
Charles Barry  
Luminous Cyber Corp  
University of California, Santa Cruz  
Santa Clara, CA, USA 95051  
charles@luminouscyber.com  
chbarry@ucsc.edu

Marc Weiss  
Marc Weiss Consulting  
University of California, Santa Cruz  
Aptos, CA USA 95003  
marcweissconsulting@gmail.com  
mweiss2@ucsc.edu

ABSTRACT
As is well-known, signals from Global Navigation Satellite Systems (GNSS) such as the US Global Positioning System (GPS) are used throughout systems that US forces depend on. Yet GPS/GNSS are particularly unreliable in areas of US engagement with enemy forces, where jamming and spoofing would be advantageous to an adversary. We propose a solution that uses a software defined receiver and advanced algorithms to provide Alternative Position, Navigation and Timing (A-PNT) using Time Difference of Arrival (TDOA) of Low Earth Orbit (LEO) Signals Of OPportunity (SOOP). In this mode of using LEO signals, no confidential knowledge of the source signal is necessary. Indeed, no a-priori knowledge of the LEO orbit parameters, nor the time of transmission of the signals is assumed. This system is designed to work standalone or can also be used to complement existing navigation sensors that are typically used in navigation systems, including GNSS and Inertial navigation. Expansion to the usage of multiple LEO constellations will serve to optimize performance and resiliency in an RF challenged environment.

INTRODUCTION
As discussed in many papers such as [1] and [2], given the widespread and growing threats to GPS/GNSS of PNT and therefore to Telemetry, there is a clear and present need for robust A-PNT solutions. Overall, Civilian and defense PNT markets exceed $160B and enable trillions of dollars in global commerce yet suffer today from the vulnerabilities and fragilities of GPS/GNSS. We present a novel solution that utilizes TDOA of LEO SOOP for Hyperbolic Positioning, and Kalman filtering methods to provide accurate and robust A-PNT (Figure 1). There is no need to collaborate with, or communicate via, the LEO satellites themselves, nor even to have a-priori knowledge of satellite orbit nor of transmission time information. Therefore, any of the many LEO satellite systems may be used as references, e.g., Starlink, Kuiper, etc. Reference stations based at known location mark the times of arrival (TOA) of identifiable RF signal features (e.g., symbols, frame markers) from LEO satellites that can be received opportunistically received. These TOA data are securely streamed to Command-and-Control (C&C) servers located in the cloud. The C&C servers compute position, velocity, altitude (PVA) for all the LEO satellites. The LEO PVA are streamed to users, also called assets, e.g., Aircraft, Drones, UAV, and Vehicles. This technology has the potential to provide robust sub-meter accuracy. Importantly, implementation is intended on COTS Software Defined Radios (SDR). All PVA and TOA data are recorded at the C&C servers for forensic analysis and algorithm testing and improvement.
The LEO SOOP TDOA architecture is shown in Figure 1. The LEO SOOP architecture requires two steps. The first step is to determine the location of the LEO satellites. Knowing the LEO PVA, the asset can then use the subset of LEO signals it sees for its own PNT. An outline of the process is as follows:

- Clients/Assets and Reference Receivers mark TOA of Terrestrial & LEO SOOP
  - Reference sensors may be stationary or mobile as long as their location is known. They must be well-synchronized to less than 1 ns.
- TOA streamed to cloud and processed for Time Difference of Arrival (TDOA)
- TDOA, Kalman filter and AI/ML determine Position, Velocity, Acceleration (PVA)
  - References stream LEO SOOP TOA along with known reference position to Cloud (sync required)
  - Client streams LEO SOOP TOA to Cloud (sync not required)
  - Cloud computes LEO PVA; streams to asset
  - Cloud and/or asset determine asset location

**ALTERNATIVE PNT IS VITAL TO US SECURITY**

GPS broadcasts are low-power (typically -110dBm to -149dBm) [1] and are particularly vulnerable to interference. Spoofing and jamming are being used by Russia in east and southeast Ukraine to negatively impacts drone and other operations. Iran, and other state actors, are also known to practice spoofing and jamming of GPS signals. This poses a threat not to civilian and defense air transport with potentially devastating consequences.

Figure 2 shows a real-time map of GPS anomalies inferred from commercial aircraft ADS-B (see [https://www.gpsjam.org/](https://www.gpsjam.org/)). Jamming and spoofing are widespread over Ukraine and Syria, however commercial flights are not conducted over these highlighted areas. Therefore, there is a clear and present need for alternatives, among which include the following.

- Two large categories of signals for PNT
  - Signals of Intent (SOI) – e.g., GPS/GNSS, eLoran
  - Signals of Opportunity (SOOP) – RF signals unintended for PNT
- Alternative Sources
  - GPS rebroadcast in other bands
While all these alternatives have varying degrees of promise, this paper focuses on the use of SOOP from LEO satellites for TDOA. Ultimately, it is envisioned that an ensemble of PNT solutions would be processed by multi-sensor filter algorithms such as Kalman filters, Extended Kalman Filter and Particle filters to achieve robust A-PNT [4].

