence. Tree-vote proportions or neural-network output scores are not automatically calibrated probabilities. The decision layer will use a validation-selected confidence threshold and permit abstention. Under live operation, the displayed warning will describe an observation anomaly consistent with the learned scenario. It will not certify that jamming or spoofing has occurred.

The proposed risk indicator summarizes signal-quality deterioration, fix availability and inference confidence using a documented heuristic. It is an operational display of the current evidence, not a probability of a future attack. The indicator should show its component values so that a user can distinguish weak reception from a position-consistency warning. Recommended actions remain limited to inspecting antenna placement, retaining the evidence window and checking the navigation solution against an independent source.

VI PLANNED EVALUATION PROTOCOL

A Data Collection and Dataset Partitioning

Evaluation will begin with several independently recorded baseline sessions under documented reception conditions. Session logs will include receiver configuration, firmware information where available, antenna placement and sampling settings. Controlled scenarios will use varied event onset, severity and duration. Importantly, the underlying recording sessions will be separated into training, validation and test groups before feature windows or altered copies are generated. Every derivative of one baseline session will remain in the same partition.

This grouping reduces leakage from overlapping windows and repeated receiver traces. Test scenarios will also include transformation settings and random seeds that the models did not encounter during tuning. A robustness test will change the perturbation pattern rather than only its magnitude. If performance collapses under that change, the model may have learned generator-specific cues. That outcome would be reported as a limitation rather than concealed by a favorable aggregate score.

The Texas Spoofing Test Battery provides recorded spoofing scenarios for evaluating civil GPS authentication methods [9]. It is a useful candidate for later independent validation, but its binary recordings are not interchangeable with a NEO-6M NMEA log. A compatible processing stage must first extract comparable

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

observables, and unavailable fields must remain identified as unavailable. The present design does not claim to have downloaded, processed or tested TEXBAT.

B Metrics and Ablation Studies

The planned classification report includes per-class precision and recall, macro-F1 and a confusion matrix. False alarms will be measured on both normal sessions and benign degradation. For event-level testing, the report will state the persistence rule used to create a warning, the number of false warning events per observation hour and the delay from labeled onset to the first qualifying warning. Missed events and abstained windows will be reported separately, so a model cannot improve its apparent reliability merely by avoiding difficult inputs.

System evaluation will record host hardware, model size, inference latency and dashboard update stability. Repeated seeds and uncertainty estimates across independent sessions will describe variation. Planned ablations remove position-related features, signal-quality features or the temporal model in turn. The analysis will examine whether any claimed benefit survives these removals and whether prediction confidence tracks actual errors. Table III summarizes the minimum scenario coverage.

TABLE III. PLANNED TEST SCENARIOS AND EVIDENCE TO REPORT

Test condition	Purpose	Evidence to report
Normal reception	Establish baseline behavior	False-warning rate and observation coverage
Benign degradation	Test confusion with ordinary disturbances	False positives and abstention rate
Jamming-like perturbation	Test quality-loss recognition	Recall, missed events and onset delay
Spoofing-like perturbation	Test position or time inconsistency	Recall under abrupt and gradual offsets
Unseen scenario settings	Test generator dependence	Metric change across held-out settings
Missing or incomplete data	Test quality gating	Abstention behavior and recovery time

VII DISCUSSION AND LIMITATIONS

The expected outcome is a reproducible educational platform with receiver logging, controlled scenarios and traceable model predictions. No measured results are available at the proposed-design stage, so the paper cannot conclude that Random Forest outperforms a threshold detector or that the hybrid model improves spoofing detection. Those comparisons are questions for the evaluation protocol. Even strong performance on generated scenarios would support only the claim that a model distinguishes those scenarios under the tested conditions.

The principal technical limitation is observability. A serial navigation interface hides much of the receiver's internal signal processing, and different physical causes may produce similar navigation symptoms. A gradual false position can remain plausible, while weak reception can arise without interference. Independent sensors, calibrated RF-power observables or a receiver exposing richer measurements could reduce ambiguity. They would also change the hardware cost and the experimental scope.

Simulation brings a separate limitation. Measurement perturbations are easier to control and reproduce than RF experiments, but they can simplify relationships among C/N_0, tracking status and navigation error. The simulator must document which relationships it assumes. Realism should be examined through comparisons with independent recorded data, not asserted from the visual appearance of dashboard traces. An observation simulator is also different from hardware-in-the-loop interference testing because it does not physically perturb the receiver.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Finally, deployment claims require evidence beyond this manuscript. The system is intended for classroom investigation and preliminary method development. Future work may evaluate richer receivers, authenticated navigation signals, independent motion references and multiple observation sites. Any such extension should preserve the separation between measured data, synthetic assumptions and confirmed event labels. This separation is necessary for both scientific interpretation and responsible use of the warning interface.

VIII CONCLUSION

We propose a low-cost framework for studying GPS quality and AI-based GNSS condition inference using a NEO-6M receiver, Arduino Uno and host-side software. The design preserves the measured baseline, creates separately labeled scenarios and evaluates feature-based and temporal models under a session-based protocol. Its main value is a clear connection between what the receiver observes, what the simulator changes and what the classifier can legitimately infer. The framework provides a practical starting point for educational research, while leaving real-interference detection, multi-band analysis and operational reliability to future empirical validation.

REFERENCES

[1] K. Radoš, M. Brkić, and D. Begušić, "Recent advances on jamming and spoofing detection in GNSS," Sensors, vol. 24, no. 13, Art. no. 4210, Jun. 2024, doi: 10.3390/s24134210.

[2] u-blox AG, "NEO-6: u-blox 6 GPS modules," Data Sheet GPS.G6-HW-09005-E, 2011. [Online]. Available: https://content.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_(GPS.G6-HW-09005).pdf. Accessed: Oct. 12, 2026.

[3] u-blox AG, "u-blox 6 receiver description including protocol specification," GPS.G6-SW-12013. [Online]. Available: https://content.u-blox.com/sites/default/files/products/documents/u-blox6-GPS-GLONASS-QZSS-V14_ReceiverDescrProtSpec_(GPS.G6-SW-12013)_Public.pdf. Accessed: Oct. 12, 2026.

[4] A. Kriezis, Y.-H. Chen, S. Lo, and T. Walter, "Identifying low cost GNSS monitor metrics for robust RFI detection," in Proc. Int. Tech. Meeting Inst. Navigation (ITM), Long Beach, CA, USA, Jan. 2024, pp. 426–440, doi: 10.33012/2024.19542.

[5] A. Kriezis, Y.-H. Chen, D. Akos, S. Lo, and T. Walter, "GNSS jamming and spoofing monitoring using low-cost COTS receivers," arXiv:2509.13600v2, Jul. 2026, doi: 10.48550/arXiv.2509.13600.

[6] N. L. Raichur et al., "Machine learning-assisted GNSS interference monitoring through crowdsourcing," in Proc. 35th Int. Tech. Meeting Satellite Division Inst. Navigation (ION GNSS+), Denver, CO, USA, Sep. 2022, pp. 1151–1175, doi: 10.33012/2022.18492.

[7] L. Breiman, "Random forests," Machine Learning, vol. 45, pp. 5–32, Oct. 2001, doi: 10.1023/A:1010933404324.

[8] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.

[9] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques," in Proc. ION GNSS, Nashville, TN, USA, 2012. [Online]. Available: https://radionavlab.ae.utexas.edu/texbat/. Accessed: Oct. 12, 2026.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)