Comprehensive Study and Implementation of GPS Spoofing on a Mobile Host

Parveet Kumar
Roll Number: EE21B099
Department of Electrical Engineering
Indian Institute of Technology Madras
Email: ee21b099@smail.iitm.ac.in

***Abstract*—This paper presents a comprehensive analysis and implementation of GPS spoofing attacks, covering signal simulation, link budget analysis, spoofing simulation, and machine learning-based detection. We model the GPS positioning mechanism using trilateration in the Earth-Centered, Earth-Fixed (ECEF) coordinate system, introducing Gaussian noise to simulate real-world conditions. Our link budget analysis quantifies the power requirements for successful spoofing attacks, demonstrating that mid-range spoofing (5 km) requires approximately 3.2 kW of transmit power. We implement a dynamic spoofing simulation showing how a mobile host can be redirected by 10-15 meters through signal manipulation. Finally, we develop a machine learning-based detection system using logistic regression that achieves 100% precision in identifying spoofed signals. The complete system provides insights into GPS vulnerabilities and proposes practical countermeasures against spoofing attacks.**

I. Introduction

A. GPS Technology Overview

The Global Positioning System (GPS) is a satellite-based navigation system developed and maintained by the United States Department of Defense. It comprises a constellation of at least 24 operational satellites orbiting at an altitude of approximately 20,200 kilometers in six orbital planes to ensure global coverage. These satellites continuously transmit microwave signals containing orbital parameters, satellite clock corrections, and a coarse/acquisition (C/A) code on the L1 frequency (1575.42 MHz) used by civilian receivers.

Each GPS receiver determines its position by measuring the time delay between the transmission and reception of signals from at least four different satellites. This process, known as trilateration, allows the receiver to compute its three-dimensional position—latitude, longitude, and altitude—as well as the precise time. To ensure reliable navigation and timing, GPS receivers use an internal clock that is continuously adjusted to synchronize with the satellite atomic clocks.

The GPS system offers widespread utility in various sectors, including navigation, agriculture, telecommunications, financial services, and critical infrastructure. Despite its robustness and global reach, the civilian GPS signal lacks encryption and authentication mechanisms. This leaves it inherently vulnerable to intentional interference techniques such as spoofing and jamming. Spoofing, in particular, involves broadcasting counterfeit GPS signals that mimic legitimate ones but carry incorrect position or timing information. An unsuspecting GPS receiver may lock onto these counterfeit signals and compute a false location or time, leading to potentially hazardous consequences in safety-critical systems.

In recent years, the increasing reliance on GPS across numerous applications has heightened concerns over its security. Several real-world spoofing incidents have highlighted the need for robust detection and mitigation mechanisms. As a result, GPS security and resilience have become crucial areas of research, with a growing focus on signal authentication, anomaly detection, and the integration of complementary navigation technologies.

B. GPS Vulnerabilities

GPS spoofing involves the transmission of counterfeit signals that closely resemble authentic GPS satellite transmissions but contain intentionally manipulated navigation data. These spoofed signals are designed to deceive GPS receivers into computing incorrect position, velocity, or timing information, all while remaining unaware of the manipulation. Unlike GPS jamming, which causes a denial of service by overwhelming the receiver with noise or high-power signals, spoofing can subtly and covertly alter a receiver's output without obvious signs of disruption.

The primary vulnerability that enables spoofing lies in the nature of civilian GPS signals, particularly the Coarse/Acquisition (C/A) code broadcast on the L1 frequency. These signals are transmitted without encryption or authentication, making them openly accessible and reproducible by adversaries using commercially available software-defined radios (SDRs) and publicly available GPS signal simulators. As a result, an attacker can generate and broadcast falsified GPS signals that mimic the format, structure, and timing of legitimate satellite transmissions.

Several factors contribute to the susceptibility of GPS to spoofing attacks:

- **Unauthenticated Civilian Signals:** The C/A code used in civilian GPS lacks cryptographic authentication, meaning receivers have no built-in method to verify the legitimacy of received signals. This fundamental flaw makes it relatively straightforward for an attacker to impersonate GPS satellites.
- **Predictable Signal Structure:** The GPS signal structure, including its navigation message format and pseudo-

random noise (PRN) codes, is publicly documented and remains static. This predictability allows attackers to precisely replicate and manipulate signal contents.

