TECH NOTES

Edition 4 – January 2025

Tech notes is a newsletter produced by the CATCA Technology Committee for the purpose of providing information to CATCA members regarding technology, current and future, in NAV CANADA.

GNSS Spoofing and Jamming in Aviation: The Threat is Real

GNSS spoofing and **GNSS jamming** disrupt Global Navigation Satellite System (GNSS) signals essential for aircraft navigation, timing, and communications. Both are serious threats to aviation safety and air traffic control (ATC), as modern aircraft and ATC systems rely heavily on GNSS to maintain precise positioning and situational awareness. While they differ in approach—spoofing deceives by providing false signals, and jamming blocks legitimate signals—they both create risks that can jeopardize flight safety, especially during critical phases like approach, landing, or congested airspace navigation.

GNSS Spoofing

Spoofing occurs when false GNSS signals are transmitted to deceive a receiver into calculating incorrect position, velocity, or time information. This type of attack can mislead aircraft systems into believing they are in a different location or traveling along an incorrect trajectory, which can go unnoticed until serious deviations arise.

Effects on Aircraft Systems:

1. **Navigation Deception**:
    - Spoofed GNSS signals can mislead the autopilot or Flight Management System (FMS) by providing incorrect position data. This could cause the aircraft to deviate from its intended route without immediate detection, leading to airspace violations or proximity to restricted zones. In a crowded airspace, it could also increase the risk of midair conflicts.
2. **Instrument Landing Errors**:
    - Spoofing during approach can disrupt the accuracy of instrument-based landings (e.g., Localizer Performance with Vertical guidance or LPV). This may lead the crew to believe the aircraft is aligned with the runway when it is actually off course, increasing the risk of missed approaches, overshoots, or runway incursions.
3. **Loss of Situational Awareness**:
    - Spoofing can make the crew lose situational awareness, especially if the inaccurate data appears to align with expected values. If unrecognized, this misalignment can delay corrective action and lead to unsafe situations, particularly near terrain or restricted airspace.
4. **Communication and Timing Disruptions**:
    - GNSS spoofing can impact aircraft communications, as many systems use GNSS for time synchronization, essential for maintaining secure communication links between aircraft and ATC. Spoofed timing data can create discrepancies that may interrupt communications, reducing situational awareness for both pilots and controllers.

Effects on Air Traffic Control:

1. **Reduced Surveillance Accuracy**:
    - ATC systems, especially those relying on Automatic Dependent Surveillance–Broadcast (ADS-B), depend on accurate GNSS data to track aircraft positions. Spoofed data can lead to inaccurate position reports, resulting in reduced reliability of surveillance data and making it challenging for ATC to manage aircraft in affected airspace effectively.

2. **Increased Workload**:
    - Misleading GNSS data can create inconsistencies that ATC personnel must resolve manually, increasing their workload. The need to cross-check radar data, request pilot confirmations, or reroute aircraft to safer altitudes or airways could stretch ATC resources, impacting safety across the airspace.

GNSS Jamming

Jamming, unlike spoofing, blocks or overwhelms legitimate GNSS signals, preventing the receiver from accessing real-time position, velocity, or timing data. When jamming occurs, aircraft systems immediately lose GNSS data, alerting the crew to the failure. However, the sudden loss of GNSS signals creates challenges for both the aircraft and ATC.

Effects on Aircraft Systems:

1. **Loss of Navigation Precision**:
    - With GNSS signals jammed, aircraft cannot rely on GNSS-based navigation, requiring the autopilot and FMS to revert to backup systems such as Inertial Navigation Systems (INS) or ground-based aids (e.g., VOR and DME). While INS provides basic positioning, it tends to drift over time, reducing accuracy and increasing the likelihood of off-course deviations.
2. **Performance-Based Navigation Disruptions**:
    - Many modern flight paths are based on performance-based navigation (PBN) using GNSS for precision. In the event of jamming, PBN routes, including approach and departure procedures, become unreliable, forcing pilots to rely on less precise navigation methods. This limitation is particularly critical during instrument approaches, where precision is essential for safe landings.
3. **Increased Pilot Workload**:
    - GNSS jamming may force the autopilot to disengage, increasing the pilot's workload, especially in congested or low-visibility environments. Manual reversion to alternative navigation sources requires pilots to adapt quickly, increasing potential for human error in high-stress situations.
4. **ADS-B and Surveillance Interruptions**:
    - ADS-B relies on GNSS for aircraft positioning data, broadcasting this information to ATC and other aircraft to avoid collisions. During GNSS jamming, ADS-B data is either inaccurate or entirely unavailable, reducing ATC's ability to track the aircraft effectively and raising the risk of collision, particularly in areas with high traffic.

