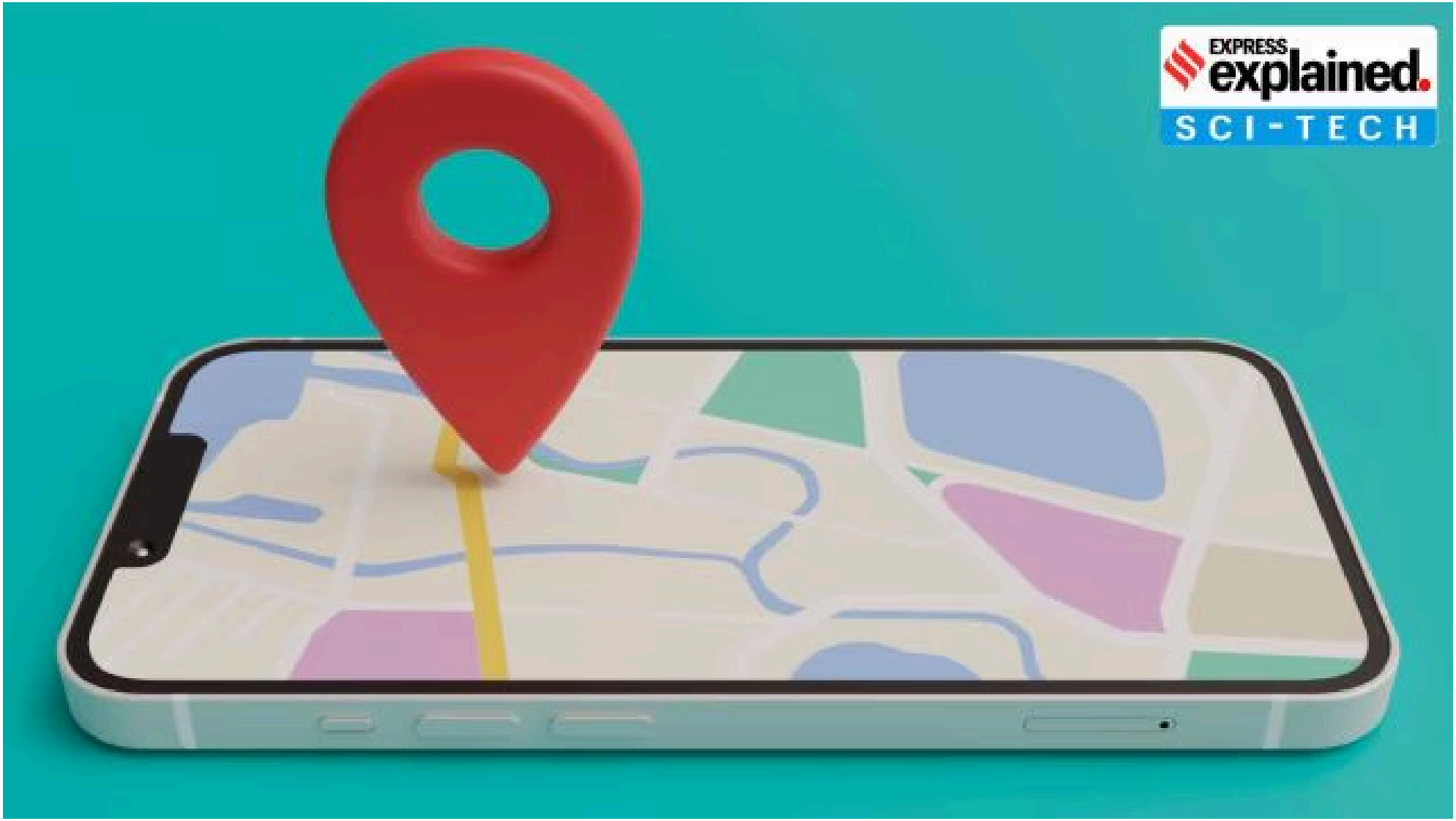
The Indian EXPRESS
JOURNALISM OF COURAGE

GPS interference threatening flights, ships: What is happening, possible solutions

Incidents of spoofing or jamming can potentially cause havoc and disrupt maritime, air, and even road traffic

Written by Sunanda Mehta
Pune | Updated: June 29, 2025 22:01 IST

6 min read



GPS interference can disrupt both military and civilian transport operations from afar, without physical confrontation. (Credit: Freepik)

A **Delhi-Jammu flight was forced to turn back** last week. Two tankers collided at the entrance of the Strait of Hormuz earlier this month. A container ship ran aground near the port of Jeddah in May.

All three mishaps had a common cause: GPS interference which, in recent years, has emerged as one of the biggest challenges for seafaring vessels and aircraft.

What is GPS interference?

GPS interference refers to spoofing or jamming, two types of deliberate cyber-attacks on Global Positioning System (GPS) signals, which disrupt or deceive vehicles' navigation systems. While both are often used synonymously with each other, spoofing and jamming refer to slightly different kinds of interference.

Also Read | Air India Express flight to Jammu returns to Delhi due to 'GPS interference'

GPS jamming, also known as GPS intervention, involves a device (jammer) emitting strong radio signals on GPS frequencies in order to overpower weaker signals. This disrupts the functioning of GPS systems by rendering receivers unable to determine location or time.