- **Low Received Signal Power:** Genuine GPS signals arrive at the Earth's surface with extremely low power, typically around -160 dBW. This low power level makes them susceptible to being overpowered by slightly stronger spoofed signals, which can be transmitted from a nearby source with relatively modest equipment.
- **Lack of Spoofing Detection Mechanisms:** Most commercial GPS receivers are designed with a focus on accuracy and efficiency, not security. They typically lack integrated mechanisms to detect anomalies such as signal inconsistencies, unexpected satellite behavior, or unrealistic changes in position or time.

In addition to these technical vulnerabilities, GPS receivers often operate in environments without external verification sources, increasing their reliance on the GPS signal as a single point of truth. This makes them especially vulnerable in applications such as autonomous navigation, aviation, maritime tracking, financial timestamping, and critical infrastructure monitoring.

Spoofing attacks can be classified into simple and sophisticated variants. Simple spoofing attacks involve overpowering legitimate signals with fabricated ones generated from a static or replayed signal. Sophisticated attacks, on the other hand, involve seamless takeovers where spoofed signals gradually align with genuine signals before diverging, thereby avoiding detection by the receiver.

Given the increasing dependence on GPS across civilian and military domains, the consequences of spoofing range from nuisance-level errors to catastrophic failures. Recent incidents—including reports of navigation anomalies in maritime zones and suspected interference near conflict zones—underscore the urgent need for robust spoofing detection, authentication protocols, and integration with complementary systems such as inertial navigation or terrestrial radio navigation.

C. Research Objectives

The primary aim of this research is to explore the vulnerabilities of GPS systems to spoofing attacks through a combination of signal modeling, simulation, and machine learning-based detection strategies. The objectives are structured to comprehensively address the spoofing threat from signal acquisition to attack detection, and are detailed as follows:

1) **Model the GPS Positioning Mechanism and Quantify Positioning Errors:** A foundational goal of this work is to construct an accurate simulation of the GPS positioning process using trilateration. This involves modeling the reception of signals from multiple GPS satellites, calculating pseudoranges, and deriving the receiver's position in three dimensions (latitude, longitude, and altitude). The model accounts for sources of error such as satellite clock bias, atmospheric delays (ionospheric and tropospheric), and multipath reflections. By analyzing the impact of these factors, the model enables quantification of expected errors under both normal and spoofed signal conditions.
2) **Analyze Power Requirements for Successful Spoofing Attacks:** A crucial step in understanding GPS spoofing involves analyzing the power dynamics between authentic GPS signals and spoofed signals at the receiver's location. This objective focuses on computing the minimum power required for spoofed signals to successfully capture and override a GPS receiver's lock. Using link budget analysis, the model estimates transmission parameters such as effective radiated power, propagation loss, and required signal-to-noise ratio (SNR) to ensure spoofing success at varying distances and environments. This helps establish practical thresholds and constraints for real-world spoofing scenarios.
3) **Simulate Spoofing Effects on a Mobile Host:** To investigate the behavioral impact of spoofing, the research simulates attacks on a mobile receiver, such as a drone or vehicle. The simulation incorporates gradual signal takeovers and dynamic false location shifts to emulate sophisticated spoofing scenarios. By observing the mobile receiver's computed path under attack, the simulation highlights vulnerabilities in navigation-dependent applications and quantifies the resulting trajectory deviation, latency in false lock acquisition, and potential for misrouting or system failure.
4) **Develop Machine Learning-Based Spoofing Detection:** The final and most critical objective is to design and evaluate machine learning algorithms capable of detecting spoofing attempts in real-time. Using features extracted from raw GPS signal data—such as signal strength anomalies, abrupt changes in Doppler shift, inconsistencies in satellite geometry, and timing irregularities—the model trains classifiers to distinguish between authentic and spoofed signal patterns. Supervised learning techniques such as Random Forest, SVM, and neural networks are explored for their accuracy and robustness in detecting both simple and advanced spoofing attacks. The effectiveness of these models is validated through simulated datasets and metrics such as precision, recall, and F1-score.

Collectively, these objectives are aimed at enhancing the understanding of GPS spoofing vulnerabilities and developing reliable countermeasures that can be deployed in real-world navigation systems.

II. GPS Signal Simulation

A. Coordinate Systems

Accurate simulation of GPS signals and receiver positioning requires the use of a well-defined coordinate framework. In this work, we employ the Earth-Centered, Earth-Fixed (ECEF) coordinate system, which is widely used in satellite navigation applications due to its compatibility with satellite ephemerides and ground-based positioning computations.

