SEPTEMBER 2019

AUTONOMY AT SCALE

Intelligent Machines Advancing Technology to Improve our Future

noblis®

For the best of reasons

NOBLIS.ORG

TABLE OF CONTENTS

Fundamental Technology:

Use Cases:

Challenges:

FUNDAMENTAL TECHNOLOGY: **A PRIMER ON POSITION, NAVIGATION & TIMING**

Matt Monaco

The ability to accurately and reliably determine position is essential to ensuring safe and efficient autonomy. The advent of Global Navigation Satellite Systems (GNSS) such as the United States Global Positioning System (GPS) has brought this technology to the masses and enabled the autonomous systems we have today. Not only does GNSS ensure accurate navigation and positioning, it also enables worldwide synchronous timing to the 100 billionths of a second. This level of precise timing is critical for the economy—providing a frequency standard for the distribution of power, synchronizing weather radars, and performing financial transactions[1].

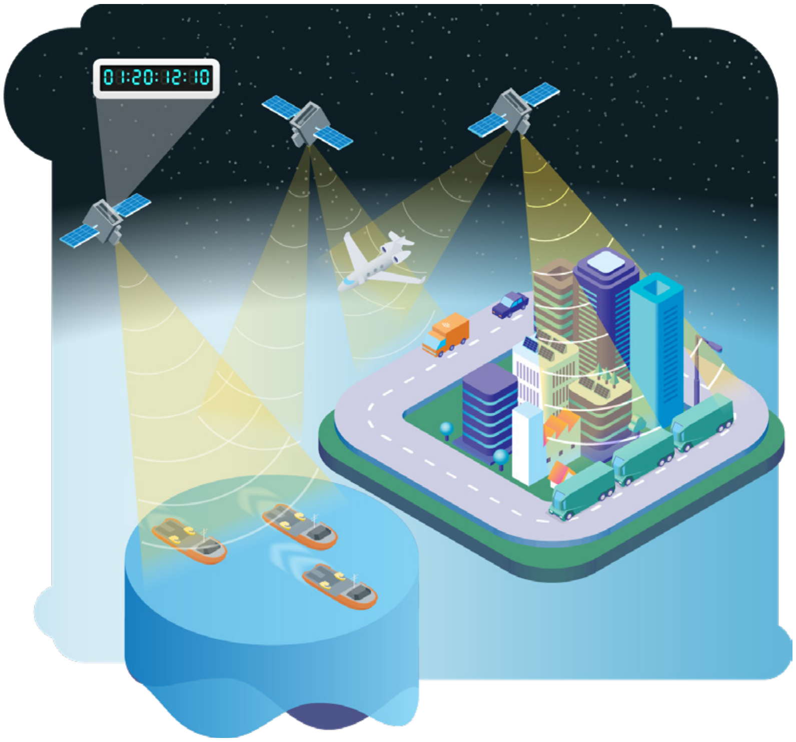


Figure 1: GNSS-PNT Sources and Limitations

While GNSS is the predominate technology used for position, navigation, and timing (PNT) in autonomy, other technologies such as Inertial Navigation Systems (INS) and fixed-position multilateralization compliment and increase resiliency. Techniques that use motion and rotation sensors to continuously calculate position by dead reckoning[2] (e.g., INS) and celestial navigation are resilient to the type of spoofing attacks and interference that can occur with GNSS and other radio navigation technologies, but with the trade-off of increased error due to their self-containment. Because all PNT technologies have their strengths and weaknesses, the combined use of multiple technologies in an integrated system can provide additional accuracy and resilience from both benign and malicious disruptions to PNT service.

GNSS PNT technologies provide another important function for autonomy beyond enabling autonomous navigation. They provide the highly precise timing essential for the execution of maneuvers of autonomous vehicles and deep space orbital maneuvers, entry, descent, and landing. This level of timing precision will become more critical as other platforms become truly autonomous and begin to operate in more constrained environments. The GNSS timing source can be utilized as a low-cost frequency standard for applications such as synchronizing radio frequency receivers and passive radars.

Alternative and Supplemental PNT for GNSS-Denied Environments

Despite the success of GNSS, it is not perfect. GNSS signals are weak and do not penetrate structures well. They require constant connectivity, offer little security measures, and are not encrypted. Current GNSS technology is also susceptible to malicious actors who can inexpensively and easily jam GPS signals, making the devices unusable. GPS signals can also be spoofed to create false positioning and timing readings, either by introducing radio waves that produce incorrect measurements of time and frequency or by spoofing the digital data used to process signals. GPS spoofing attacks are believed to have been used to down a U.S. autonomous aircraft in Iran in 2011[3].

