ChatGPT

Indicators of GPS Denial or Jamming

General Indicators

- **Lock Loss / Reacquisition:** The GPS receiver repeatedly fails to maintain a fix or continually reacquires satellites. For example, the fix quality flag may drop from 3D fix to no fix even with a clear sky. Erratic lock behavior (frequent loss of lock and retries) is a strong red flag [1]. Simple modules often have an LED or status flag – if it blinks (indicating loss of fix) despite normal conditions, GPS is likely denied.
- **Satellite Count Drop:** A sudden fall in the number of satellites in view is telling. In one analysis, events with interference showed "drop in number of satellites tracked accompanied by drop in SNR on all satellites" [2]. If the receiver goes from tracking many sats to tracking only 3–4, position quality plummets (PDOP spikes) and typically no solution is possible [2] [3].
- **Signal Strength Anomalies:** Monitor carrier-to-noise (C/N_0) or SNR on each channel. Jamming often drives the noise floor up, causing C/N_0 to plummet on all channels simultaneously [1] [2]. Likewise, an unusually high automatic gain control (AGC) voltage or a sudden, uniform SNR drop is a sure sign of interference [1] [4]. Many receivers (including u-blox chips) report AGC and C/N_0; flags like "C/N_0 abnormally low" or any active CW-interference alarm should trigger a warning [1] [5].
- **Data Integrity Errors:** Check for corrupted or missing GPS messages. Repeated NMEA/UBX checksum failures, truncated sentences, or parity errors mean the signal is being scrambled. Similarly, any Receiver Autonomous Integrity Monitoring (RAIM) or internal quality monitors reporting an integrity alert indicates inconsistent satellite data (often due to jamming). While simple modules lack full RAIM, a worsening DOP (dilution of precision) or unexplained fix loses also count here.
- **Position/Velocity Jumps:** Watch the reported fix for unrealistic behavior. Sudden "teleport" jumps in position when stationary, or wild swings in computed velocity (e.g. GPS reports moving fast while encoders say stopped) are telltales of signal spoofing or strong interference [1]. Even frequent small oscillations ("jitter") beyond normal GPS error bounds suggest the solution is being corrupted. In practice, any time the position drifts rapidly without the rover moving, or the filter reports large innovation errors, GPS should be suspected.

RTK-Specific Indicators

- **RTK Fix Loss (FIX→FLOAT):** In RTK mode, a drop from a full "RTK-FIX" to "RTK-FLOAT" or single-point indicates loss of carrier-phase lock. This can happen if the jamming obscures the carrier signal needed to resolve integer ambiguities. Track the RTK status word (e.g. UBX-NAV-STATUS or NMEA GGA fix flag); an unanticipated downgrade is a red flag [6].
- **Carrier-Phase Cycle Slips:** RTK relies on continuous carrier tracking. Multiple simultaneous cycle slips (sudden integer jumps in L1/L2 phase) are symptomatic of strong interference or sudden blockage [6]. For example, if many satellites slip lock at once (or L2 slips occur in clear conditions), the RTK solution will instantly lose fix. Logging or monitoring the raw phase residuals will reveal these slips.

- **Loss of Correction Data:** RTK depends on base-station corrections (e.g. RTCM via radio/NTRIP). A jammer may swamp the radio link or corrupt the stream. Watch for missing or malformed RTCM messages – if the corrections stop or become invalid, the rover reverts to float or single. Frequent link drops or checksums in the RTCM stream indicate an attack.
- **Solution Inconsistency:** Even if fix is maintained, large jumps or inconsistency in the centimeter-level solution can signal trouble. For example, the baseline between base and rover suddenly "wandering" or inflated position error messages (post-convergence spikes) imply loss of integrity. High float ambiguity or diverging covariance in the RTK filter also warrant alarm.
- **Built-in Jamming Flags:** Many modern RTK receivers have dedicated jamming detection. For instance, u-blox's ZED-F9P (a common RTK module) provides a UBX-SEC-SIG flag that goes active on jamming [7]. If available, monitor these security or interference indicators – any "jamming detected" message should immediately trigger a failover.

Other Indicators (by System)

