Report on GPS Spoofing and Communication Anomalies Affecting Indian Aviation Operations

Date: 12 November 2025

Executive Summary

In early November 2025, multiple Indian airlines and Air Traffic Control (ATC) units reported **anomalies and disruptions** in communication and navigation systems, primarily in the **northern and western regions of India**. These disturbances led to **flight delays, cancellations, and route diversions**, significantly impacting operational efficiency and passenger safety.

Preliminary assessments indicated two concurrent factors:

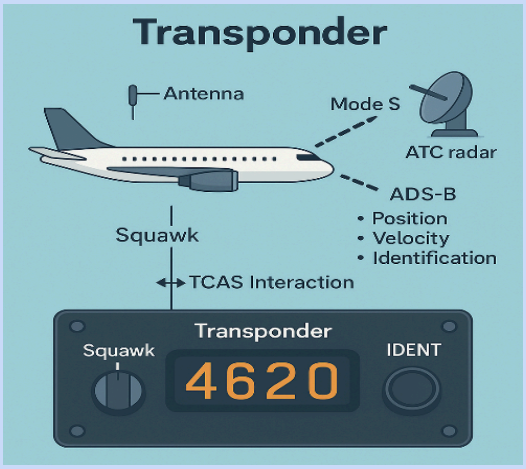
> **A technical malfunction** in the **Automatic Message Switching System (AMSS)**, and
>
> **Possible GPS spoofing activity**, particularly along sensitive flight corridors near India's northern borders.

This report analyses the nature of GPS spoofing and jamming, summarizes the reported incidents, identifies high-risk corridors, and recommends immediate and long-term measures to mitigate these threats.

1. Introduction

Air traffic operations rely on a network of sophisticated communication, navigation, and surveillance systems to ensure safe and efficient flight management. Any compromise in these systems — whether through technical faults or deliberate interference — poses a significant risk to aviation safety.

In the past months, Indian aviation authorities have faced repeated disruptions attributed to **malicious communication interference** and **GPS signal anomalies**. This report seeks to explain technical aspects of these events and evaluate their root causes.



2. Understanding Spoofing

2.1 Definition

Spoofing refers to the act of **interfering with or falsifying communication signals between two electronic devices**. By impersonating a legitimate source, an attacker can intercept or manipulate information transmitted between devices.

2.2 Example of Communication Spoofing

Consider two individuals, *A* and *B*, communicating via mobile phones. An attacker can create a **fake cell tower** that intercepts *A's* communication, allowing the intruder to **listen, record, or send fake messages** to *B* while pretending to be *A*. This deception can lead to misinformation, miscommunication, or security breaches.

3. Overview of GPS Jamming

3.1 Definition

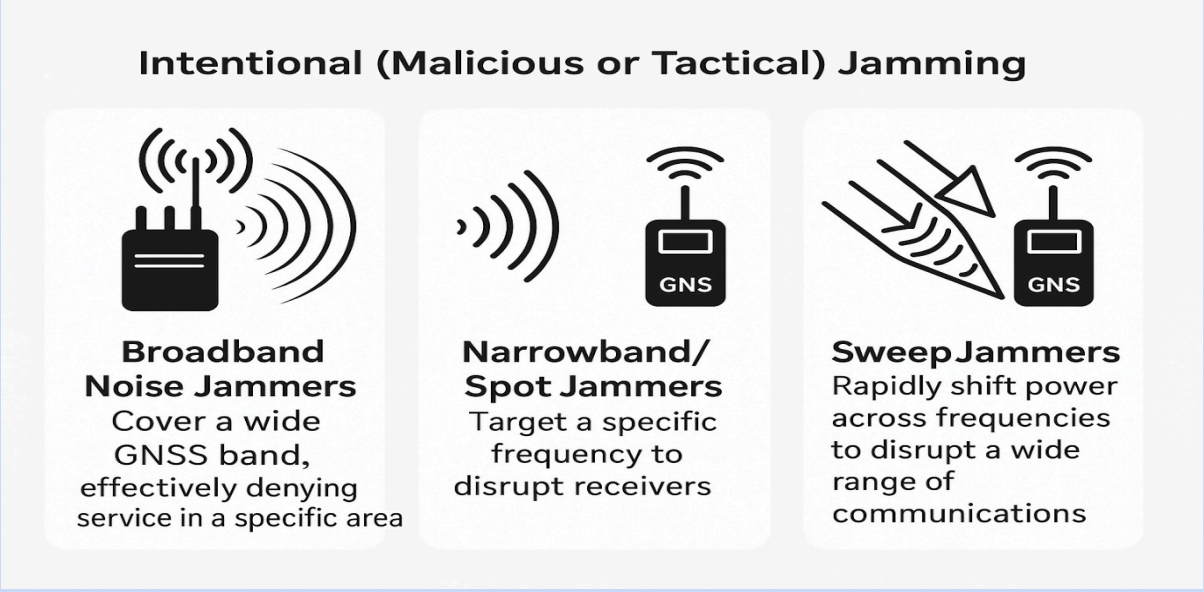
GPS jamming occurs when a transmitter emits radio signals that **overwhelm the GPS receiver's ability to detect legitimate satellite signals**. Because GPS signals are inherently weak and unencrypted, they are particularly vulnerable to jamming.