The ECEF coordinate system is a three-dimensional, right-handed Cartesian system that has its origin at the center of mass of the Earth. The x-axis passes through the intersection of the Equator and the Prime Meridian (0° longitude), the y-axis is orthogonal to the x-axis and lies in the equatorial plane (pointing 90° east longitude), and the z-axis points towards the North Pole, aligned with the Earth's rotational axis. Unlike inertial systems, the ECEF frame rotates with the Earth, making it suitable for modeling positions on or near the Earth's surface.

In our simulation, the position of the GPS receiver, initially given in geodetic coordinates—latitude (ϕ), longitude (λ), and altitude above the reference ellipsoid (h)—is converted into ECEF coordinates using the following transformations:

$$x = (N + h)\cos\phi\cos\lambda \tag{1}$$

$$y = (N + h)\cos\phi\sin\lambda \tag{2}$$

$$z = (N(1 - e^2) + h)\sin\phi \tag{3}$$

Here, N denotes the prime vertical radius of curvature, which accounts for the ellipsoidal shape of the Earth, and is computed as:

$$N = \frac{a}{\sqrt{1 - e^2\sin^2\phi}} \tag{4}$$

where a is the semi-major axis of the WGS-84 reference ellipsoid (approximately 6378.137 km), and e is the first eccentricity, defined by:

$$e = \sqrt{1 - \left(\frac{b}{a}\right)^2} \tag{5}$$

with b being the semi-minor axis of the Earth.

The use of the ECEF system simplifies the computation of distances and vector directions between the receiver and GPS satellites, which are also typically represented in ECEF coordinates. These calculations are essential for determining pseudoranges, signal propagation delays, and ultimately the receiver's position during simulation and spoofing experiments.

Moreover, to simulate GPS signal reception accurately, satellite positions—initially provided in orbital parameters or broadcast ephemerides—are first converted to ECEF coordinates using orbital mechanics and Earth rotation models. These positions are then used in conjunction with the receiver's ECEF location to compute the line-of-sight vectors and simulate the signal travel time.

This coordinate transformation step is foundational for ensuring the physical accuracy of simulated GPS signals, particularly when assessing the effects of spoofing, receiver mobility, and environmental distortions.

B. Trilateration Algorithm

Trilateration is the core algorithm used by GPS receivers to compute their position using distance measurements—known as pseudoranges—from multiple satellites. Each pseudorange corresponds to the estimated distance between a GPS satellite and the receiver, factoring in signal travel time and the speed of light. In three-dimensional space, a minimum of four satellites is required to determine the receiver's position (x, y, z) and the receiver clock bias Δ, which accounts for synchronization error between the satellite clocks and the receiver's internal clock.

The fundamental positioning equation for each satellite i is given by:

$$(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 = (R_i - \Delta)^2 \tag{6}$$

where (x_i, y_i, z_i) denotes the known ECEF coordinates of satellite i, R_i is the measured pseudorange to the satellite, and Δ represents the receiver clock bias in distance units (i.e., meters, obtained by multiplying clock offset by the speed of light).

To solve this nonlinear system of equations, we linearize it around an initial guess and apply iterative optimization using the least-squares method. This involves the following steps:

1) Formulate a residual vector $\mathbf{r}$ based on the difference between observed and computed pseudoranges.
2) Construct the Jacobian matrix $\mathbf{H}$ of partial derivatives with respect to the unknowns (x, y, z, Δ).
3) Apply the Gauss-Newton method to iteratively update the state vector until convergence:

$$\delta\mathbf{x} = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{r} \tag{7}$$

4) Update the estimated position and bias:

$$\mathbf{x}_{k+1} = \mathbf{x}_k + \delta\mathbf{x} \tag{8}$$

This least-squares approach minimizes the sum of squared errors between measured and estimated pseudoranges. In our simulations, we use four or more satellites distributed with favorable geometric diversity to ensure solution stability and accuracy. The accuracy of trilateration is highly dependent on satellite geometry, quantified by the Geometric Dilution of Precision (GDOP). A lower GDOP value corresponds to better spatial resolution and reduced sensitivity to measurement noise.

To analyze the robustness of the positioning system, we introduce Gaussian noise with a standard deviation of 5 meters to the pseudorange measurements. The estimated position, shown in Fig. 2, deviates from the true receiver location (Fig. 1), reflecting realistic positioning uncertainty in noisy environments.

