GPS JAMMING, SPOOFING

Rarely do we have days without notice of deliberate GPS interference somewhere in the U.S., usually from the military. But that's only one source of GPS errors.

Modern WAAS GPS provides ILS-like precision position and guidance, which can be affected by natural ionospheric disturbances and unintentional or intentional jamming. Spoofing by altering the apparent WAAS GPS position is also a growing problem, particularly in Eastern Europe. It's time we explored these GPS errors.

WAAS/GPS Fundamentals

The GPS satellites transmit their orbital data in a long extended-data stream. The time of arrival of the low-amplitude data stream from the satellite is critical in determining the aircraft's position. The GPS satellites, owned by the Department of Defense, are not geostationary—they rotate around the Earth in low orbits. "WAAS satellites" are in geostationary orbits much higher than the GPS satellites.

The term, "WAAS satellites," is actually a misnomer as the FAA leases three commercial satellites for receiving and rebroadcasting the GPS error corrections that were calculated on the ground. These are "bent pipe" transmissions, where the satellite merely retransmits the signal from the ground. WAAS is a satellite-based augmentation system using augmentation data initiated on the ground, as opposed to a ground-based transmitter system.

Fundamental concepts for a satellite-based augmentation system were wide area of coverage and ease of installation. If a user had an antenna and receiver to detect the GPS satellite transmissions, it would be "easy" to add a channel to receive the corrections from another satellite. The WAAS/GPS receiver augments the GPS position it receives from the GPS satellites with the corrections from the WAAS satellite.

The ground-based augmentation systems (GBAS) broadcast the corrections to a receiver in the aircraft, and the augmentation of the GPS position is done in the flight management or navigation computer. Several years ago, there were two ground-based augmentation systems in service in the U.S., one at Houston and one at Newark to provide GPS-based Cat III capability. Due to several factors, GBAS has lost favor within the FAA.

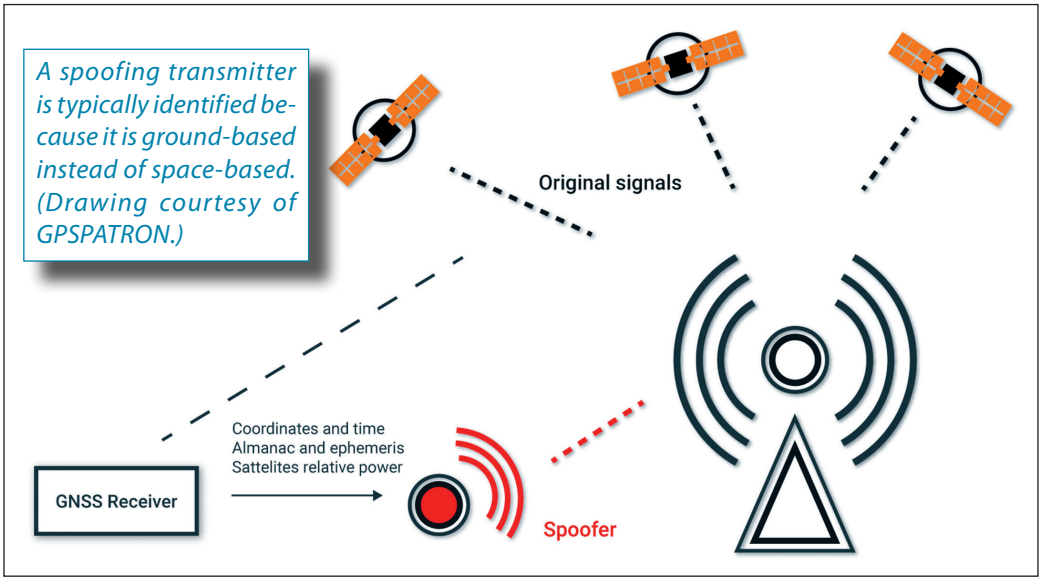
Natural Phenomena

Solar events and magnetic storms can cause errors in the calculated position and in worst-case situations, loss of GPS positioning. The sunspot cycle occurs in an 11-year period. We are currently in a peak of high activity. The FAA Technical Center issues a quarterly report, "Wide Area Augmentation System Performance." The latest report (#87 January 2024) had 15 pages of electromagnetic events that caused moderate to significant degradation of LPV and LPV 200 service.

GPS Jamming

A common reason for losing GPS position is unintentional or intentional jamming. There was a famous case of a truck parked at Newark Airport for several hours where the driver had left an illegal jammer on while the truck was parked. The intent was not to jam the GPS receivers at the airport but to prevent the truck's logging and mapping system from reporting where the truck was located. The driver was fined almost $32,000 for the incident.

Since Interstate 95 runs parallel to Runway 4R/22L at EWR, there are also brief outages due to long-haul truckers inadvertently jamming the GPS signals at the airport. The GPS transmitter power is only 50 to 60 watts, and due to the long distance between the receiver and the satellite, it is easy to overpower the weak signal arriving at the GPS receiver. The jammer overloads the GPS receiver's front end and blocks the genuine signal. U.S. military exercises will often involve GPS jamming.