SOOP has been studied and tested for several decades, but it is the advent of low-cost, ubiquitous and highly effective Software Defined Radio (SDR) platforms, and a flourishing engineering community for SDR development, that has led to recent successful implementations. In particular, Figure 3 shows the results of a Signals of Opportunity (SOOP) implementation using Digital FM Radio and TDOA multilateration. In this case, the system used:

- Fixed Terrestrial RF sources
  - AM, FM, DAB, OTA DTV
  - Known transmitter locations
  - Vastly greater power than satellite
- TDOA algorithms difference Time of Arrival (TOA) of signals emanating from different locations to compute asset location.
  - FM HD Radio signals achieved 30 ns (10 m) accuracy
Although this demo system achieved fair position accuracy at 10 m using Digital FM Radio, much better accuracy should be achievable with a higher bandwidth signal such as those being proposed and fielded in LEO services.

**Figure 3**: SOOP using terrestrial Digital FM Radio to achieve 30ns (10m) position accuracy.

**LEO Signals of Opportunity for PNT**

Figure 4 shows a snapshot of the positions of a 717-satellite subset of the active Starlink, OneWeb, Iridium, GlobalStar, Iridium, and Orbcomm LEO constellations. In times, thousands, if not tens of thousands of LEO satellites will be in orbit, offering ample global coverage with sufficient density for LEO SOOP TDOA.

**Figure 4**: Subset of Starlink, OneWeb, Iridium, GlobalStar, Iridium, and Orbcomm satellites

---

TDOA HYPERBOLIC POSITIONING

Figure 5: 3D Asset Position is at intersection of hyperboloids formed from TDOA.

GPS/GNSS use Time of Arrival (TOA) measurements along with telemetry from the GNSS of the position and time of transmission of the satellite. Using TOA in this mode for positioning is done by intersecting spheres defined by the TOA from each satellite. This can be called Spherical positioning. Our proposed system, using SOOP and TDOA data, works by intersecting hyperboloids defined by the TDOA created by differencing the TOA for each satellite signal and the pairs of reference sensors receiving it. Hence this is called Hyperbolic positioning.

Hyperbolic positioning is a mathematical multilateration technique for find the position of an RF source. The TOA of signals arriving several reference sensors are differenced from the TOA of the signal arriving at least one primary reference sensor to form TDOA data. Each TDOA defines a hyperbola in 2 dimensions and the surface of a hyperboloid in 3 dimensions. The TDOA process is shown geometrically in Figure 5, where the position of the source (LEO satellite) is found at the intersection of three hyperboloids. Four references are required to form the minimum 3 hyperboloids needed to find position in three dimensions. In many cases, there will be TDOA from more than 4 reference stations allowing multilateration. It is required that each sensor be very accurately synchronized (to less than 1 ns) in order to achieve sub-meter accuracy. In practice, the location is found as a solution to a linear algebraic formulation and solved iteratively. One such algorithm, is the Taylor Series approximation of the TDOA solution, known as Foy’s algorithm [5]. Our simulations use Foy’s algorithm in 3-D. In this paper, we refer to the process as TDOA Hyperbolic Positioning, or more simply, as TDOA.

Advantages/ Disadvantages: TDOA with LEO Satellites

- Previous Studies
  - Doppler results measured: ~ 8 m accuracy [6]
  - Doppler GDOP estimates 1-5 m accuracy [7]
  - Results simulated combining INS and LEO signals ~ 10 m [8]
  - Results measured combining INS and LEO signals ~ 20 m [9]
- We propose Time Difference of Arrival – Hyperbolic positioning with LEOs
Advantages with LEOs
- 20 times closer to Earth than GNSS signals ➔ 300 - 2,400 times more RF power than GNSS
- Many thousands of satellites by One Web, Space X (Starlink), Amazon (Kuiper), and others
- Diverse Frequency bands and directions

Disadvantages – and mitigations
- These being communications satellites, they are unlikely to provide several satellites visible at a given location
- With high comm data rates, side-lobes may be strong enough for PNT
- Positioning may require using multiple constellations
- Ground sensors need sync and position
- Estimators can assist sensor position and sync

**LEO Constellations**

The ever-growing number of LEO constellations offers ample numbers of visible LEO satellites that provide SOOP for TDOA. Table 1 highlights a number of constellations, showing dozens of potential satellites visible 7.5° above the horizon. In practice, fewer will be usable for TDOA due to focused spot beams. In addition to a minimum of 4 visible satellites, accurate TDOA requires sufficient signal bandwidth. GPS/GNSS operates in 20MHz to provide sub-meter accuracy. Starlink, in particular, has many subcarriers with 50Mhz channel bandwidth and this affords the potential to achieve position accuracy on a par with GNSS.