The U.S. government has initiated multiple efforts to improve the operation of GPS systems, including efforts to ensure the resiliency of critical infrastructure by providing recommendations to operators, manufacturers, and researchers[4]. The National Timing Resilience and Security Act of 2017 names the U.S. Department of Transportation (USDOT) as the responsible party to establish terrestrial backup timing systems for GPS[5]. This includes requirements for the system to be terrestrial, wireless, robust to disruption, and able to reach remote locations and penetrate buildings. While this is initially designed to be a timing backup to GPS, the system must—to the maximum extent possible—be expendable to provide full PNT services. Potentially related to this new legislation, there is restored interest in enhancing existing legacy radio-based PNT infrastructure, such as enhanced long-range navigation (eLORAN), as a national backup for GPS[6]. A surface-based radio navigation technology, eLORAN works similarly to GPS and has been in existence for over 50 years. The predecessor to eLORAN, LORAN-C, was operated by the U.S. Coast Guard until it was shut down in 2010 due to the prevalence of GPS. The recent prevalence of GPS jamming and spoofing has renewed interest and urgency in ensuring that a resilient backup exists.

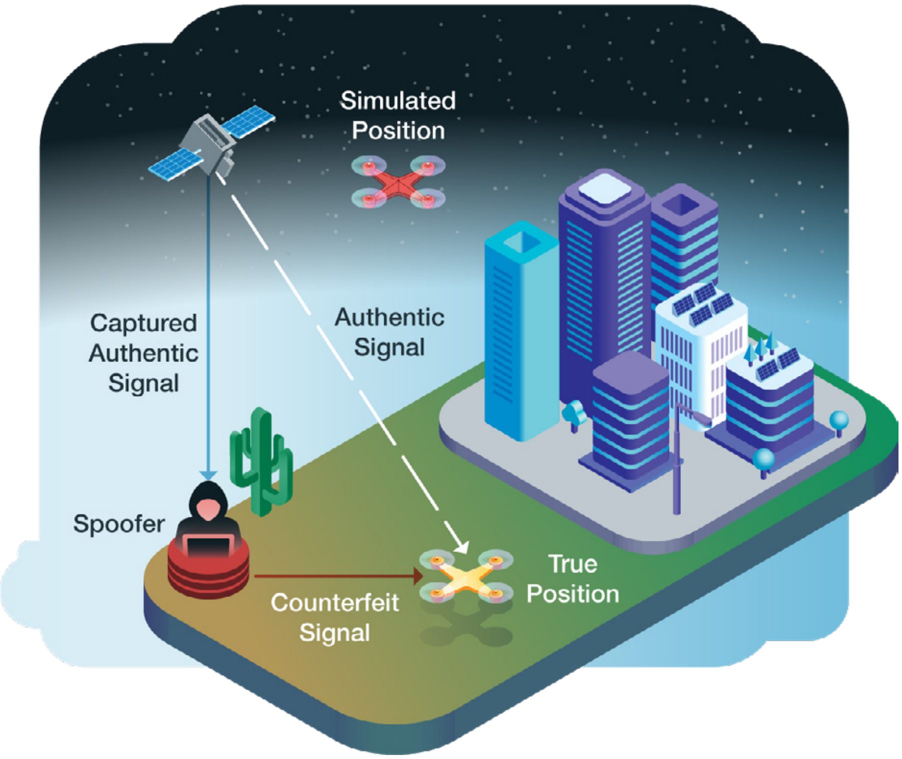


Figure 2: GNSS technologies can be susceptible to interference and malicious activities

Research efforts to develop countermeasures and resiliency to PNT attacks have recently increased as the search for new technologies to supplement GNSS intensifies. U.S. government agencies such as the Defense Advanced Research Projects (DARPA)[7], all military branches[8], and the Department of Homeland Security (DHS)[9] have increased investment into developing technologies that both increase the robustness of GNSS and create alternative sources of PNT. Examples of this research include efforts to increase the accuracy of INS sensors through advances in MEMS and to reduce the size and cost of highly precise timing standards such as man-portable atomic clocks, quantum clocks, or X-ray pulsar timing.

UTILIZING SENSOR SYSTEMS FOR PNT

While LIDAR alone cannot provide accurate of vehicle positioning, when fused across a large number of cooperating vehicles that are sharing data, it has the potential to assist in assuring accurate PNT, especially where GNSS is not available.

The Future of PNT and Autonomy

As broader autonomous applications continue to expand our reliance on highly accurate and precise PNT, additional sources of PNT must be used in tandem with GNSS. For most civilian autonomous applications, it is conceivable that ground-based systems (similar to what is used today for civilian air traffic management) will be developed to provide a level of redundancy. While this redundancy reduces the reliance on a sole source of PNT, ground-based systems are still susceptible to jamming and interference. Future autonomous systems will likely couple hybrid and autonomous PNT solutions that combine external PNT sources (such as GNSS) with internal (INS) and secondary sensors to augment and enhance performance.

Autonomy at scale is critical for attaining this level of assurance: the vast collections of sensor networks created by autonomous systems working collectively at scale will enable high-performing PNT solutions in all operating environments.

PNT RESILIENCY FOR CONNECTED AND AUTONOMOUS VEHICLES

Noblis has been at the forefront of connected vehicle applications for the past decade, working with USDOT and its research arms. Through this work, Noblis has gained unique expertise in understanding PNT in the connected vehicle and infrastructure spheres.