A spoofing transmitter is typically identified because it is ground-based instead of space-based. (Drawing courtesy of GPSPATRON.)

GPS Spoofing

GPS Spoofing is much more insidious and alarming. Spoofing alters the GPS signal to make the receiver believe it is in

a different location than its actual position. Spoofing attacks can range from very sophisticated, where the message content is altered, to simply delaying the arrival time. Spoofing can be done through the WAAS or GPS channel. GPS satellite spoofing attacks are often detected by a jump in the time reported from the GPS.

Even if you checked the NOTAMS and RAIM predictions it's good to keep an eye on the GPS Status page if you detect any anomaly. There are techniques to determine if a GPS signal is spoofed, such as whether the signal is arriving from space or a ground source. Fortunately, in the U.S. we rarely have issues with GPS spoofing, but in the Eastern Mediterranean region, the European Union Aviation Safety Agency (EASA) and the International Air Transport Association (IATA) have declared jamming and spoofing to be a "significant challenge" to aviation safety.

Besides EASA, the FAA is concerned about spoofing. TSO-C146e for Stand-Alone Airborne Navigation Equipment Using the Global Positioning System Augmented by the Satellite Based Augmentation System devoted two pages to Cybersecurity and Spoofing Mitigation. More recently, on January 25, 2024, the FAA issued a Safety Alert for Operators (SAFO) that stated: "Recent GPS/GNSS jamming and spoofing activities reported by civil air operators operating globally pose a potential safety of flight risk to civil aviation.

"GPS/GNSS disruptions often occur in and around conflict zones, military operations areas, and areas of counter unmanned aircraft systems (UAS) protection. The term GNSS includes satellite augmentation systems. The recent jamming and spoofing incidents may pose increased safety of flight risks due to possible loss of situational awareness and increased pilot and regional Air Traffic Control (ATC) workload issues.

"With increasing frequency of GPS/GNSS disruptions, the Federal Aviation Administration (FAA) recommends flight crews put additional emphasis on closely monitoring aircraft equipment performance for any discrepancies or anomalies, promptly informing ATC of any apparent GPS/GNSS degradation and being prepared to operate without GPS/GNSS navigation systems."

RIGHT: The GPS Status page should be used to look for signal anomalies. Many pilots first notice a jump in the GPS time when spoofed. (Avidyne image)

GPS Checks

While not required if your aircraft is equipped with a WAAS-capable GPS receiver, a preflight check of RAIM or SAPT prediction for the flight is always a good idea. Besides checking the prediction, you should review the NOTAMS for military exercises affecting the GPS.

If losing GPS was confined to losing navigational information in flight, it would be inconvenient but not necessarily hazardous. Today, however, many systems are so integrated that you will typically lose the moving map, terrain overlay, fuel remaining at the destination, the frequencies of ATC facilities in the local area, and numerous other pieces of information, even potentially including attitude and other flight-critical data.

Airline equipment has a robust attitude and heading reference system (AHRS) or inertial reference units (IRU) that do not require external aiding to calculate attitude and heading. In general aviation aircraft, the solid-state MEMS gyros and accelerometers require "aiding" from air-data and/or GPS to generate a correct attitude and heading. In case of a GPS outage, having connected the GPS and an air data computer to the AHRS for aiding is better than connecting two GPS units. Refer to "Avionics Systems Issues" in the March 2023 issue of *IFR* Magazine. You should also note if your standby attitude and heading unit uses MEMS gyros/accelerators aided by GPS.

While losing GPS due to jamming is a problem, having the apparent position of the aircraft moved (spoofed) to a different location creates a much more bewildering mental problem. The information isn't missing; it is just very misleading. Sorting out what is correct and what is incorrect requires a thorough knowledge of the system.

If you have problems with jamming or spoofing, ask ATC for help. Remember all ATC facilities guard 121.5 MHz, so if you can't raise anyone, try that frequency. The controller can give you vectors for navigation (hopefully, you are in visual conditions), but if the jamming area affects other aircraft, the controller will be very busy. Last, if a U.S. government agency is the source of the jamming/spoofing, the ATC facility can issue a "stop buzzer" order to stop the jamming exercise. Remember that term, but don't request "stop buzzer" unless it is a true emergency rather than an inconvenience.

Additional information on jamming and spoofing can be found at:

- Mentour Pilot YouTube channel: "The END of GPS for Aviation?! Spoofing At Work." The video is well worth watching.
- Tracking of GPS interference areas worldwide can be found at: https://gpsjam.org/
- GPS Service Outages & Status Reports: https://www.gps.gov/support/user/
- OPS Group GPS Spoofing Update: Map, Scenarios and Guidance https://ops.group/blog/gps-spoofing-update-08nov2023/ | IFR

Bob Teter attended GPS design seminars in Washington, DC, before the first satellite was in orbit. However, the most interesting information was on military satellite systems used for positioning prior to GPS.