Effects on Air Traffic Control:

1. **Loss of Accurate Position Data**:
    - With GNSS jamming, ATC loses accurate ADS-B data, making it challenging to monitor aircraft location, speed, and altitude. In non-radar areas, where ATC heavily depends on ADS-B, this disruption can lead to significant blind spots, limiting ATC's ability to ensure safe separation between aircraft.
2. **Increased Separation Requirements**:
    - To compensate for reduced surveillance accuracy, ATC may need to increase separation between aircraft, which can reduce airspace efficiency and increase delays. With broader separation standards, capacity in crowded airspace diminishes, impacting the overall flow of air traffic and potentially delaying other flights.
3. **Coordination with Pilots**:
    - When jamming occurs, ATC may need to work closely with pilots to confirm positions, verify altitudes, or reroute aircraft using radar or voice communication alone. This additional coordination increases workload for both controllers and pilots, which can strain ATC resources during peak times and introduce the potential for miscommunication.

Mitigation Measures

Counteracting GNSS spoofing in air traffic control involves several strategies to enhance the integrity and security of navigation systems. Here are some effective measures:

1. **Multi-Source Navigation Systems**: Use a combination of navigation systems, such as Inertial Navigation Systems (INS), radar, traditional ground-based navigation aids (NAVAIDS), and multiple GNSS constellations.
2. **Signal Authentication**: Implement signal authentication techniques to verify the legitimacy of GNSS signals. This can include the use of cryptographic methods to ensure that the signals have not been altered.
3. **Monitoring and Anomaly Detection**: Establish monitoring systems that can detect anomalies in GNSS signals, such as sudden changes in position that do not align with expected flight paths.
4. **Training and Awareness**: Provide training for air traffic controllers and pilots on recognizing potential spoofing events and the appropriate responses to such incidents.
5. **Regular Audits and Assessments**: Conduct regular assessments of GNSS systems and their security measures to identify vulnerabilities and improve countermeasures.
6. **Use of Enhanced GNSS Technologies**: Explore advanced GNSS technologies like Differential GPS (DGPS) or Satellite-Based Augmentation Systems (SBAS) which can provide more accurate and reliable positioning information.
7. **Collaborative Data Sharing**: Foster collaboration with other aviation authorities and organizations to share information about threats and effective countermeasures against spoofing.
8. **Implementing Geo-Fencing**: Use geo-fencing techniques to restrict aircraft operations in certain areas, ensuring that if a plane deviates from its authorized path, it can trigger alerts.
9. **Emergency Procedures**: Develop and disseminate clear emergency procedures for pilots and air traffic controllers to follow if they suspect GNSS spoofing.
10. **Regulatory Measures**: Advocate for regulatory frameworks that require aviation systems to adopt robust anti-spoofing technologies and practices.

By combining these strategies, Canada can enhance its resilience against GNSS spoofing and ensure safer air traffic operations.

Both forms of interference represent serious safety concerns for aviation, highlighting the need for strong detection measures, alternative navigation systems, and effective air traffic control (ATC) coordination to mitigate these threats.

Efforts are in progress to expand and enhance ground-based navigation across Canada. Additionally, Transport Canada has issued Civil Aviation Safety Alert (CASA 2024-10), offering guidance for aircraft operators on utilizing both conventional NAVAIDs and conventional approach/arrival procedures. CATCA members must also be prepared for the possibility of aircraft needing to use these traditional tools and procedures, even unexpectedly.

Next Newsletter – May 2025

If you have questions or would like more information about ATS technology or CATCA technology roles, please contact any member of the CATCA Technology Committee or email techcommittee@catca.ca

---

Technology is a useful servant but a dangerous master. ~ Christian Lous Lange