GPS Interference

Posted at: 11/07/2025

GPS Interference: A Growing Threat to Global Navigation and Security

---

Context

In recent years, **GPS interference** has emerged as a growing threat to **global navigation systems**, especially affecting **aircraft** and **seafaring vessels**. With increasing reliance on GPS for both **civilian and military operations**, any disruption poses significant **safety, security, and geopolitical risks**. The issue has gained critical relevance amidst **ongoing conflicts**, **cyber warfare**, and rising **technological vulnerabilities**.

What is GPS and GPS Interference?

- The **Global Positioning System (GPS)** is a **space-based radio navigation system**, owned by the **U.S. Government** and operated by the **United States Air Force (USAF)**.
- It provides:
  - **3D positioning with meter-level accuracy**.
  - **Time accuracy to the 10-nanosecond level**.
  - **24/7 global coverage** for navigation and timing.

GPS Interference refers to deliberate or accidental disruption of GPS signals, primarily through:

- **Jamming** – Blocking or overpowering the original signals.
- **Spoofing** – Sending fake signals to mislead GPS receivers.

Types of GPS Interference

1. GPS Jamming

- Uses a **jammer device** that emits **strong radio signals** at GPS frequencies.
- Prevents GPS receivers from detecting authentic signals.
- **Effect**: Completely disables GPS-based location and timing.

2. GPS Spoofing

- Sends **false signals** on the same frequency as GPS satellites.
- Tricks receivers into interpreting **incorrect positional or timing data**.
- **Effect**: Misguides vehicles by feeding them false locations instead of cutting signals.

> *While both are cyber threats, spoofing manipulates the system; jamming simply disables it.*

Causes of GPS Interference

- **Electromagnetic radiation** from nearby electronics.
- **Atmospheric disruptions**: ionospheric disturbances, **solar flares**.
- **Deliberate attacks** using jamming/spoofing devices.
- **Cyber warfare** and **espionage** in conflict-prone zones.

Why is GPS Interference Dangerous?

Military Operations at Risk

- Spoofing can mislead **fighter jets or drones**, increasing chances of **collisions or navigation errors**.
- In **2024**, around **700 GPS spoofing incidents** were reported **daily worldwide**, highlighting the growing scale.

Civilian Transport Disruptions

- Navigation failures may lead to:
    - **Airplane accidents**
    - **Maritime groundings**
    - **Traffic mismanagement**

Maritime Navigation Threats

- Spoofing can cause **sudden course deviation**, aiding **piracy** or **collision**.
- **Persian Gulf** and **Red Sea** are vulnerable areas.
- As per **Windward (Q1 2025)** data:
    - **350% increase** in spoofing incidents in the **Red Sea** compared to 2024.
    - Some ships reported **location jumps of hundreds of nautical miles**.

Geopolitical Tensions

- Accusations of GPS sabotage may escalate into:
    - **Diplomatic standoffs**
    - **Cyber retaliation**

- **Military conflicts**

Airspace Avoidance Measures

- Aircraft avoid regions with spoofing threats.
- Example: **Restricted airspace during the Russia–Ukraine war** to prevent GPS-related mishaps.

Overdependence on GPS

- Reliance makes systems vulnerable during denial of access.
- India faced this during:
  - **1999 Kargil War**
  - **2009 and 2012 BrahMos missile tests – U.S. denied GPS access**.

False Data Risks

- May lead to:
  - **Aircraft collisions**
  - **Civilian ship accidents**
  - **Unintended territorial entry**

How Can GPS Interference Be Prevented?

1. Use of Alternative Navigation Systems

- **Inertial Navigation System (INS)**:
  - Uses **gyroscopes and accelerometers** to calculate position without external signals.

- **VHF Omnidirectional Range (VOR)** and **Distance Measuring Equipment (DME)**:
    - Provide **ground-based navigation** support.
- **Instrument Landing System (ILS)**:
    - Helps in **precision landing**, unaffected by spoofing.

2. Enhanced Pilot and Crew Training

- Encourage vigilance and communication with **air traffic control**.
- Detect suspicious GPS behaviour and switch to **manual navigation**.

3. Advanced Alert Systems

- Automated systems to **detect spoofing/jamming**.
- Immediate switching from **auto-pilot to manual mode** if needed.

4. Terrestrial Navigation Methods

- Involve manual checks using:
    - **Lighthouses**
    - **Radar systems**
    - **Visual or coastal navigation aids**

What Lies Ahead?

- **Diversifying navigation systems** is essential to reduce overreliance on GPS.
- Adoption of **multi-constellation GNSS** systems like:

    - **GLONASS (Russia)**
    - **Galileo (EU)**
    - **BeiDou (China)**

- These offer **redundancy and resilience** against interference and improve **strategic autonomy**.