Comprehensive Study and Implementation of GPS Spoofing on a Mobile Host

This project explores GPS spoofing, a technique to deceive GPS receivers by transmitting counterfeit signals. It covers simulation of GPS signals, link budget analysis, practical spoofing implementation, and machine learning-based detection mechanisms, this study aims to build a full-stack spoofing simulation and develop countermeasures to detect such attacks effectively.

Course: EE4901 - Mini Project

Roll Number: EE21B099

Institute: IIT Madras

by Parveet Kumar

Introduction to GPS and Spoofing

GPS Overview

GPS is a satellite-based navigation system providing precise location, velocity, and time synchronization worldwide. It is widely used in transportation, aviation, agriculture, defence, and smartphone navigation.

GPS Spoofing

GPS spoofing involves transmitting fake GPS signals to trick receivers into computing incorrect locations. This project focuses on simulating such attacks and developing data-driven detection methods.

Simulation of GPS Signal

Problem Statement

- GPS-based navigation is foundational for countless modern applications: from civilian mapping and logistics to military precision targeting.
- However, GPS signal integrity is susceptible to environmental disturbances and deliberate attacks.
- One critical vulnerability arises from the inherent reliance on satellite time-of-arrival signals, which can be delayed or spoofed.
- Misleading or inaccurate location computation can cause failure in navigation systems, fleet operations, and real-time asset tracking.

Theory Behind Trilateration

- A GPS receiver calculates its position by measuring its distance to multiple satellites using signal travel times.
- The intersection of spheres, each centered at a satellite and with a radius equal to distance, determines the receiver's position.
- Minimum four satellite signals are required to solve for the four unknowns.

Mathematical equations involve solving for

$$(X,Y,Z,\delta) : Ti = (X - Xi)^2 + (Y - Yi)^2 + (Z - Zi)^2 = (c.Ti + c.\delta)^2$$

Where Ti is time difference between the time at which signal is sent to time of receiving the signal.

Where δ is receiver's clock bias.

Proposed Solution - GPS Simulation

- Simulated six satellites in an Earth-Centered, Earth-Fixed (ECEF) coordinate system.
- Receiver placed at a known location on Earth's surface.
- Gaussian noise ($\sigma \approx 5$–10 meters) added to pseudorange measurements to emulate signal fluctuations due to atmospheric conditions.
- Position estimated using a linearized least squares solution to the nonlinear trilateration equations.
- Position converted back to latitude and longitude to validate geographic plausibility.