3.2 Types of Jamming

a. **Unintentional Jamming:**

Caused by overlapping wireless frequencies or misconfigured equipment.

b. Intentional or Tactical Jamming:



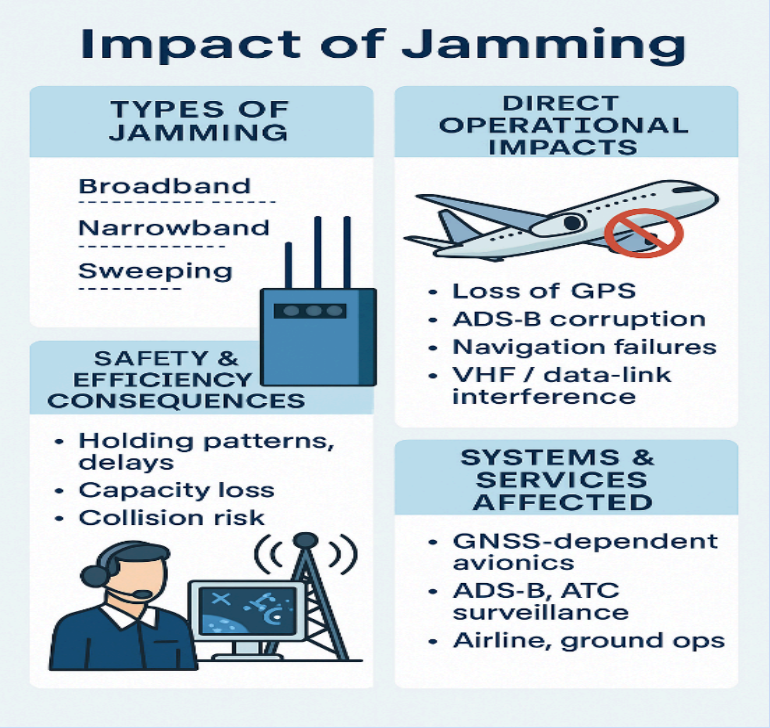
Broadband Noise Jammers: Block a wide GNSS band, effectively denying service over an area.

Narrowband/Spot Jammers: Target a single frequency used by GPS receivers.

Sweep Jammers: Rapidly shift transmission power across multiple frequencies to disrupt communication channels.

3.3 Impact of Jamming

Jamming interferes with essential services, including:

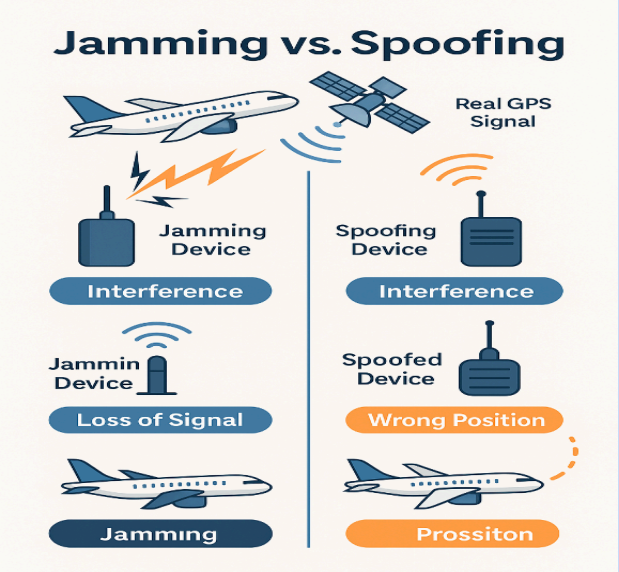


Emergency communication lines (Police – 100, Ambulance – 108, Fire & Rescue – 101)

