Homeland Security

NCCIC
National Cybersecurity & Communications Integration Center

NCC
National Coordinating Center for Communications

Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure

UNCLASSIFIED
TLP: WHITE

Table of Contents

Introduction

Almost every aspect of American life today relies on some aspect of positioning, navigation, and timing (PNT) data provided by the Global Positioning System (GPS) and other Global Navigation Satellite Systems (GNSS).[1] This paper is intended as a Best Practices Guide to be used for Improving the operations and development of Global Positioning System (GPS) equipment used by Critical Infrastructure. This paper is sponsored by the Department of Homeland Security's Science & Technology Directorate in coordination with the Office of Infrastructure Protection and the National Coordination Office for Space-Based Positioning, Navigation and Timing and provides owners, operators, researchers, designers, and manufacturers with information to improve the security and resilience of PNT equipment across the spectrum of equipment development, deployment, and use. Specifically, recommendations consider:

- Installation and operation strategies that can be implemented for current equipment; and
- Strategies that can result in more resilient new and/or improved products based on existing technology and knowledge.

Implementing these recommendations will lead to increased "competence"—that is, equipment that is better able to accommodate imperfections in their inputs, regardless of whether these imperfections are intentional or not. The appendices include observations and interactions with critical infrastructure owners and operators whose insights on their use of PNT information provided significant background for this document; details on the operational benefits of blocking antennas; and research topics where additional information could add to the knowledge of relevant communities and capabilities of equipment using GNSS-provided data for PNT operations.

[1] This document focuses primarily on GPS-based operations. It does not address sources of timing or frequency not provided by GNSS systems (such as Network Time Protocol or Two-Way Satellite Time and Frequency Transfer) in any detail.

Threat/Hazard Characterization

A. Interference and Jamming:

Interference arises from unintentionally produced RF waveforms that raise the effective noise floor in the receiver processing, thus degrading or denying a receiver's ability to operate. Jamming is intentionally produced RF waveforms that have the same effect as interference; the only difference is the intent to degrade or deny a target receiver's operation.

B. Spoofing:

Spoofing is caused by RF waveforms that mimic true signals in some ways, but deny, degrade, disrupt, or deceive a receiver's operation when they are processed. Spoofing may be unintentional, such as effects from the signals of a GPS repeater, or they may be intentional and even malicious. There are two classes of spoofing:

- **Measurement spoofing** introduces RF waveforms that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change.
- **Data spoofing** introduces incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT.

Either type of spoofing can cause a range of effects, from incorrect outputs of PNT to receiver malfunction. The onset of these effects can be instantaneous or delayed and it is possible for effects to continue even after the spoofing has ended.

Installation and Operation Strategies for Owners, Operators, and Installers

Employing the following installation and operation strategies can improve the resilience of equipment receiving and processing GNSS signals. These recommendations focus on steps owners, operators, and third party installers can take, external to the equipment, that can be employed immediately on current equipment. Implementation of these strategies should use best judgement based on application- and site-specific information.

1) **Obscure antennas**. Install antennas where they are not visible from publicly accessible locations or obscure their exact locations by introducing impediments to hide the antennas. For example, installing optically opaque, but electromagnetically transparent, barriers around the area where the antenna is mounted, such as plastic fencing, would visibly hide the antennas, but would not interfere with their operation.
    •
2) **Provide decoy antennas**. Leave or install a clearly visible antenna as a decoy and connect it to a sensor, as indicated in Installation and Operation Strategy 10. Place it in a location that is readily observed from publicly accessible spaces, and far from the actual antenna (300 m would be preferable since that is the "length" of a coarse/acquisition (C/A) signal chip).
    •
3) **Carefully select antenna locations**. Install the true antenna away from (preferably at least 10 m) and at least slightly above nearby structures so the local multipath environment is benign and antenna beam patterns are not distorted. Choose a location where the antenna has an adequate view of the sky. For stationary timing receivers, antennas should have a clear view of the sky in at least a ±30 degree sector around vertical at all azimuth angles. Simultaneously, seek locations where the roof lines or other building structures block RF propagation from the ground and other publicly accessible locations.
    •
4) **Employ blocking antennas**. Blocking antennas not only help protect a receiver from interference and jamming, but can also attenuate spoofing signals.[2] They also help resist knockoff jamming that may be employed to make a receiver more susceptible to spoofing attacks. Stationary timing receivers can use horizon-nulling antennas with fixed reception patterns, while any receiver may benefit from controlled reception pattern antennas (CRPAs) with adaptive antenna electronics. For timing receivers, reference Installation and Operation Strategy 5, "Calibrate" to ensure that the associated bulk delay can be accommodated in receiver calibration and that any delay variation[3] introduced by the antennas and antenna electronics is a small fraction of the needed timing accuracy. See Appendix C for a detailed discussion of the operational benefits of blocking antennas.
    •
5) **Introduce redundancy**. If it is feasible and affordable, install two or three antennas at widely diverse locations (e.g., near different ends of a building or at different locations on a ship). Drive independent receivers from these antennas and compare outputs from these different devices. Significant discrepancies between two such devices, or identical position outputs from spatially distinct antennas, should cause