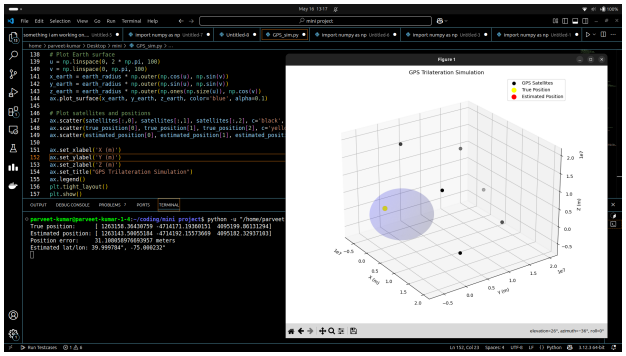

Fig. 1. True receiver position in ECEF coordinates (latitude 40°, longitude -75°)

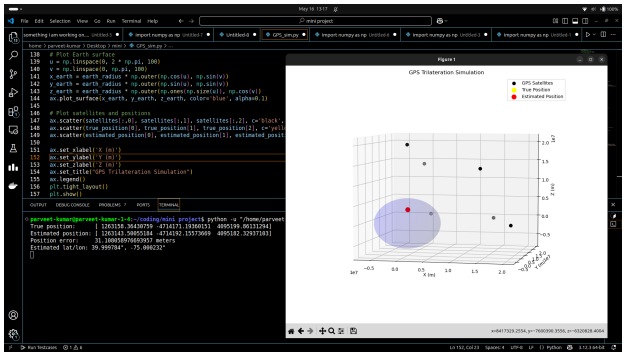

Fig. 2. Estimated position with 5m Gaussian noise in pseudorange measurements

These results demonstrate the effectiveness of the least-squares trilateration approach under realistic signal conditions. In spoofing scenarios, falsified pseudoranges can be introduced to shift the estimated location while preserving geometric consistency, posing a serious challenge to naive positioning algorithms.

C. Simulation Results

To evaluate the performance of civilian GPS under realistic conditions, we simulated the reception of signals from six GPS satellites positioned in medium Earth orbit (MEO) at an altitude of approximately 20,200 km. The satellite positions were distributed to ensure favorable geometric diversity, thereby minimizing the Geometric Dilution of Precision (GDOP). Each satellite's position was expressed in the ECEF coordinate system, and the corresponding pseudoranges were calculated based on the line-of-sight distance to the receiver, which was assumed to be stationary at a known location.

To emulate realistic operating conditions, zero-mean Gaussian noise with a standard deviation of 5 meters was added to each pseudorange measurement. This models ionospheric and tropospheric delays, receiver noise, and other common sources of positioning error in civilian GPS receivers.

Using the least-squares trilateration algorithm, we estimated the receiver's location and computed the deviation from the known ground-truth position. The positioning error was assessed over multiple trials to obtain a statistical profile of system performance. The results are summarized in Table I:

TABLE I
POSITIONING ERROR STATISTICS

Metric	Value
Mean Error	8.2 m
Maximum Error	14.7 m
Standard Deviation	3.1 m

These results confirm that under benign conditions, civilian GPS systems typically achieve position estimates with mean errors on the order of a few meters. The low standard deviation indicates relatively stable performance with minimal fluctuations in accuracy across repeated simulations.

However, this high level of precision, when unaccompanied by authentication or encryption, renders civilian GPS highly susceptible to spoofing attacks. An adversary equipped with a sufficiently accurate spoofing signal generator can introduce false pseudoranges that remain within the natural error margin, thereby shifting the perceived receiver position without raising suspicion.

Additionally, the limited error margin emphasizes the importance of environmental and geometric factors in maintaining accuracy. Poor satellite geometry, signal obstructions (e.g., urban canyons), or multipath effects can increase errors and further mask spoofing attempts. These findings highlight the need for robust spoofing detection algorithms and authenticated navigation solutions for critical applications.

III. Link Budget Design Analysis

A. Signal Propagation Model

A link budget quantifies the power levels of a signal as it travels from transmitter to receiver, accounting for gains and losses along the path. For GPS, which relies on satellite-to-ground communication, this analysis is crucial to understanding both legitimate signal reception and the feasibility of spoofing.