Defense and law enforcement communication networks

Aviation navigation and ATC coordination systems

4. Jamming vs. Spoofing



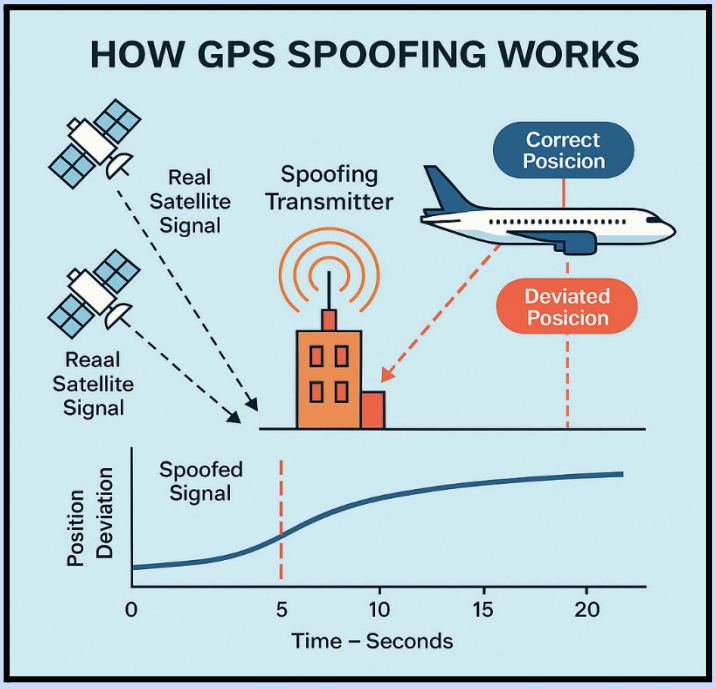
Aspect	Jamming	Spoofing
Nature	Disrupts or blocks communication signals	Deceives systems by sending false signals
Effect	Denies or degrades service	Misleads receivers into believing false data
Detection	Often detectable through loss of signal	Harder to detect as systems appear functional
Severity	Temporary disruption	Potentially catastrophic navigation errors

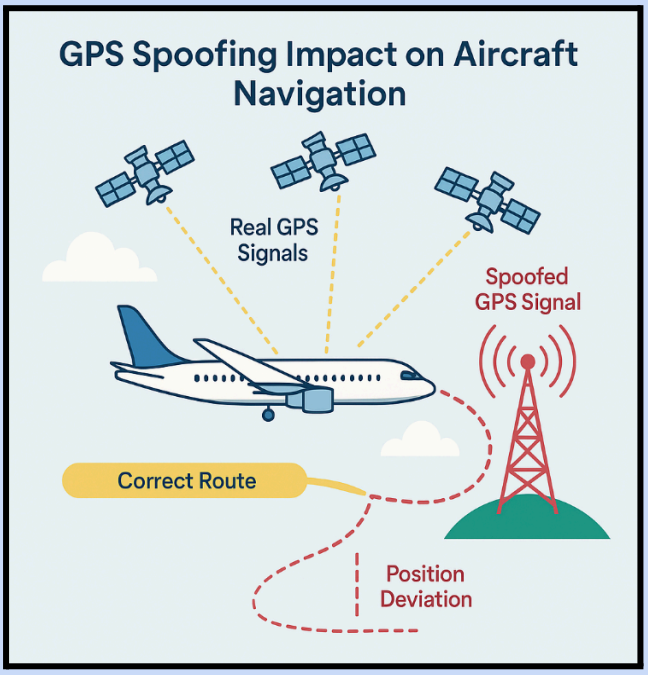
5. Mechanism of GPS Spoofing

5.1 How GPS Spoofing Works

GPS receivers in aircraft rely on satellite signals to determine **Position, Navigation, and Timing (PNT)** data.

During a spoofing attack, a **fake transmitter** broadcasts counterfeit satellite signals, deceiving the receiver into **accepting false coordinates or time data**.





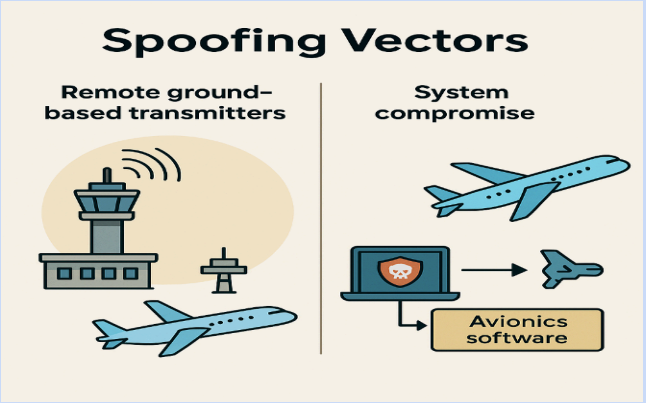
This results in:

Incorrect flight path calculations

Erroneous altitude or position data

Potential disruption of onboard avionics timing systems

5.2 Methods of Execution:



.