Results - Estimated vs. True Position

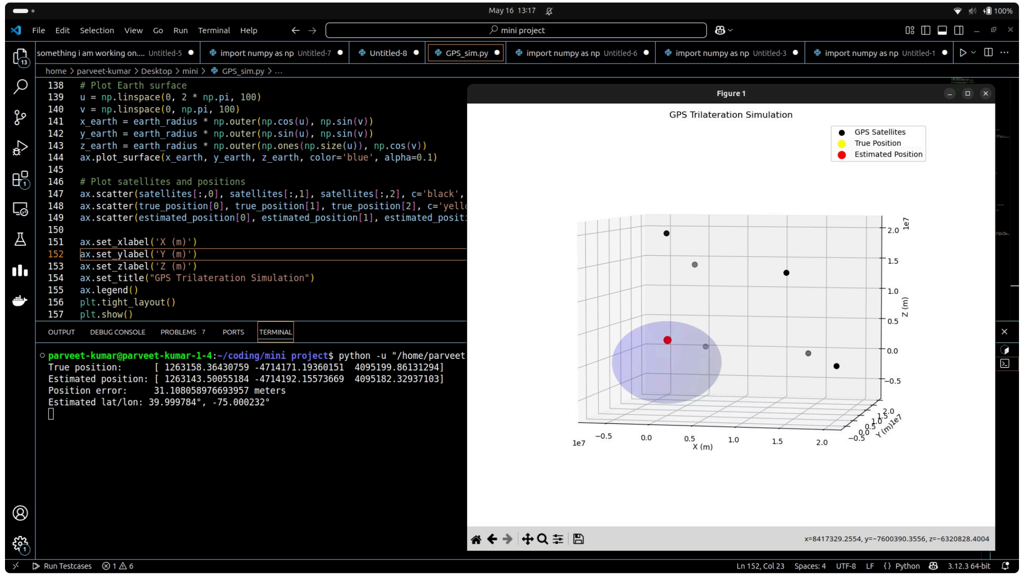


Fig : Estimated Position of Receiver

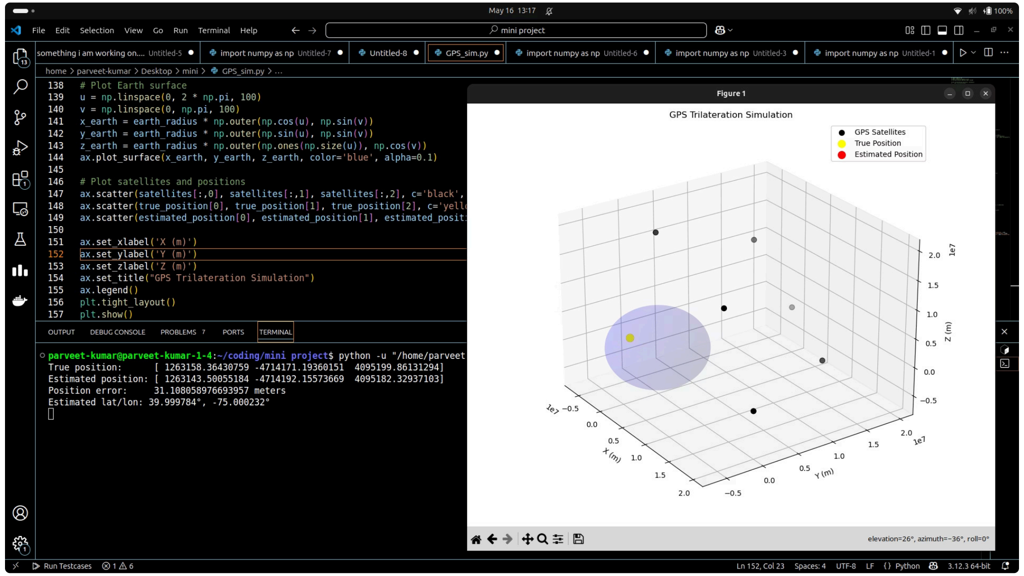


Fig: Real Position of Receiver

Results - Estimated vs. True Position

- The simulation outputs a position estimate with an average error in the range of 7–12 meters.
- Visualization showed satellite constellation, true position, and estimated point in 3D.
- Latitude/longitude conversion proved the location was geographically close.
- The experiment demonstrated that position can still be estimated under moderate noise, but highlights fragility to stronger signal distortions.

Insights and Challenges

- Noise in signal timing drastically affects positional accuracy.
- Satellite geometry (Dilution of Precision - DOP) plays a crucial role in accuracy.
- Simplified models ignore effects like ionospheric delay, satellite drift, or multipath reflections.
- These challenges form the basis of vulnerabilities that spoofing exploits.

Link Budget Analysis and Spoofing Power Requirements

1

Link Budget Concept

Evaluates total gain and loss from transmitter to receiver, helping determine minimum power needed for spoofing to override legitimate signals.