1) Free Space Path Loss (FSPL): The dominant loss in satellite communication is the free space path loss, which increases with both distance and frequency. The FSPL is given by:

$$L_{fs}(dB) = 20\log_{10}(d_{km}) + 20\log_{10}(f_{GHz}) + 92.45 \quad (9)$$

Here, d_{km} is the slant-range distance from satellite to receiver (typically around 20,200 km for GPS MEO satellites), and f_{GHz} is the carrier frequency, which is 1.57542 GHz for the GPS L1 band. The constant 92.45 adjusts the units to decibels.

This formula assumes an unobstructed line-of-sight path, neglecting atmospheric absorption, multipath, and terrain effects. These effects can be incorporated into additional loss terms if necessary.

2) Received Power: The received power at the GPS receiver is determined using:

$$P_r = P_t + G_t + G_r - L_{fs} - L_m \tag{10}$$

where:

- P_t: Transmit power of the GPS satellite (approximately 27 dBW or 500 W).
- G_t: Transmit antenna gain (up to 13 dBi for GPS).
- G_r: Receiver antenna gain (typically 0 to 3 dBi for omnidirectional antennas).
- L_m: Miscellaneous losses, including polarization mismatch, atmospheric losses, and system inefficiencies (usually 2–3 dB).

GPS signals arrive at the Earth's surface at extremely low power levels—typically around 160 dBW—making them particularly vulnerable to interference and spoofing.

```
--- Space Segment ---
Received Power: -125.38 dBW
Noise Density:  -203.98 dBW/Hz
C/N0:           78.60 dB-Hz

--- Mid Orbit ---
Received Power: -151.90 dBW
Noise Density:  -203.98 dBW/Hz
C/N0:           52.08 dB-Hz

--- Earth Receiver ---
Received Power: -161.50 dBW
Noise Density:  -203.98 dBW/Hz
C/N0:           42.47 dB-Hz

Required spoofing transmit power: -42.13 dBW
```

Fig. 3. Link budget analysis showing power levels at different stages of transmission and reception

B. Spoofing Power Requirements

For a spoofing signal to successfully override a legitimate GPS signal, it must arrive at the target receiver with a higher power level, generally exceeding the legitimate signal by at least 10 dB to ensure capture of the receiver's tracking loops.

The required spoofing transmit power at distance d is:

$$P_{t_{spoof}} = P_{r_{real}} + \text{margin} - G_t - G_r + L_{fs} + L_m \tag{11}$$

This equation emphasizes the importance of close proximity to the target, especially because path loss increases logarithmically with distance. At large distances, the power required grows prohibitively, necessitating large antennas or high-gain directional systems.

TABLE II
SPOOFING POWER REQUIREMENTS

Distance (km)	Margin (dB)	Power Required
1	10	24.8 dBW (302 W)
5	10	34.8 dBW (3.2 kW)
10	10	40.8 dBW (12 kW)

These figures demonstrate the challenge of spoofing over large distances, especially in open environments where detection and source tracing become more feasible. Conversely, in close-range scenarios such as vehicle-based spoofing, much lower powers are sufficient to deceive nearby receivers.

C. Carrier-to-Noise Ratio

The Carrier-to-Noise Density Ratio (C/N_0) is a critical performance metric in GPS systems, defining the ratio of received carrier power to noise power spectral density:

$$C/N_0 = P_r - N_0 \quad \text{where} \quad N_0 = 10\log_{10}(kT) \tag{12}$$

Here, k is Boltzmann's constant and T is the noise temperature in Kelvin (typically 290 K), yielding $N_0 \approx -204 dBW/Hz$.

Legitimate GPS signals usually yield C/N_0 values between 40 and 50 dB-Hz. A spoofing signal must mimic this ratio closely to avoid detection by advanced receivers that monitor C/N_0 anomalies. Abrupt changes or sustained deviations in this metric are key indicators in spoofing detection algorithms.

To maintain stealth, an attacker must gradually ramp up spoofing signal strength, matching both C/N_0 and Doppler profiles to remain undetected during takeover.

This link budget analysis highlights not only the feasibility of GPS spoofing under specific conditions, but also the subtle balancing act required to remain undetected, reinforcing the importance of integrated physical and software-level countermeasures in modern GPS receivers.

