SPACE-BASED POSITIONING
NAVIGATION & TIMING

NATIONAL ADVISORY BOARD

NATIONAL SPACE-BASED POSITIONING, NAVIGATION, AND TIMING ADVISORY BOARD

White Paper

GPS High Accuracy and Robustness Service (HARS)

May 5, 2023

This white paper was prepared by the board to support recommendation number PNT27-04-ECAS, to develop and implement a GPS High Accuracy and Robustness Service (HARS) delivered to users via the Internet, which was approved at the PNTAB-27 meeting (Nov. 16-17, 2022) and formally submitted to the National Space-Based PNT EXCOM co-chairs via Memorandum on January 27, 2023.

(page intentionally left blank)

GPS High Accuracy and Robustness Service (HARS) Executive Summary

v1.3 2023-05-05

The problem: GPS is falling behind other Global Navigation Satellite Systems (GNSSs) such as Europe's Galileo and China's Beidou. GPS has adopted an approach of allowing augmentation by third-party systems (such as Assisted-GNSS in mobile phones, WAAS for aviation accuracy and integrity, and commercial RTK for precision users), rather than providing specialized advanced services itself. Also, the data message modulated on the GPS signals is fragile. Environmental effects or malicious actions can prevent a receiver from reading the information or manipulate what is read, limiting robustness of the GPS signals.

Currently, GPS is the primary system in almost all GNSS chips, even chips made in Europe or Asia. That is: chips are designed to acquire GPS signals first, then signals from other systems. But Galileo and BeiDou are deploying high accuracy services that provide sub-meter position accuracy, enhancing satnav use in many civil applications. The absence of any plan for GPS to offer a similar high accuracy service could cause GNSS chips to begin using Galileo or BeiDou, rather than GPS, as the primary system.

A switch away from GPS as the primary PNT system is a problem for the US Government because it will lose its strategic advantage. Existing commercial chips are used in many strategically important US assets, such as airlines, ships, and organizations that support the US military. Once these chips change their architecture to Galileo-first or BeiDou-first, these strategic use cases become dependent on these services. It is one step in the direction of not having a GNSS system at all, and borrowing the system of another power; exactly the situation that Europe and China were in before they built their own systems. GPS would no longer be the "pre-eminent space-based PNT service" called for in Space Policy Directive 7 [1].

The Solution: A high accuracy and robustness service (HARS) provides information to user receivers, reducing errors and enhancing the ability to operate in challenging conditions. The PNT Advisory Board has identified a solution that the U.S. Government can provide a HARS without adding cost and complexity to GPS itself; instead obtaining the needed information from Government or Government-sponsored organizations and providing it over the Internet to properly equipped receivers.

The result would be a world-class HARS at a small fraction of the cost or time, compared to implementing it on new GPS satellites. The HARS would provide cryptographically-protected robust (resistant to jamming and spoofing) GPS for critical infrastructure, and would enable new applications (such as lane-dependent route guidance in automobile navigation and emergency vehicle guidance, GPS-only precision positioning of drones) that extend the societal benefits of GPS. HARS would be secure and less sensitive to radio noise and disruptions including spoofing.

The ask: Funding and operator
The HARS system needs funding and an operator, such as the USSF, the DOT, or similar.

GPS High Accuracy and Robustness Service (HARS), white paper

v1.3 2023-05-05

Overview: The problem and Solution

The problem: GPS is falling behind the EU (Galileo) and China (BeiDou), because it is constrained to maintain backwards compatibility and the lifetime of its satellites is too long to replenish the constellation with up-to-date services. The satellites and ground control system cannot be replaced quickly enough to add features such as high accuracy services, and data encryption or cryptographic signatures. New signals such as L2C, L1M, L2M, and L5 are taking decades to roll out, even today they are only present on a subset of the constellation [2]. The new civil codes do offer resilience against unintentional interference and ionospheric delay errors. However, they do not allow for the introduction of innovative new services such as those now being offered by Galileo and BeiDou.

GPS is the primary system in almost all GNSS chips, even chips made in Europe or Asia. That is: chips are designed to acquire the US-provided GPS signals first, then the other systems [4]. If GPS continues to fall behind we will see the next generation of GNSS chips switch to Galileo-first or BeiDou-first, and GPS will lose its primacy and influence on the world.

The lack of innovative new services such as precise point positioning and data encryption/signatures is a problem for all GPS users. A switch away from GPS as the primary constellation is a problem for the US Government because it will lose its strategic advantage. Existing commercial chips are used in many strategically important US assets, such as airlines, ships, and organizations that support the US military. Once these chips change their architecture to Galileo-first or BeiDou-first, these strategic use cases become dependent on these services. It is one step in the direction of not having a GNSS system at all, and borrowing the system of another power; exactly the situation that Europe and China were in before they built their own systems. GPS would no longer be the “pre-eminent space-based PNT service” called for in Space Policy Directive 7 [1].