2

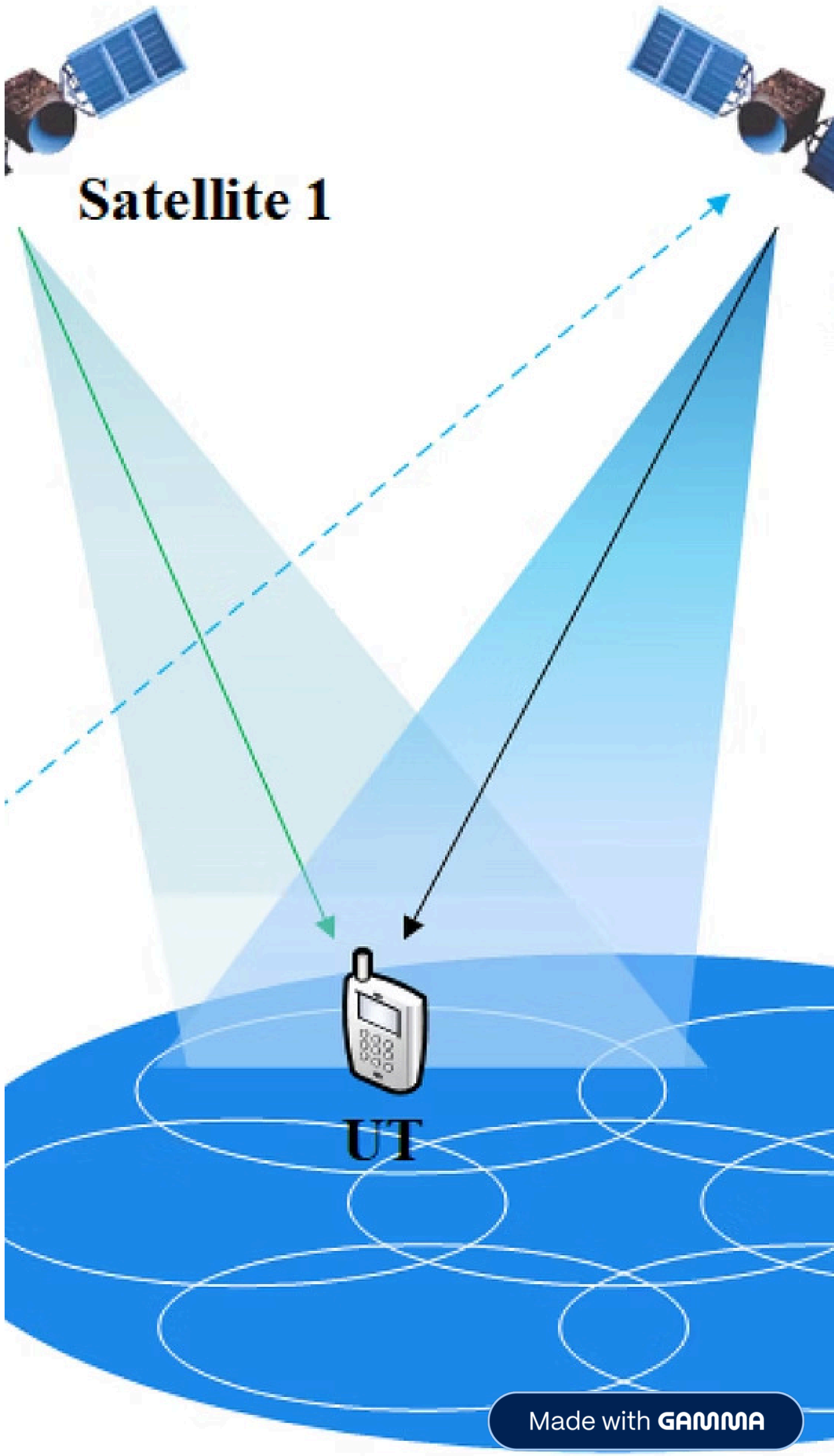
Path Loss Formula

Signal attenuation depends on distance and frequency, with GPS L1 frequency at 1.57542 GHz. Greater distance or frequency increases loss.

3

Power Calculation

To spoof successfully from 5 km, attacker requires nearly 34.8 dBW power, exceeding legitimate signal by 10 dB to maintain signal lock at receiver.



Problem Statement - Link Budget for Spoofing

- GPS signals originate from satellites over 20,000 km away and arrive at Earth with very low power.
- Attacker devices can locally transmit stronger signals that overshadow satellite transmissions.
- To assess spoofing feasibility, it is necessary to compute the power an attacker would need based on distance and system parameters.
- Without such analysis, defenses cannot be reliably designed against close-range spoofing.