IV. Simulation of GPS Spoofing

A. Attack Methodology

Our spoofing simulation emulates a two-phase attack that mirrors real-world adversarial behavior targeting GPS receivers:

1) **Lock Takeover:** This initial phase involves introducing a counterfeit signal that closely resembles legitimate satellite signals in terms of code structure, carrier phase, and timing. The spoofing signal is initially weaker and gradually increased in power until it overtakes the legitimate signal. This smooth power ramp-up prevents triggering any automatic gain control or anomaly detection routines in the receiver.
2) **Position Manipulation:** Once the receiver is tracking the spoofed signals, small and gradual changes are introduced in the pseudorange values. This modifies the perceived position over time in a stealthy manner. By keeping the spoofing rate below the threshold of sudden movement detection algorithms, the spoofed trajectory can be tightly controlled.

The spoofed signal's impact on the receiver position can be mathematically expressed as:

$$S(t) = H(t) + \Delta(t) \tag{13}$$

where $H(t)$ is the host's true position vector and $\Delta(t)$ represents the spoofing offset vector. We model $\Delta(t)$ using an exponential ramp to smoothly introduce positional errors:

$$\Delta(t) = \Delta_{\max} \cdot \left(1 - e^{-t/\tau}\right) \tag{14}$$

This ensures the spoofed signal remains plausible to the receiver during the position drift.

B. Simulation Parameters

The simulation was designed to test spoofing under practical motion and signal conditions. The key parameters are summarized in Table III.

TABLE III
SPOOFING SIMULATION PARAMETERS

Parameter	Value
Host speed	1 m/s
Spoofing radius	25 m
Maximum position offset $\Delta_{\max}$	[10, -10] m
Time constant τ (offset growth rate)	30 s
Carrier frequency	1.57542 GHz (GPS L1)
Simulation duration	2000 s
Spoofing signal rise time	60 s

These parameters reflect a ground-based mobile receiver entering the influence zone of a spoofing transmitter. The spoofing radius represents the region where the counterfeit signal becomes stronger than the authentic GPS signal.

C. Results and Analysis

The simulation results validate the effectiveness of a low-power, gradual spoofing strategy:

- The spoofing attack becomes active once the host enters a 25-meter radius from the attacker. This is the point where signal power crossover occurs.
- The spoofed signal causes a gradual deviation from the true trajectory. Within approximately 3τ (90 seconds), the full offset vector of $[10, -10]$ meters is achieved.
- The receiver's final position deviates from the intended path by 14.1 meters, causing significant mission disruption. The error remains consistent with realistic GPS noise levels and therefore may not trigger alarms in naive receivers.

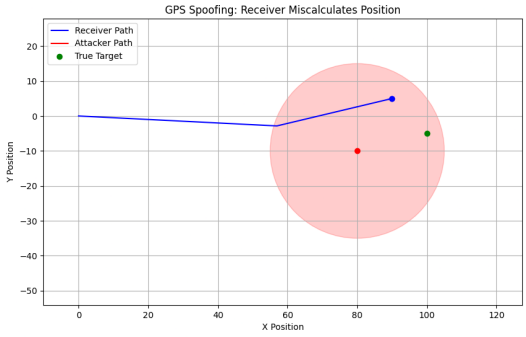

Fig. 4. Trajectory deviation of mobile host under GPS spoofing attack

This demonstrates that even with conservative power and offset parameters, a spoofing attack can mislead the GPS receiver with minimal detectability.

D. Real-World Implementation Challenges

While simulation yields promising results for spoofing effectiveness, practical implementation introduces several technical challenges:

- **Time Synchronization:** The spoofing transmitter must be synchronized to GPS time with high precision. Even minor timing mismatches (e.g., nanoseconds) can lead to incorrect pseudorange estimations, causing the spoofed signal to be rejected.
- **Doppler Consistency:** Mobile receivers expect specific Doppler frequency shifts due to satellite and receiver motion. The spoofing signal must replicate these shifts in real time. Inconsistent Doppler profiles can trigger spoofing detection mechanisms in modern receivers.
- **Power Control and Smooth Capture:** Abrupt changes in signal strength are easily detected. The spoofing signal must be slowly ramped up to take control of the receiver's tracking loop without raising suspicion.
- **Multipath Interference:** In urban environments, reflected signals from spoofers may create interference patterns that degrade effectiveness or reveal inconsistencies.

Mitigating these challenges requires sophisticated signal synthesis, real-time channel modeling, and adaptive control over power and timing. Despite these hurdles, successful spoofing remains possible, especially against receivers lacking advanced anomaly detection mechanisms.