The solution.
Innovative new services cannot wait for a full replenishment of the GPS constellation. Instead we can use flexible “out-of-band” delivery mechanisms that can be implemented much more rapidly. New services should be made available to the user community through the internet, reliably and securely. Thus, they would not be restricted by GPS’s low bit rate and need for backwards compatibility. This approach could be used to provide high rate GNSS error corrections to allow Precise Point Positioning (PPP), authentication, and more. The disadvantage is that the user equipment will need to have separate connectivity to the internet. However, such capability already exists with mobile phones and many other receiver implementations. Further, such connectivity will only increase across the user community, with satellite internet providing the ability to reach terrestrial users wherever the GPS signals do.

The first new service that should be provided would be a High Accuracy Robustness Service (HARS) similar to that planned on the other constellations. There are already government organizations that generate the essential components required for broadcast to the users. These should be made readily available to all GNSS users in order to ensure GPS maintains its relevance in the hierarchy of satellite navigation systems.

There are three components of systematic errors that GPS HARS can remove:

1. Satellite orbit and clock errors
2. Ionospheric errors
3. Tropospheric errors

Corrections for each of these constitutes a high-accuracy-service:

1. There are government organizations that have the expertise to compute precise GNSS orbit and clock errors (see, for example, the GDGPS report from the PNTAB [3]).
2. Models of the ionospheric TEC (total electron content) can be computed similarly.
3. There are already US Government-provided global models of weather data which is enough to compute the tropospheric errors.

These corrections together can be provided over the internet; in an analogous way to how A-GPS Assistance data is currently provided to every smartphone, allowing GPS to work in mobile phones.

Along with the corrections, the Nav Data (ephemeris) can be cryptographically signed and delivered on the same channel. This solves the problem of spoofed nav data.

By providing cryptographically signed corrections and Nav Data over the internet, GPS solves the problem of long satellite-refresh cycles and falling behind the accuracy and security innovations of other GNSS, meets requirements of SPD 7, and re-establishes itself as the premier system.

Solution details

Service to Enhance Robustness and Security

HARS **Augments** GPS by increasing accuracy, as described below; it can also **Toughen** GPS by enabling greater receiver sensitivity and providing verifiable Nav data (ephemeris) to defeat spoofing. Since cellular signals are received at much higher power, they can be used in environments where GPS receivers cannot read the data message from the GPS signals, enhancing robustness.

Cryptographic data signing is a process that uses a digital signature to prove the authenticity, integrity and non-repudiation of a piece of data. This process involves taking the data and a private key from an asymmetric cryptography private-public key pair and generating a digital signature that is attached to the data. The recipient of the data can then use the sender's public key, along with received data and signature, to verify the signature. That procedure in turn verifies that the data has not been tampered with and that it did indeed come from the claimed sender. This process can defeat spoofing by ensuring that the data can be traced back to its original source and that any changes to the data can be detected.

A NIST lightweight cryptography standard can be used for resource constrained use cases (such as GPS chips) [5]. A lightweight cryptographic hash can be used for signing, using algorithms such as HMAC, described in [6].

The HARS service could include, beyond the corrections discussed above, a pre-broadcast of the raw navigation message data. The pre-broadcast would anticipate the actual broadcast of the satellites by several seconds (e.g. 10 seconds). This raw navigation data with digital signature authentication is then distributed to the users. The users can compare the navigation data bits received via HARS to the navigation data bits they are decoding from the satellite signals they are tracking. In the event of a data spoofing attack, the data will not match and the user can be alerted to distrust the satellite signals they are receiving as they are not from the authentic source.

In addition to the security benefits of the HARS navigation data pre-broadcast, there is a benefit to robustness of signal tracking. If the user receiver no longer needs to demodulate the navigation data, then the receiver correlation time may be extended well beyond the time of one navigation data bit interval. This can allow the receiver to track a satellite signal at a much lower C/No, thus achieve better performance in challenging environments (e.g. under heavy tree canopy, indoors, or in the presence of interference.)

Furthermore, increased coherent integration time, sometimes known as “super-correlation”, leads to directional antenna gain for a moving receiver. This adds robustness against spoofers and jammers.

Additional methods to toughen GPS and GNSS can be incorporated into this service. For example, the Galileo HAS (High Accuracy Service) provides corrections to orbit and clock data for both Galileo and GPS satellites. Galileo and GPS have long had a cooperative relationship. Practically all commercial GPS receivers are now multi-constellation GNSS receivers. We have seen several constellation failures in the recent past (including Galileo clock errors). HARS can provide constellation reliability data for both GPS and Galileo, enhancing the robustness of commercial GPS receivers that also use Galileo.