Proposed Solution - Link Budget Model

- Calculate Free Space Path Loss (FSPL) to evaluate signal degradation

$$Lfs = 20log10(dkm) + 20log10(fghz) + 92.45$$

  - d: distance in kilometers
  - f: frequency in GHz ($GPSL1 = 1.57542GHz$)
- Use the link budget equation:

$$Pr = Pt + Gt + Gr - Lfs - Lm$$

- Compare satellite-received signal to spoofer signal to compute required attacker power.
- Add margin (10–15 dB) to ensure spoofed signal dominates.
- Include gain/loss factors: antenna gains (G_t, G_r), path losses, and miscellaneous losses (L_m).

Results - Power Analysis and C/N0

- Legitimate satellite signal ≈ -130 dBW
- Spoofing from 100 m requires only a few watts of transmit power.
- Spoofing from 5 km needs ≈ 34.8 dBW (~3.2 kW)
- Computed Carrier-to-Noise Ratio (C/N0) confirms signal lock would switch to spoofed signal.
- Results highlight that power-efficient spoofers are a realistic threat.

```
--- 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
```

Spoofing Simulation and Visualization of Spoofing Attack

Attack Outcome

The host's path deviates from the true trajectory, following the spoofed data. The spoofed trajectory appears valid internally, demonstrating spoofing's subtlety and effectiveness.

Visualization

Dynamic plots illustrate the host's true path, attacker's position, and spoofed path, highlighting the divergence caused by the spoofing event.

Problem Statement - Host Redirection via Spoofing

- A moving host, such as a delivery drone or autonomous vehicle, follows GPS coordinates to reach its destination.
- An attacker with a portable transmitter can spoof GPS signals and redirect the host without physical contact.
- This attack has serious consequences in defense, commercial delivery, and civilian safety.

Proposed Solution - Host and Attacker Simulation

- Host modeled to move linearly toward a fixed target at 1 unit/s.
- Spoofer is positioned statically near the target with a spoofing radius of 25 units.
- When host enters spoofing range, spoofed position is offset from true position by [+10,-10] .
- Spoofing event is tracked and host's path diverges accordingly.
- Simulation updated at each timestep (dt = 1), checking spoofing status and updating path.

Results - Deviation of Trajectory

- After spoofing begins, host starts to deviate from its true path.
- Its GPS reports false coordinates, and navigation continues based on this misinformation.
- A clear divergence is seen in the plotted paths—actual vs perceived.
- Host ultimately fails to reach the real destination

Google Docs

Screencast from 2025-05-23 15-05-24 (online-video-cutter.com).mp4

Analysis and Observations

- Continuous spoofing leads to sustained misdirection.
- Receiver remains unaware due to constant, plausible signal updates.
- Demonstrates feasibility of non-invasive hijacking of autonomous systems.
- Simulation confirms that GPS-only navigation is vulnerable to localized spoofing.

Challenges and Motivation for Spoofing Detection

Challenges in Spoofing

Accurate timing alignment and synchronization are difficult. Anomalies in Doppler shift or clock drift risk detection. Receiver countermeasures include inertial sensors and timestamp cross-checks.