Ground-Based Spoofing: Using high-powered transmitters near airports or flight paths.·

System Compromise: Exploiting hardware or software vulnerabilities to inject malicious code or malware.

5.3 Capability and Source

GPS spoofing requires **high-grade, military-level equipment** and **technical expertise**. Such activities are **beyond the capacity of individuals or private organizations** and are generally attributed to **state-sponsored entities**.

In November 2025, **Ukraine reported destroying a special forces reconnaissance unit** in the **Black Sea**, suspected of using equipment for GPS interference — underscoring the global nature of this threat.

Image of Ukrainian forces destroying the unused oil rig used for GPS Spoofing

6. Incident Summary: India, November 2025

6.1 ATC System Malfunction

The **Airports Authority of India (AAI)** reported that the **Automatic Message Switching System (AMSS)** failed on **6 November 2025**, with the issue persisting into **7 November 2025**.
This halted automated routing and flight-plan data transmission, forcing air traffic controllers to **switch to manual operations**, leading to **widespread delays and cancellations** across northern and western India.

According to DGCA report around 465 incidents of GPS interference/spoofing in border regions (mainly Amritsar and Jammu) between November 2023 and February 2025 reported

6.2 GPS Spoofing Indicators

Media and aviation data monitoring sources detected **abnormal ADS-B readings**, with aircraft positions **fluctuating by up to 335 km within seconds**.
The **Navigation Integrity Category (NIC)** value dropped from **8 (normal)** to **0 (unreliable)**, confirming **GPS data manipulation**.

These incidents led to:

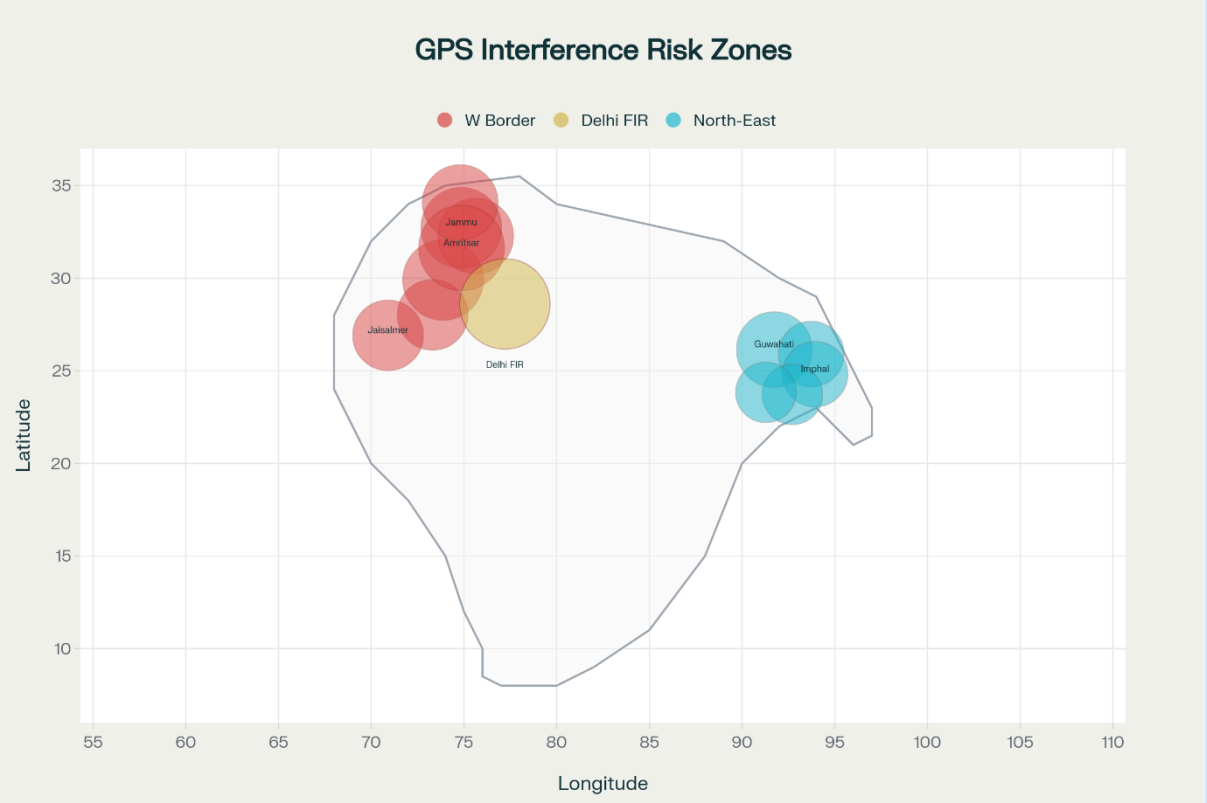
- Misreported aircraft positions on ATC radar
- Loss of navigation accuracy
- Flight diversions and premature returns to origin airports