State Space Representation Corrections

The systematic errors in the GPS system can be grouped into three:

- satellite orbit and clock errors
- ionospheric errors
- tropospheric errors

As shown in the figure:

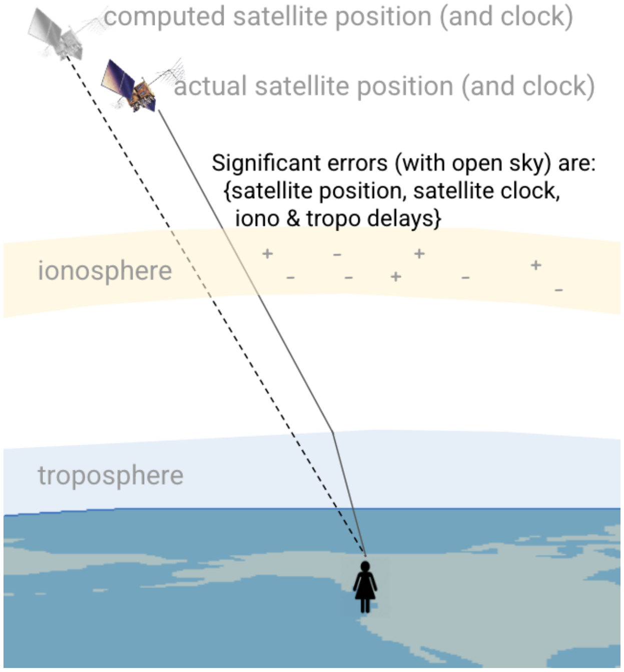
computed satellite position (and clock)
actual satellite position (and clock)
Significant errors (with open sky) are: {satellite position, satellite clock, iono & tropo delays}
ionosphere
troposphere

Figure 1: The components of errors in the GPS system.

Satellite orbit and clock

There are government organizations that have the expertise to compute GPS orbit and clock errors (see, for example, the GDGPS report from the PNTAB, Oct 27, 2021). These organizations observe the satellite signals from a network of GPS reference stations (such as IGS), and then they compute high quality orbits and clock values for the satellites. These can be used as the orbit and clock values for HARS.

Ionosphere

GPS currently broadcasts the Klobuchar ionosphere model to allow single frequency users to correct for ionospheric propagation error. For dual-frequency receivers, the user can directly compute and mitigate first-order ionospheric propagation error. The Klobuchar model is still widely implemented in mass market receivers such as cell phones. The GPS Klobuchar model is underperforming compared to the ionospheric correction broadcasting systems implemented by Galileo, BDS, and QZSS.

Recommendation: In recent years, machine learning has demonstrated improved accuracy in ionospheric TEC predictions with an impressive lead time of up to 72 hours. The machine learning prediction results can be implemented in a relatively coarse grid (say 2.5 degree latitude by 5 degree longitude), this can drastically improve the accuracy (beyond the current BDS and Galileo model performances). Such an implementation will provide the ionospheric corrections for HARS.

Troposphere: Troposphere error can be very well modeled by standard atmosphere parameters. The presence of water vapor poses the largest deviation from the standard atmosphere models and it is a very localized phenomenon. Tropospheric errors can be removed by standard approaches at the receiver, such as estimating zenith tropo delay. This can be assisted by the provision of local temperature, air pressure, and relative humidity. NOAA already provides these parameters at a global scale, and they can be included in the HARS data.

Data delivery:
Correction data should be digitally signed, and made available over the internet. This process will use cryptographic means for authentication to ensure that the HARS data received by the user is actually the real HARS data provided by the HARS service provider (e.g. the US Government or designee thereof).   Such secure connections are well known and supported by current standards that are widely used. The US Government will be responsible for generating and exposing the data to the Commercial Services such as Google, Apple, et al. These commercial services will then have the responsibility of distributing the data to their users, in a similar way to how they currently distribute Assisted-GPS data to phones and other connected devices.