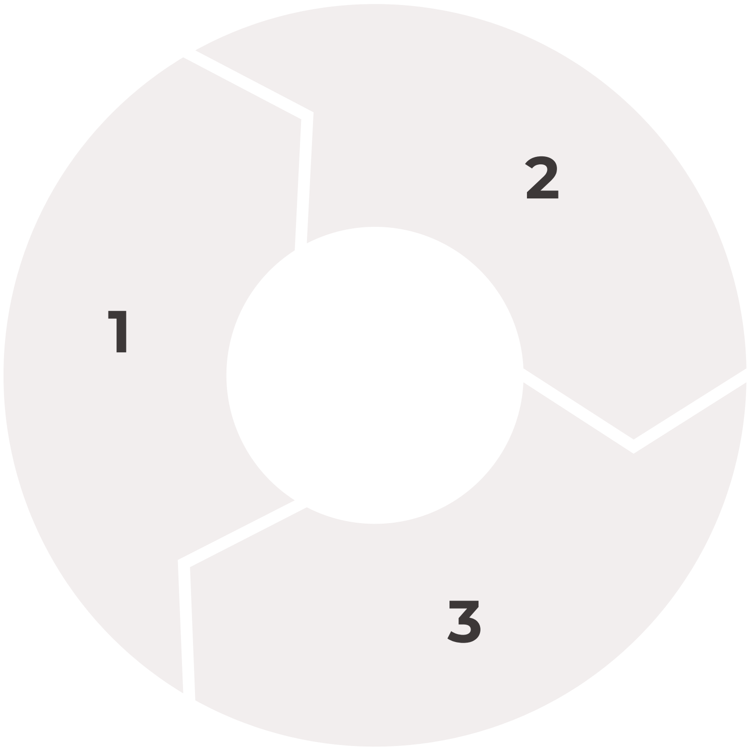
Detection Motivation

Real-world spoofing incidents cause navigation errors in vehicles and ships. Intelligent, autonomous detection systems are essential to counter growing threats.

Machine Learning Based Spoofing Detection

Anomaly Detection Approach

Simulates spoofing by injecting sudden location jumps. A supervised ML model classifies normal vs. spoofed patterns using GPS data without hardware changes.



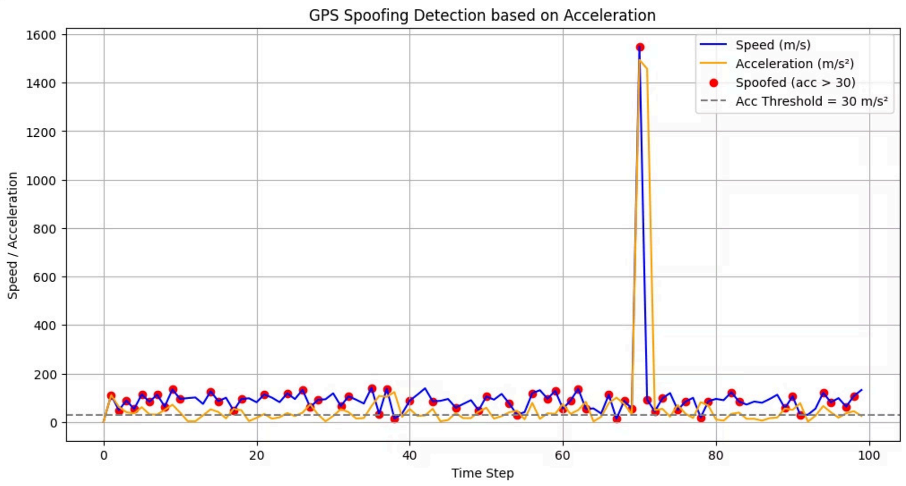
Feature Engineering

Uses latitude, longitude, speed, and displacement. Distance jumps between consecutive points serve as primary features for anomaly classification.

Implementation & Results

Geopy calculates distances; threshold-based labeling flags spoofed points. The model accurately detects anomalies, enabling real-time spoof detection with low complexity.

Anomaly Detection Visualization



The plot shows a spoofing point detected due to a sudden acceleration spike over 30 m/s^2. The model accurately flagged it as spoofed, showing effective real-time detection.

- Generate synthetic GPS trace simulating a moving object.
- Introduce spoofing at a specific point by adding large offset in lat/lon.
- Extract spatial features such as displacement between consecutive GPS points.
- Use threshold-based classification to flag abnormal jumps.