[2] Blocking antennas are an element of defense. While they do not completely block undesired signals or waveforms, they do attenuate them. This is important since even a relatively low-power interference source located hundreds of meters from the antenna can produce damaging received power levels. For example, 1 mW transmit power received by a -10 dBi receive antenna 500 m away produces approximately -130 dBW received power level (approximately 25 dB greater than the received power of a true signal), assuming free space propagation. Even if the blocking antenna produces an additional 20 dB of attenuation, 100 mW transmitter power produces the same effect from 500 m distance. If a sophisticated spoofed signal is matched to the received power of the true signals, the unknown presence of a blocking antenna will cause the spoofing signals to be received at low enough power that they likely will not affect receiver processing.

[3] Delay variation is a particular concern with adaptive antennas, and needs to be assessed carefully relative to the desired accuracy.)

transition to holdover sources. Develop and test procedures to identify and resolve discrepancies between receivers.

6) **Calibrate**. Determine (through specifications or measurements) the delay characteristics of antenna and antenna electronics, making sure the bulk delay is small enough to be compensated in a timing receiver. Evaluate delay variations—due to thermal effects, aging in fixed pattern antennas and their electronics, and the effects of adaptive anti-jam antennas and their antenna electronics—and ensure they are consistent with accuracy requirements.

7) **Avoid using low elevation signals**. Especially if horizon-nulling antennas are used, timing receivers should not use measurements from lower elevation (e.g., below 25 degree elevation) satellites since those signals are attenuated by the horizon-nulling antennas. Even if horizon nulling-antennas are not used, it may be beneficial to exclude lower elevation angles since they are poorer quality—generally received at lower power and more degraded by propagation phenomena.

8) **Use position hold for stationary timing receivers**. Use timing receivers that operate in position hold mode, making sure they are installed and properly configured (surveyed) to work in this mode. In this mode, they need to receive signals from as few as one satellite in order to provide timing measurements. If the receiver uses timing receiver autonomous integrity monitoring (TRAIM), determine how many satellites the receiver needs for TRAIM and what the receiver's behavior is if it does not receive signals from that number of satellites. If the option exists, it may be preferable for a receiver to operate with only high-elevation satellites, even if TRAIM cannot then be supported.

9) **Employ high-quality holdover devices**. Timing receivers should be backed up by an independent timing source, such as a Rubidium or Cesium clock, that can freewheel with sufficient accuracy for long enough that proper GPS reception can be restored after an incident. Positioning receivers can be backed up with inertial sensors.

10) **Add a sensor/blocker**. Sensors can detect characteristics of interference, jamming, and spoofing signals, provide local indication of an attack or anomalous condition, communicate alerts to a remote monitoring site, and collect and report data to be analyzed for forensic purposes. In addition, if there is an adequate backup or holdover device (see Installation and Operation Strategy 9, "Employ high-quality holdover devices"), a sensor can also protect a receiver by blocking the RF input to the receiver when interference or jamming waveforms or spoofing signals are detected. This blocking limits the potential for any persistent impact on the receiver functionality or performance, and helps ensure handover to an uncontaminated backup or holdover device until the attack or anomaly is removed. If the backup or holdover device can operate with only intermittent disciplining from GPS, then relatively high rates of false detections can be accommodated from a sensor/blocker, while still providing adequate PNT information. Of note, sensor products are currently available, but have not been independently evaluated and characterized and may not address all the threat characteristics of interest.

11) **Practice good cyber hygiene**. Since both the GNSS receiver and any associated processors are computers, and often networked computers, good cyber hygiene, like that used for any other mission critical computer, is essential [5]. Firewalls, virus protection, and other defenses should be installed and maintained. Software patches and updates should be authenticated and then applied promptly. Two-factor authentication, including strong passwords, should be required for access. All factory default and maintenance passwords

should be changed, with passwords regularly updated. If there is no need for continuous network connectivity, it may be prudent to operate without network connection except when it isneeded.