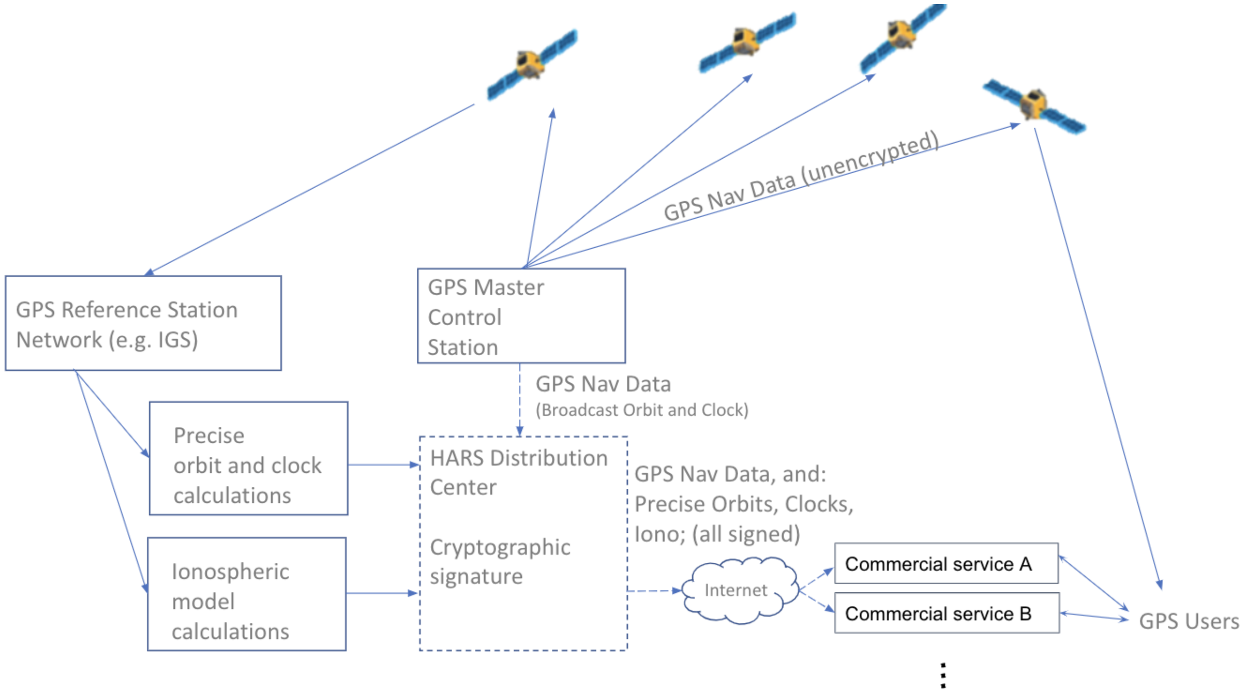
GPS Nav Data (unencrypted)
GPS Reference Station Network (e.g. IGS)
GPS Master Control Station
GPS Nav Data
(Broadcast Orbit and Clock)
Precise orbit and clock calculations
Ionospheric model calculations
HARS Distribution Center
Cryptographic signature
GPS Nav Data, and: Precise Orbits, Clocks, Iono; (all signed)
Internet
Commercial service A
Commercial service B
GPS Users
⋮

Figure 2: Cryptographic data signing and delivery block diagram for the proposed GPS High Accuracy and Resilience Service (HARS). All the components exist except for the block and arrows shown with dashed lines. The HARS service will provide GPS users with much higher security and accuracy of their GPS signals than they currently experience. The US Government will be responsible for generating and exposing the data to the Commercial Services (labeled A,B, … in the diagram) such as Google, Apple, …. These commercial services will then have the responsibility of distributing the data to their users, in a similar way to how they currently distribute Assisted-GPS data to phones and other connected devices.

Recommendation

The GPS system should add a corrections service and digitally signed Nav Data, available over the internet. The HARS system must be funded and have an operator, such as the US Space Force, the Department of Transport, or similar.

References

[1] Space Policy Directive 7 (SPD 7)
https://www.federalregister.gov/documents/2020/12/16/2020-27892/the-national-space-policy

Section 1e https://www.federalregister.gov/d/2020-27892/p-56

"the United States shall … Improve the cybersecurity of GPS [and] its augmentations"

[2] "*A Brief History of GPS L5*" Chris Hegarty, Stanford PNT Symposium, Nov 2010.
[L5 proposed 1995, Signal Specification published 2000, first launch 2010]

[3] "*GDGPS Way-Ahead*." Betz, J., et al.. GDGPS Task Force Report to the 25th Session of the National Space-Based PNT Advisory Board. December 9, 2021. Sheraton Pentagon City Hotel, Arlington, Virginia. https://www.gps.gov/governance/advisory/meetings/2021-12/betz.pdf

[4] "*Who's Your Daddy?, Why GPS will continue to dominate consumer GNSS*", Frank van Diggelen, Stanford PNT Symposium 2013. And: Inside GNSS Magazine Mar-Apr 2014.

[5] NIST lightweight cryptography standard
https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices

[6] Lightweight cryptographic signing https://en.wikipedia.org/wiki/HMAC