- **(NEO-6M)** *GPS Module Status:* Watch NEO-6M outputs. If the GGA fix quality suddenly becomes 0 (no fix) or reverts from 3D to 2D with no apparent reason, the GPS is suspect. Likewise, frequent re-set of the time-of-week or losing the ephemeris/almanac (requiring a long reacquisition) are signs of RF jamming. Blinking activity LEDs (if present) or serial inactivity bursts despite power on also indicate denial.
- **(NEO-6M)** *Satellite/SBAS Loss:* If the NEO-6M loses SBAS/DGPS corrections (e.g. WAAS/EGNOS) that were previously available, or if it suddenly cannot see SBAS satellites, interference on L1 is likely. In a clean environment the module maintains a stable fix; a spurious loss of WAAS signal lock or differential lock is suspicious.
- **(RTK)** *INT/IOD Checks:* Advanced RTK modules may show inconsistencies between L1 and L2 measurements. For example, inability to track L2 for a satellite (while L1 is fine) can be detected as an internal "bad telemetry word" or ICC (Integrated Channel Count) alert. Also, if RTK integer bias resets often, watch for local jamming. These are subtle internal flags.
- **(RTK)** *Base-Rover Divergence:* In cases with known baseline, an RTK float solution that drifts beyond the expected radius (given the antenna separation) signals an anomaly. If the rover's computed coordinates start to violate the physical distance to the base station, jamming or spoofing may be corrupting the carrier phase.
- **(Sensor Fusion)** *INS vs GPS Discrepancy:* Compare inertial/wheel-deadreckoning to GPS. Large inconsistencies (e.g. IMU indicates forward motion but GPS still reads static, or the encoders report miles traveled while GPS delta is small) indicate GPS failure [8]. In practice, a Kalman filter's innovation for the GPS measurement will grow when GPS is wrong; if the IMU/odometry-predicted position drifts far from the GPS fix, switch modes [8].
- **(Sensor Fusion)** *Drift Rate Mismatch:* With pure IMU/encoder dead-reckoning, the rover's predicted drift is limited (e.g. a few m/s^2 accel bias); if GPS suddenly reports movement requiring unrealistic acceleration or if it contradicts the IMU attitude (e.g. says turning when IMU said straight), that's a cue that GPS is giving bad data. Monitoring consistency in velocity and heading between sensors helps catch subtle jamming.
- **(Sensor Fusion)** *UWB/Drone Cross-Check:* When available, compare the GPS-based position to the alternate position from UWB drones. A persistent offset beyond normal error between the UWB multilateration fix and the GPS fix means GPS is unreliable. Since the drones are outside the jam zone, their UWB-ranging solution should be trusted during GPS outages. Large discrepancies (> a few meters) or a sudden collision of the two solutions warrant switching to the UWB-based APS.

Triggering APS (Alternative Positioning System) Mode

To ensure timely fallback, the rover should continuously monitor both GPS metrics and auxiliary sensors. Key triggers include:

- **GPS Quality Metrics:** Thresholds on satellite count, C/N_0, fix status and DOP should be enforced. For instance, if satellites drop below a safe minimum (e.g. <5–6) or if *all* C/N_0 values suddenly fall below a pre-set limit, switch to APS [2] [1]. Similarly, any integrity flag (RAIM fail, UBX-SEC-SIG, or a security warning) must force a switchover.
- **Clock/Signal Continuity:** If the GPS solution stalls (no new fixes for >1–2 s) or the time-of-week jumps, trigger APS. Continuous absence of valid GPS data (or only 2D fixes) over a short time horizon indicates denial.
- **IMU/Wheel Inconsistency:** Monitor the navigation filter's innovation or covariance. If the INS/odometry-predicted state diverges by more than the expected drift (e.g. > a few meters beyond normal error) from GPS, that indicates degraded GNSS. In practice, one should compute the expected dead-reckoned uncertainty and if the GPS update lies outside this bound repeatedly, switch modes [8].
- **Velocity/Heading Mismatch:** If GPS-derived velocity or heading deviates sharply from the inertial estimates (beyond what wheel slippage or maneuvering could cause), interpret this as GPS error. For example, zero IMU acceleration with a sudden GPS velocity spike means GPS is lying.
- **UWB/Drone Checks:** Actively compare the UWB-based position (from the drone swarm) with GPS. Even though UWB is the alternative, during ambiguous cases it can validate GPS. If UWB-derived distance measurements or multilateration fixes systematically conflict with GPS (e.g. >1–2 m difference or inconsistent trajectories), trigger APS.
- **Persistent Errors:** Build in a simple logic: if any critical anomaly (low satellites, SNR drop, fix loss) persists beyond a short debounce time (to avoid false positives), lock out GPS and enable APS (inertial/UWB mode). The exact thresholds depend on rover speed and terrain, but must ensure safety margins in urban or forested areas where GPS can fluctuate.

Sources: GPS jamming and denial indicators as documented in GNSS security literature [1] [2] [7] [6] [8] (and manufacturer manuals) guide these checks. Monitoring both raw signal metrics (sat count, C/N_0, AGC) and cross-sensor consistency (INS/odometry, UWB) provides a comprehensive early warning to switch from GPS to APS.

---

[1] GNSS under attack: Recognizing and mitigating jamming and spoofing threats - GPS World
https://www.gpsworld.com/gnss-under-attack-recognizing-and-mitigating-jamming-and-spoofing-threats/

[2] [3] Integrity and Continuity Analysis for GPS
https://www.iaa.ie/docs/default-source/publications/gps-performance-monitoring/integrity-and-continuity-analysis/2023q1_integrity_continuity_iaa_v1.0.pdf?sfvrsn=f6f311f3_5

[4] [5] Innovation: Monitoring GNSS interference and spoofing — a low-cost approach - GPS World
https://www.gpsworld.com/innovation-monitoring-gnss-interference-and-spoofing-a-low-cost-approach/

[6] Innovation: Cycle Slips - GPS World
https://www.gpsworld.com/innovation-cycle-slips/

[7] ZED-F9P Integration manual
https://content.u-blox.com/sites/default/files/ZED-F9P_IntegrationManual_UBX-18010802.pdf

8 Insight: Anti-jamming and anti-spoofing for GNSS/INS
https://www.septentrio.com/en/learn-more/insights/insights/why-secure-gps-receivers-are-crucial-gnss/ins-systems