<table>
<thead>
<tr>
<th>Name</th>
<th>No. of Planes</th>
<th>Sats./Plane</th>
<th>Total No. of Sats.</th>
<th>Inclinations(s) (deg)</th>
<th>Altitude(s) (km)</th>
<th>Min. No. Visible Above 7.5° Elev. Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iridium</td>
<td>6</td>
<td>11</td>
<td>66</td>
<td>86.4</td>
<td>780</td>
<td>1</td>
</tr>
<tr>
<td>OneWeb (Initial)</td>
<td>18</td>
<td>40</td>
<td>720</td>
<td>87.9</td>
<td>1200</td>
<td>19</td>
</tr>
<tr>
<td>Starlink (Initial)</td>
<td>32</td>
<td>50</td>
<td>1600</td>
<td>53.0</td>
<td>1150</td>
<td>56°</td>
</tr>
<tr>
<td>Kuiper</td>
<td>34</td>
<td>34</td>
<td>1156</td>
<td>51.9</td>
<td>630</td>
<td>17°</td>
</tr>
<tr>
<td>Starlink (Final)</td>
<td>51</td>
<td>50-75</td>
<td>2825</td>
<td>53.8-81.0</td>
<td>1110-1325</td>
<td>81</td>
</tr>
</tbody>
</table>

*In ± 65° latitude range. †In ± 60° latitude range.

Table 1: Characteristics of large LEO constellations

- Starlink has permission to transmit in/near Ku, and Ka bands
  - Satellite to Terminal: 10.7-12.7, 37.5-42.5 GHz
  - Satellite to Gateway: 17.8-18.6, 18.8-19.3, and 37.5-42.5 GHz
  - Tracking, Telemetry, Control: 12.15-12.25, 18.55-18.6, 37.5-37.75 GHz
  - Reference: “What Frequency Does Starlink Use?”
- All downlink signals are valid for use in TDOA
- Channel bandwidth of 50 MHz (Ku):
  - Potential for range accuracy of 1ns (0.3m)
  - Potential for LEO position to meter(s) (see simulations, below)

---

SIMULATION RESULTS

We show a first simulation in Figure 6. This is a single simulation with a single set of values of additive white Gaussian noise (AWGN) for range error of 0.3 m (= 1 ns), resulting in a 0.8 m LEO satellite position error. This geometry makes the view angle from the sensors on the circle to the satellite at 35 degrees. This provides a good Position Dilution of Position (PDOP) for determining position of the LEO. PDOP is the geometric function that gives the expected accuracy of positioning as a multiplier of the range error. We show more about this later with Figure 10.

Figure 6: 8 Sensors at radius 830 km, 1 at center, LEO Asset 590 km high

Figure 7 gives a full Root-Mean-Squared Error (RMSE) by averaging over 100 trials with different AWGN for each input error value. We have highlighted the 0.3 m (= 1 ns) input value giving an output of 0.8 m.

Figure 7: Asset (LEO) position accuracy RMSE as a function of range error standard deviation.
Figure 8: 400 Sensors within 830 km, LEO Asset 590 km high

The second simulation scenario, shown in Figure 8, is similar to Figure 6, but with 400 sensors within the circle. This yielded 0.06 m LEO satellite position error given a 1 ns range accuracy. 0.06 m in position is equivalent to better than 0.2 ns accuracy. The concept here is that positioning the satellite can be estimated simultaneously with positioning the users.

Figure 9: Asset (LEO) position accuracy RMSE over 100 trials with AWGN, as a function of range error standard deviation.

In Figure 9 we compute the RMSE over 100 trials with AWGN range error, analogous to Figure 7, but with the 400 sensors as in Figure 8. We highlight the 0.3 m = 1.0 ns input error showing an output position error of 0.3 m = 1.0 ns.

Our last simulation figure is of the Position Dilution of Precision (PDOP) for the 9-sensor configuration. We compute PDOP for TDOA using equations similar to those in [10]. The geometry is the same as for Figure 6 and Figure 7. PDOP is the multiplicative factor that predicts the position estimation error given error in the range measurement. The plot shows PDOP over an x-, y-plane of constant height of 590 km, as in the other figures.
LEO TDOA Total Position Dilution of Precision (PDOP)

CONCLUSIONS

• GPS/GNSS vulnerabilities drive the need for robust alternative PNT to support telemetry
• Massive numbers of LEO satellites that are becoming available can provide signal sources for Alternate PNT
  • Starlink, Kuiper, Iridium, many more coming
• TDOA techniques can be used for PNT accuracy without requirements on LEO signals
  • Requires accurate timestamp of significant instant, e.g., Framing Symbol(s)
• Simulations show potential for user A-PNT accuracies comparable with GPS
  • For 0.3 m (= 1 ns) range error we find sub-meter LEO positioning accuracy
  • If we can jointly estimate the LEO position with users under the satellite a 0.3 m (=1 ns) range error conservatively leads to better than 0.3 m (= 1 ns) position error

Authors acknowledge the contributions of Professor Ricardo Sanfelice, Director, Cyber Physical Systems Research Center, University of California at Santa Cruz, Masterclock CEO, John Clark, and Robert Swirksy.

REFERENCES