GPS spoofing involves a device transmitting signals on the same frequencies used by GPS satellites, overwhelming or blocking the GPS receivers from acquiring or maintaining the right satellite signals. Unlike jamming, which disrupts signals entirely, spoofing deceives the receiver into trusting false data.

Why is GPS interference dangerous?

GPS interference can disrupt both military and civilian transport operations from afar, without physical confrontation.

"The risks are real and alarming. Spoofing can cause a pilot to misjudge the aircraft's position, increasing the chance of collisions with terrain or other aircraft," Air Marshal Bhushan Gokhale (retd), former vice-chief **of Air Staff**, told *The Indian Express*. "For ships, the consequences of loss of situational awareness include groundings or collisions, disrupting entire maritime operations," he said.

Also Read | North Korean GPS manipulation disrupted dozens of planes and vessels, says South Korea

In 2024, reports indicated up to 700 daily GPS spoofing incidents globally, highlighting the scale of the threat. For critical infrastructure, such as air traffic control, port operations, and VTS-vessel traffic systems, spoofing can cascade into broader systemic failures.

"GPS interference is not limited to air and water… With our increasing reliance on GPS navigation on roads, spoofing can cause havoc by triggering traffic jams and immobilising transport systems, especially in critical times as desired by an adversary or anyone with rogue intentions," Air Marshal Gokhale added.

Where are such incidents common?

GPS interference can occur due to various reasons, not all of them malicious. These include electromagnetic radiation from nearby devices, adverse atmospheric conditions like ionospheric disturbances, solar activity (such as flares), and, of course, intentional jamming/spoofing.

Most often, countries with advanced electronic warfare capabilities and involved in an active conflict are responsible. While interference may or may not be targeted at civilian vessels, those in the vicinity, relying on the same GPS infrastructure, are nonetheless susceptible.

For instance, GPS interference has disrupted maritime navigation in the Persian Gulf and the Red sea amid ongoing conflicts throughout the region. Maritime tech consultancy Windward's Q1 2025 data show a 350% rise in spoofing incidents in the Red Sea alone compared to 2024–**with** some vessels **having** experienced sudden position jumps of hundreds of **nautical miles.**

Such incidents have also been witnessed in Eastern Europe, amid the ongoing war between Russia and Ukraine.

For aircraft, spoofing is one of the primary risks of being in the airspace of countries in war. “This is one of the reasons for that air space being avoided by all aircraft during war. We immediately avoid these areas as a preventive measure,” said a former in-charge of safety with an airline.

Russia was the first to experience a large-scale GPS spoofing attack in 2017, according to Captain Sachin Mundhra, **COO Adani Karaikal Port,** master mariner. “In June 2017, more than 20 ships near Novorossiysk Port, Russia, reported sudden GPS errors — their navigation systems showed them miles inland at an airport. Investigation findings showed the ships’ AIS (Automatic Identification System) displayed identical false positions. The analysis suggested a deliberate GPS spoofing attack,” he said.

How do ships/aircraft mitigate risks of GPS interference and deal with the issue once detected?

Aircraft experiencing GPS spoofing mid-air have to rely on alternative navigation systems.

Inertial Navigation Systems (INS) are the primary backup: these use gyroscopes and accelerometers to track the aircraft’s current position based on its last known location. VHF Omnidirectional Range (VOR) and Distance Measuring Equipment (DME) provide ground-based radio navigation, allowing pilots to further cross-check their position.

Pilots can also use celestial navigation or dead reckoning (the process of calculating one’s position by estimating the direction and distance travelled) in extreme cases, though these are less common in modern aviation. The Instrument Landing Systems (ILS), critical for precision approaches during landing, are unaffected by GPS spoofing.

Directorate General of Civil Aviation (DGCA) has emphasised enhanced crew training. “Pilots are also encouraged to listen carefully to the control room to pick up any chatter of suspected GPS spoofing and become immediately cautious of the possibility,” **a** former flight-safety official said.

Modern ships typically run on auto-pilot: a course is assigned after which a GPS-based system autonomously determines control inputs to stay in course. During suspected spoofing, the ship’s crew resorts to manual helm control-steering, with terrestrial

navigation, which involves manual position fixing using land-based aids like lighthouses and radars, the immediate alternative to maintain situational awareness.

Moreover, shipping companies are adopting multi-constellation Global Navigation Satellite System (GNSS) systems to mitigate against GPS interference. These use navigation systems of multiple countries to counter the digital threat — the United States' GPS, Russia's GLONASS, the European Union's Galileo, and China's Bei Dou, among others.

Diversification is probably at the core of mitigating the risks of GPS interference.

The Indian military has deployed the indigenous Navigation with Indian Constellation (NavIC), developed by the Indian Space Research Organisation (ISRO). NavIC is designed to provide precise positioning and timing services across India, and up to 1,500 km beyond its borders.

"During the 1999 Kargil war, India's request for the use of American GPS for information about positioning, timing & navigation of hostile forces was denied. Likewise, in 2009 and 2012, India's Brahmos missile failed to hit targets in trial operations as the US shut off GPS satellites without any warning. Such unsavoury incidents necessitated the need for NavIC. Its resilience and reliability were ably tested during Operation Sindhoor," Air Marshal Gokhale said.

This article went live on June twenty-ninth, twenty twenty-five, at forty-five minutes past six in the morning.

TAGS: GPS