Demo: I Am Not Afraid of the GPS Jammer: Exploiting Cellular Signals for Accurate Ground Vehicle Navigation in a GPS-Denied Environment

Ali A. Abdallah†, Zaher M. Kassas†, and Chiawei Lee‡
† University of California, Irvine, USA
‡ US Air Force Test Pilot School, Edwards Air Force Base, California, USA
abdalla2@uci.edu, zkassas@ieee.org, and chiawei.lee@us.af.mil
Video Demonstration: https://www.youtube.com/watch?v=kwpCRXz-5gM

THIS demo presents unprecedented attack-defense results of a ground vehicle navigating to a meter-level accuracy in a real-world GPS-denied environment, by exploiting ambient cellular signals exclusively and no other sensors.

Today's vehicular navigation systems fuse information from a global navigation satellite system (GNSS) receiver (e.g., GPS) and an inertial measurement unit (IMU). Relying on GNSS alone to aid an IMU poses an alarming vulnerability: GNSS signals could become unavailable or unreliable in environments under a malicious attack (jamming or spoofing). Without GNSS, the IMU errors will accumulate and eventually diverge, compromising the vehicle's safe and efficient operation.

Current trends to supplement a navigation system when GNSS signals become unreliable are traditionally sensor-based (e.g., vision, lidar, sonar, and odometers). These sensors extract *relative* motion information to reduce the IMU's error divergence rate. However, these are dead-reckoning-type sensors; therefore, during prolonged periods of GNSS outage, the error will eventually diverge. Moreover, these sensors only provide *local* position estimates, may not properly function in all environments (e.g., fog, snow, rain, dust, nighttime, etc.), and are still susceptible to malicious attacks.

The authors developed a defense mechanism that exploits ambient cellular signals to produce an accurate, sustained navigation solution without GNSS. In contrast to the aforementioned sensors, *absolute* position information could be extracted from cellular signals to provide bounded IMU errors. Moreover, cellular signals are more difficult to jam and spoof than GNSS and are practically unaffected by poor weather conditions. To demonstrate the efficacy of this mechanism in a real-world GPS-denied environment, the authors were invited to participate in live GPS jamming experiments, called NAVFEST, at Edwards Air Force Base (AFB), California, USA. GPS signals were jammed with high-powered jammers, spread over an area of around 50 miles, which transmitted a variety of waveforms at jamming-to-signal ratio (J/S) exceeding 100 dB (see Fig. 1).

The vehicle was driven into the jammed environment, where it traversed 5 km in 180 seconds, of which, GPS signals were unavailable for the last 3.9 km. During the jamming attack, the vehicle-mounted navigation system, which utilized a commercial high-end GPS receiver (Septentrio AsteRx-i V) with a tactical-grade IMU (Vectornav VN-100) accumulated a position root mean-squared error (RMSE) of 238 m. In contrast, the developed defense mechanism exploited signals from eight cellular long-term evolution (LTE) towers, whose positions were mapped prior to the experiment, from the U.S. cellular providers T-Mobile and Verizon, one of which was more than 52 km away from the ground vehicle. These signals were processed by the author's software-defined radio (SDR) to produce pseudorange measurements, which were fused through an extended Kalman filter to estimate the vehicle's trajectory. The defense mechanism achieved a position RMSE of 2.6 m exclusively with cellular LTE signals and no other sensors. The results are summarized in Fig. 2. Note that to obtain the vehicle's ground truth trajectory, a vehicle-mounted GNSS-IMU system was used, which utilized signals from the non-jammed GNSS constellations (Galileo and GLONASS). It is worth noting that the unprecedented 2.6 position RMSE achieved in this demo are an order of magnitude smaller than previously published results in the same environment, which achieved a position RMSE of 29.4 m. Further details can be found in the video.

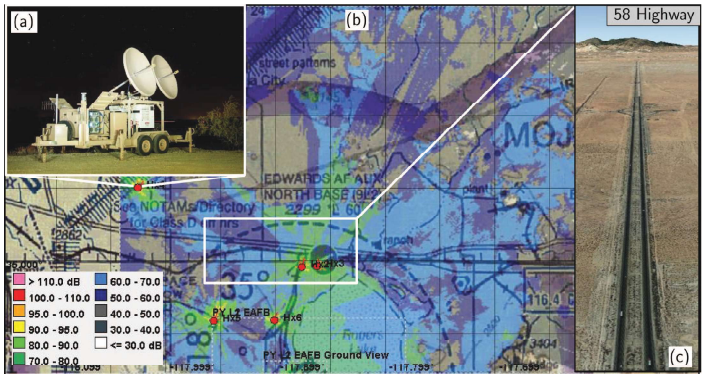

Fig. 1. NAVFEST GPS jamming laydown: (a) one of the jammers used in the experiment, (b) J/S heat map and the jammers' locations, (c) the 58 Highway, where the ground vehicle was driven. Map data: Edwards AFB.

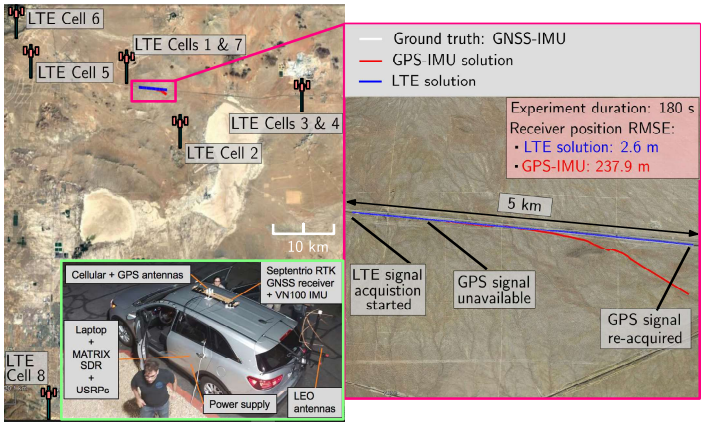

Fig. 2. Navigation solutions for (i) GPS-IMU, (ii) cellular LTE, and (iii) GNSS-IMU ground truth. Map data: Google Earth.

This work was supported by ONR grant N00014-19-1-2511, NSF grant 1929965, and DOT grant 69A3552047138. DISTRIBUTION STATEMENT A. Approved for public release; Distribution is unlimited 412TW-PA-20399.
Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022
24 April 2022, San Diego, CA, USA
ISBN 1-891562-68-1
https://dx.doi.org/10.14722/autosec.2022.23049
www.ndss-symposium.org