7. High-Risk Corridors for GPS Interference

Amritsar and Jammu:
Frequent reports of GPS interference and spoofing within the Amritsar and Jammu FIRs.

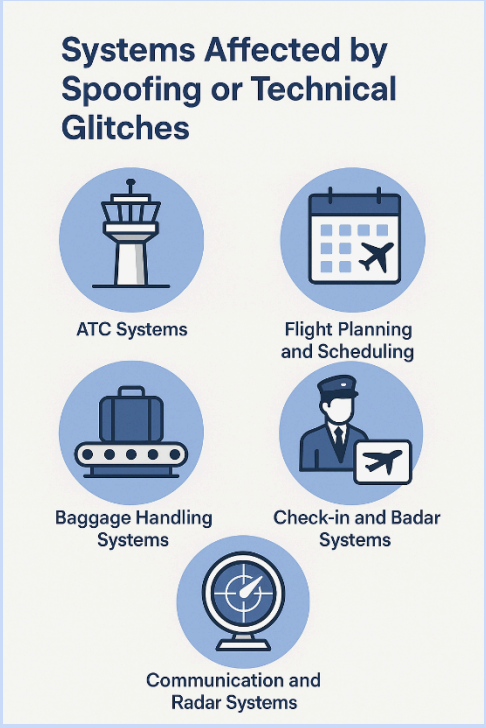
Delhi:
Severe spoofing incidents within a **60-nautical-mile radius**, lasting several consecutive days.

Border Regions:
Air routes near **India–Pakistan borders** and the **North-Eastern region** are particularly vulnerable due to proximity to foreign electronic warfare infrastructure.



As of **7 November 2025**, airlines reported **"severe GPS spoofing"** over Delhi lasting **seven days**, prompting DGCA investigation.

8. Systems Potentially Affected



Air Traffic Control Systems: Manage aircraft movement on runways and in airspace.

Flight Planning and Scheduling Systems: Handle slot allocation, crew management, and routing.

Baggage Handling Systems: Depend on automated scanners and conveyors.

Check-In and Boarding Systems: Linked to reservation databases and boarding pass readers.

Communication and Radar Systems: Facilitate real-time coordination between ground and airborne systems.

Disruptions to any of these interdependent networks can significantly hinder aviation operations.

9. Findings

Technical Cause:
Temporary failure of the AMSS caused operational delays but did not directly compromise flight safety.

Security Concern:
Persistent GPS spoofing patterns indicate possible **external interference** in sensitive northern flight corridors.

Operational Impact:
Manual processing of flight plans and communication errors resulted in **cancellations, diversions, and airspace congestion**.

10. Recommendations

10.1 Immediate Actions

Implement **real-time GPS anomaly detection systems** at all major ATC centers.

Issue **operational advisories** to airlines operating in high-risk corridors.

Strengthen **cybersecurity audits** of all ATC and airline systems.

Establish a **24/7 Joint Aviation Cyber Monitoring Cell** involving DGCA, AAI, and defense agencies.

10.2 Medium- to Long-Term Measures

Develop **GPS signal authentication systems** (e.g., encrypted GNSS services).

Enhance **redundant navigation systems** using inertial and terrestrial references.

Collaborate with **international aviation and defense partners** to track and trace spoofing sources.

Conduct **training and simulation programs** for ATC personnel to handle spoofing/jamming scenarios.

11. Conclusion

The incidents reported across Indian airspace in November 2025 underscore the **dual challenge of technical reliability and electronic security** in modern aviation. While system malfunctions can disrupt operations, **GPS spoofing presents a more complex and potentially hostile threat** that requires national-level coordination and technological resilience.

Maintaining the integrity of India's air navigation systems demands **continuous vigilance, inter-agency cooperation, and investment in advanced detection technologies** to safeguard both domestic and international aviation operations.

Prepared by:

Riyaz
Former Police Officer, Cyber Investigator and researcher, based in Hyderabad
Freelancer
Email-riyaz.cyb@gmail.com

Date: 12th of November 2025