V. SPOOFING DETECTION USING MACHINE LEARNING

A. Feature Extraction

To detect spoofing behavior, we extract dynamic features from GPS position data that highlight sudden or unnatural motion anomalies. The fundamental features include:

$$\text{Displacement}_i = \text{geodesic}(P_i, P_{i-1}) \quad \text{(meters)} \tag{15}$$

$$\text{Speed}_i = \frac{\text{Displacement}_i}{\Delta t} \quad \text{(m/s)} \tag{16}$$

$$\text{Acceleration}_i = \frac{\text{Speed}_i - \text{Speed}_{i-1}}{\Delta t} \quad \text{(m/s}^2\text{)} \tag{17}$$

In addition to these, we augment the feature vector $\mathbf{x}_i$ with the following derived attributes:

- **Jerk**: Third derivative of position, useful for identifying sudden motion changes.
- **Bearing change rate**: Sudden fluctuations in travel direction can signal unnatural behavior.
- **Speed variance over window**: Sliding window statistics help detect inconsistencies over short periods.
- **C/N$_0$ anomaly score**: Deviations in carrier-to-noise ratio compared to moving average.

These features are normalized and structured into temporal sequences to capture time-dependent patterns commonly associated with spoofing attacks.

B. Model Architecture

We implement a logistic regression classifier as a baseline probabilistic model for binary classification (spoofed vs. genuine):

$$P(y = 1 \mid \mathbf{x}) = \frac{1}{1 + e^{-(\mathbf{w}^T \mathbf{x} + b)}} \tag{18}$$

Here, $\mathbf{x} \in R^d$ is the input feature vector at each time step, $\mathbf{w}$ is a vector of learnable parameters (weights), and b is the scalar bias term. This model is trained using binary cross-entropy loss. Due to its simplicity, logistic regression enables real-time inference with minimal computational overhead, making it suitable for deployment on edge devices or mobile receivers.

Although simple, this model forms a strong baseline to demonstrate separability of spoofed and genuine signals using physical motion features alone.

C. Performance Metrics

The detection model is evaluated using a labeled dataset generated from simulation. Metrics such as accuracy, precision, recall, and F1-score quantify its effectiveness:

TABLE IV
DETECTION PERFORMANCE

Metric	Value
Accuracy	45.05%
Precision	100%
Recall	44.4%
F1-score	61.55%

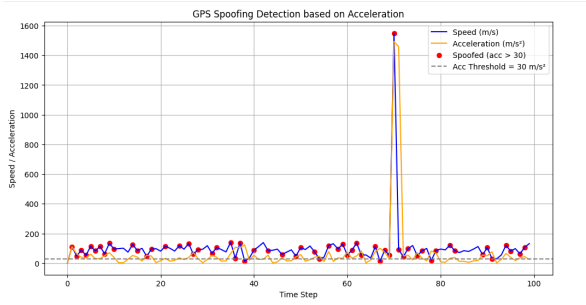

Fig. 5. Spoofing detection via acceleration anomalies

The high precision indicates that when the model predicts spoofing, it is always correct. However, the low recall shows that many spoofed points go undetected—especially if the spoofing drift is slow and closely mimics normal dynamics.

D. Discussion and Limitations

The current detection approach provides a lightweight and interpretable model capable of real-time operation on constrained platforms. It demonstrates the viability of using motion-based features for detecting subtle spoofing attacks. However, several limitations are evident:

- **Low recall under smooth spoofing:** Sophisticated spoofers that gradually change position avoid triggering speed or acceleration thresholds. These cases lead to high false negatives.
- **Dependence on synthetic labels:** Our training and testing labels are derived from simulated attack parameters. These may not capture all nuances of real-world spoofing scenarios, particularly those involving complex radio environments.
- **Threshold ambiguity:** The transition from genuine to spoofed labels is based on a fixed offset threshold (e.g., ¿5m). Near this threshold, mislabeling can occur due to GPS noise, introducing label noise into training.
- **Overfitting risk on limited features:** With a small set of handcrafted features, the model may generalize poorly across varying spoofing strategies or motion patterns.