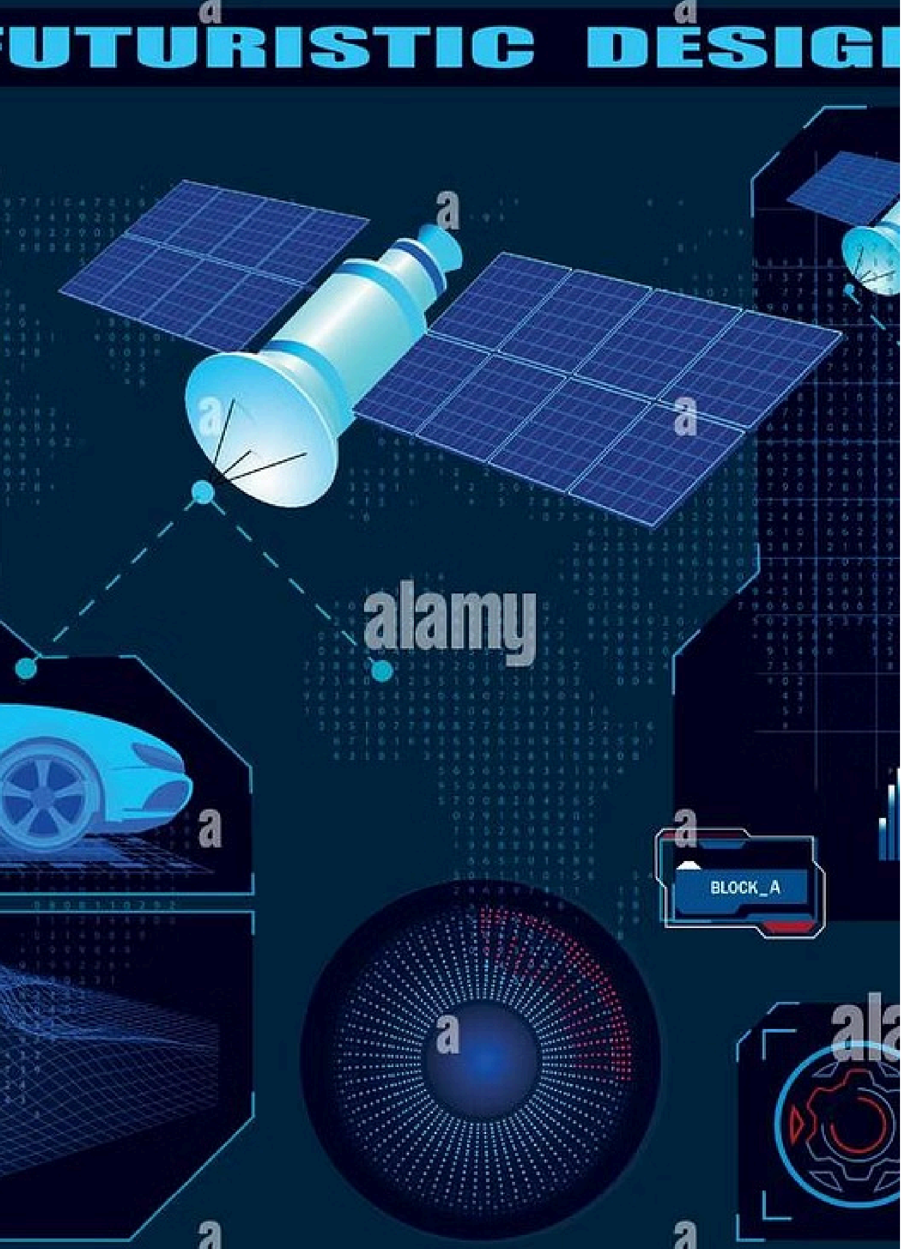
```
Confusion Matrix:
[[40 59]
 [ 0  1]]

Classification Report:
              precision    recall  f1-score   support

      Normal       1.00      0.40      0.58        99
     Spoofed       0.02      1.00      0.03         1

    accuracy                           0.41       100
   macro avg       0.51      0.70      0.30       100
weighted avg       0.99      0.41      0.57       100
```

Evaluation Metrics and Confusion Matrix

📉 Confusion Matrix Results

	Predicted Spoofed	Predicted Normal
Actual Spoofed	TP = 40	FN = 59
Actual Normal	FP = 0	TN = 1

- **Accuracy**: 45.05%
- **Precision**: 100%
- **Recall (Detection Rate)**: 44.4%
- **F1-Score**: 61.55%



Summary, Limitations, and Future Work

Summary

Developed an end-to-end GPS spoofing framework with simulation, link budget analysis, practical spoofing, and ML-based detection using Python.

Limitations

Focused on single host and attacker under ideal conditions. Detection model is basic and requires validation with real-world noisy data.

Future Work

Extend simulations with 3D terrain, multipath, jamming, and dynamic spoofing. Develop multi-modal detection combining GPS with accelerometer and magnetometer data.