The position of a connected and autonomous vehicle (CAV) is perhaps the variable most dependent on reliable accuracy. For this reason, the resiliency of positioning the CAV is of upmost importance. Position is primarily gained from onboard GPS but can also be verified from several other sources. This can quickly become a problem for a wide range of reasons, whether they are nefarious or simply environmental. Vehicles often lose GPS signal in the "urban canyons" of large cities or the vast expanse of rural areas. In the case of a malevolent actor, they may be attempting to spoof the signal of multiple vehicle sensors. A CAV is unable to communicate its position to another vehicle if it is unsure of its own position, leading to the greater problem of trust between driverless cars. In the event of poor GPS coverage, what can be done when the GPS-enabled vehicles suddenly lose their most vital sense?

This is where misbehavior detection and authorization come into play. Through credentialing and authorizing devices that talk to each other, engineers can create a basic trust system between devices that extends to the vehicles where they are installed. Noblis leads this effort through a range of projects aimed at understanding, diagnosing, and de-credentialing a CAV's positional information.

To detect position inaccuracies, Noblis has taken an approach that compares aggregated position data from all vehicles within range of a central data observer—primarily a device installed on infrastructure to detect vehicles passing by. To aid in "sniffing" for the positions of other vehicles, an algorithm was built to select those that stand out as unusual. These messages are flagged and then tracked back to a certification list. If they misbehave often, they will no longer be allowed to communicate to other connected vehicles and will be forced to go without the full benefit of the autonomous applications. This approach is currently being tested for USDOT and Noblis anticipates it will be installed in CAVs in the future.

SOURCES

1 Retrieved from www.gps.gov/applications/timing

2 Dead reckoning is the calculation of position by advancing from the current position based upon a known velocity vector and elapsed time

3 Peterson, Scott and Faramarzi, Payam. (2011, December 15). Exclusive: Iran hijacked US drone, says Iranian engineer. The Christian Science Monitor. Retrieved from https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer.

4 U.S. Department of Homeland Security. Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure. Washington, DC. Retrieved from https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf

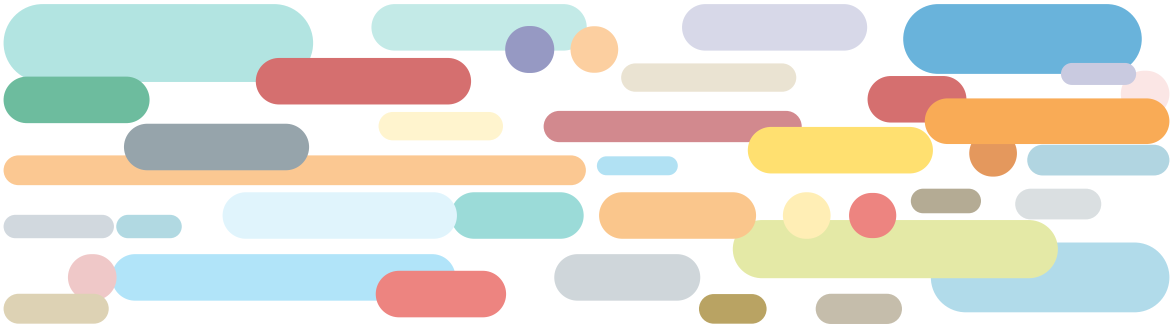
5 2018, December 5. President signs National GPS Timing Resilience and Security Act – GPS World [Blog]. Resilient Navigation and Timing Foundation. Retrieved from https://rntfnd.org/2018/12/05/president-signs-national-timing-security-and-resilience-act-gps-world/

6 Gallagher, Sean. 2017, August 7. Radio navigation set to make global return as GPS backup, because cyber. Retrieved from https://arstechnica.com/gadgets/2017/08/radio-navigation-set-to-make-global-return-as-gps-backup-because-cyber/

7 2014, July 24. Beyond GPS: 5 Next-Generation Technologies for Positioning, Navigation & Timing (PNT). Retrieved from https://www.darpa.mil/news-events/2014-07-24

8 Erwin, Sandra. (2017, December 15). Congress demands additional security, backup for military GPS signal [Blog]. Retrieved from https://spacenews.com/congress-demands-additional-security-backup-for-military-gps-signal/

9 2018, August 12. New DHS Risk Center to Deal with GPS, PNT Issues. Resilient Navigation and Timing Foundation. Retrieved from https://rntfnd.org/2018/08/12/new-dhs-risk-center-to-deal-with-gps-pnt-issues/



ABOUT NOBLIS

Noblis is a nonprofit science, technology, and strategy organization that brings the best of scientific thought, management, and engineering expertise with a reputation for independence and objectivity. We work with a wide range of government and industry clients in the areas of national security, intelligence, transportation, healthcare, environmental sustainability, and enterprise engineering. Together with our wholly owned subsidiary, Noblis ESI, we solve difficult problems of national significance and support our clients' most critical missions.

NOBLIS.ORG

noblis®

For the best of reasons

☎ 703.610.2000 answers@noblis.org @NoblisInc