GPS Jamming and Spoofing – No Longer an Emerging Threat

Austin Albright, Oak Ridge National Laboratory

Abstract:

In order to monitor and quickly respond to an issue when transporting radioactive material, we need to know where that material is as it is transported. The safety of the shipment necessitates knowing numerous time and position related details during the entire process: when it stops, how long it was stopped, where along its planned route it is, is it on the planned route, and so on. To do this, we need the information provided by a global navigation satellite system (GNSS) receiver. GNSS receivers are also commonly referred to as Global Positioning System (GPS) receivers due to GPS being the most well-known of the GNSS satellite constellations. Once GNSS jamming was a capability possessed by a few militaries, while GNSS spoofing was only a theoretical threat. Today, jammers can be purchased by anyone over the Internet [1]. Spoofing has transitioned from theory, to an emerging threat, to an emerged threat anyone with some technical savvy, YouTube, and a software-defined radio (SDR) can perform [2]. This paper will present some steps that can be taken today to help mitigate the risk from jamming and spoofing.

For context, jamming is the simplest technique and because of that simplicity the most prevalent threat to GNSS positioning. GNSS jamming is when a stronger signal at the same frequencies as the GNSS satellites' signals is transmitted to interfere with a GNSS receiver's ability to receive the signals from the satellites. Spoofing on the other hand is a technique where signals identical to those transmitted by the satellites are transmitted at slightly stronger power to trick a GNSS receiver into using the spoofed signals instead of the true satellite signals. Spoofing can be used to change the time, location, or both reported by a receiver. Spoofing can be used to cause a GNSS receiver to report that it is traveling as expected when it actual may be stopped or traveling in the wrong direction. Spoofing can allow a vehicle to appear to be safely parked to the remote monitoring center when it is actually underway.

What was once only the potential threats of GNSS jamming and spoofing to deny and compromise PNT information used to monitor cargo and assets is now a daily occurrence in and near conflict zones, is used regularly by criminal elements involved in cargo hijacking [3] and by "normal" people circumventing the monitoring of their company vehicle [4] without realizing the risk to everyone around them. In order to protect our abilities to safeguard and securely transport radioactive and nuclear material steps to detect and/or protect from attacks on GNSS derived time and position information that is so critical to monitoring and responding are needed. Several steps that can contribute to detecting and protecting the GNSS receiver that provides this critical information are presented in this paper.

[1] *L. Dyer, "No More Jammer Sales: It's Time for Global Enforcement,"* SpaceNews, Apr. 2024. [Online]. Available: https://space4peace.org/no-more-jammer-sales-its-time-for-global-enforcement/, Accessed: 7-Aug-2025

[2] Crazy Danish Hacker, “GPS Spoofing w/ BladeRF - Software Defined Radio Series #23.” Sep. 2016. [Video]. YouTube. https://www.youtube.com/watch?v=VAmbWwAPZZo, Accessed: 7-Aug-2025.

[3] Editor. “GPS Jammers Used in 85% of Cargo Truck Thefts - Mexico Has Taken Action.” Resilient Navigation and Timing Foundation, Oct. 2020 [Online]. Available: https://rntfnd.org/2020/10/30/gps-jammers-used-in-85-of-cargo-truck-thefts-mexico-has-taken-action, Accessed: 28-Aug-2025.

[4] C. Matyszczyk, “Truck driver has GPS jammer, accidentally jams Newark airport.” CNET, Aug. 2013. [Online]. Available: https://www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport, Accessed: 28-Aug-2025.