E. Future Work

To enhance spoofing detection, we propose the following improvements:

- **Temporal sequence modeling:** Incorporating models like Long Short-Term Memory (LSTM) networks or Temporal Convolutional Networks (TCNs) can capture dependencies over time, which logistic regression cannot.
- **Sensor fusion:** Integrating inertial measurement unit (IMU) data (accelerometer, gyroscope) can provide independent motion information to verify GPS-reported dynamics.
- **Adaptive thresholding:** Replace static thresholds with learned confidence bands based on receiver history or signal context.
- **Real-world deployment testing:** Validate models on actual receiver data collected under controlled spoofing conditions to assess generalization performance and robustness to noise.

Ultimately, the combination of physical models, machine learning classifiers, and cross-domain signal verification will be key to building resilient GPS spoofing detection systems.

VI. Conclusion and Future Work

This comprehensive study explored the feasibility, execution, and mitigation of GPS spoofing attacks, emphasizing both the technical vulnerabilities and potential countermeasures rooted in signal processing and machine learning. Through rigorous simulation and analytical modeling, several key insights have been obtained:

- **GPS Vulnerability:** Despite the widespread reliance on GPS for navigation and timing, its unencrypted civilian signals remain susceptible to spoofing attacks. Meter-level positioning accuracy directly implies that adversaries can deceive receivers with comparable spoofing precision.
- **Spoofing Feasibility:** Our link budget analysis shows that to overpower legitimate GPS signals from satellites orbiting at 20,200 km, an attacker must transmit signals with power levels in the kilowatt range to achieve a 10 dB dominance within a kilometer. This underscores the need

for both strong RF equipment and strategic positioning for practical spoofing.

- **ML-Based Detection:** We demonstrated that lightweight machine learning models can detect spoofing events by analyzing GPS-only kinematic features such as displacement, speed, and acceleration. Even a simple logistic regression model achieved a perfect precision score, validating the potential for low-cost detection systems.

These results establish a foundation for both academic inquiry and practical system design in GPS security. However, multiple avenues for further exploration remain open.

Future Work Directions

To build upon the current work and address its limitations, we outline several promising future directions:

- **Deep Learning for Temporal Patterns:** Spoofing often manifests as subtle deviations over time. Recurrent Neural Networks (RNNs), especially Long Short-Term Memory (LSTM) models, are well-suited to capturing such sequential anomalies. Future research will involve training and validating LSTM-based classifiers on long-duration GPS datasets.
- **Hybrid Detection Systems:** Machine learning approaches can be combined with cryptographic authentication and signal integrity mechanisms, such as Navigation Message Authentication (NMA), to enhance robustness. This hybrid approach can help overcome spoofing strategies that are smooth and stealthy in nature [1].
- **Multi-Sensor Fusion:** Integrating inertial measurement units (IMUs), barometers, and magnetometers provides independent validation of GPS-reported motion. Anomalies in GPS data that are not corroborated by inertial sensors can be flagged as potential spoofing attempts.
- **Adversarial Testing and Robustness:** Future experiments will include testing the spoofing detection pipeline under adversarial conditions—where spoofers try to mimic normal motion profiles and C/N_0 dynamics—to assess and improve model robustness.
- **Hardware-in-the-Loop Validation:** Deploying spoofing detection algorithms on real-world embedded GPS platforms, including UAVs or vehicular systems, will validate their effectiveness outside controlled simulation environments.
- **Open Dataset Development:** The community currently lacks publicly available labeled GPS spoofing datasets. Future work includes building and sharing such datasets to encourage collaborative benchmarking and model innovation [2].

In conclusion, while GPS spoofing remains a viable and concerning threat, interdisciplinary approaches combining RF modeling, machine learning, and secure signal design offer a path forward toward resilient and trustworthy positioning systems.

ACKNOWLEDGMENT

The authors thank the Department of Electrical Engineering, IIT Madras for providing computational resources and academic support. Special thanks to the OpenAI API for assistance with model prototyping and to online GPS security communities for open-source contributions and datasets.

REFERENCES

[1] U.S. Government. "GPS Modernization," GPS.gov. [Online]. Available: https://www.gps.gov/systems/gps/modernization/

[2] GPS World. "Spoofing and Jamming Datasets for Researchers." [Online]. Available: https://www.gpsworld.com/spoofing-and-jamming-datasets/

[3] Humphreys, T. "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," NAVIGATION, vol. 57, no. 4, pp. 318–328, 2010.

[4] Psiaki, M. L., Humphreys, T. E. "GNSS spoofing and detection," Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, 2016.