Development Strategies for Manufacturers

Manufacturers should develop and produce future GNSS receivers, along with their integration into different types of equipment, to provide enhanced competence, including robustness and security. This section identifies a set of strategies equipment designers and manufacturers can use for such enhancements. As they consider purchasing of new equipment, owners and operators can use these development strategies to identify capabilities and features which will enhance the resilience of their operations. Of note, in general, the development strategies identified here are based on existing information and proven techniques that merely need to be implemented in products. In contrast, Appendix B identifies topics where more research is needed before results are ready for implementation in products.

1) **Extend data spoofing whitelists to sensors**. Existing data spoofing whitelists have been and are being implemented in government reference software, and should also be implemented in sensors. Sensors should be updated or replaced to implement more comprehensive whitelisting of the legacy navigation (LNAV) message used for C/A signals as they are developed, as well to address any other signals being used. Spoofing detection capabilities should be evaluated against known and emerging spoofing attacks, and updated as needed based on techniques such as those described and referenced in Development Strategy 8, Enhance anti-measurement spoof processing.

2) **Plan for growth**. Receiver and processor hardware and software should be architected and designed for adaptability and growth. Software should be securely upgradeable, with the capability of retaining a current version while downloading a new version that can provide bug fixes, enhancements, and defenses against additional threats. When a new software version is installed, there should be a user-selectable time for switchover to that new version, allowing multiple systems to switch over synchronously. The interface for upgrading the software should be nonproprietary, with full open or government-owned documentation. Software upgrade processes should rely on strong authentication, and, in many cases, it may be desirable for upgrades to be enabled only by a physical setting on the unit. Even after an update is installed and enabled, the receiver and processor should be able to return to the previous software version, if necessary. Ample margin (perhaps at least 50%) should be left in computing resources and storage to accommodate growth in software functionality and size.

3) **Implement software assurance**. Sound software assurance practices should be followed. These practices involve not only software development, but also continued maintenance, including those practices summarized in Installation and Operation Strategy 11, Practicing good cyber hygiene.

4) **Return to known good state**. Software should be written so that the processing returns to a known good state either manually by an external command or automatically if the processing is determined to be in an unacceptable state. For example, software should monitor its own operation for situations, such as endless looping, and command a return to a known good state.

5) **Address all components.** As feasible, the development strategies above would be employed in both the GPS receiver and any associated processor. However, if the GPS receiver is a purchased device and the above strategies cannot be fully implemented in it, they still should be applied in any associated processor.

•

6) **Enable secure remote access and management**. When onsite access and management are not possible or sufficient, it should be possible to securely connect the receiver or associated processor to a network for management (see Development Strategy 2, Plan for growth) and information extraction. Diagnostic information, including the ability to access and download results of instrumentation described in Development Strategy 12, Instrument receivers capture data should be securely accessible from offsite.

•

7) **Enhance anti-jam capabilities**. To the extent possible, the GPS receiver should be specified and developed to provide good anti-jam capabilities so that it can operate through high received levels of interference and jamming. Adaptive analog-to-digital conversion [7] can provide benefits against some types of interference or jamming. Narrowband interference excision techniques are highly desirable and could even be included as an applique if desired. Similarly, signal processing that suppresses constant modulus interference or that estimates and subtracts structured interference or jamming can be included in the receiver processing, or even in an applique. High-sensitivity acquisition processing using long coherent integration times and many noncoherent integrations, with code Doppler compensation as needed, should be provided. Robust signal tracking algorithms should be employed using narrow loop bandwidths, including the use of carrier-aided code tracking. Stationary timing receivers should be able to use particularly small loop bandwidths once they have acquired signals and initiated tracking. Cross-signal aiding in signal tracking, such as vector-locked loops, can also be used for increased robustness. Receivers for mobile applications can be equipped with inertial sensors, enabling coupling (loose, tight, or ultratight) between signal tracking and inertial sensors.

   If low C/N_0 causes the receiver to lose lock, the receiver should follow prudent steps during reacquisition. For example, it should limit its signal search to as small an initial time uncertainty (ITU) and initial frequency uncertainty (IFU) as possible (guided by high-quality time and frequency information from the holdover device) and perhaps temporarily use more sensitive thresholds in anti-measurement spoofing and anti-data spoofing as discussed below. The receiver should scan the entire ITU and IFU, recognizing and reporting the existence of multiple signals having the same spreading code, since such an event likely indicates the presence of spoofing signals.

- In addition, the receiver processing the signals should recognize and report the presence of interference and jamming. Recognition can be as simple as monitoring for significant changes in the RF power (using a J/N meter or equivalent) and for changes in effective C/N_0. Reports of interference should be provided at the output interface of the receiver, and also passed to the anti-spoofing logic. Once interference or jamming has vanished, it can be prudent to delay reacquiring the signal for many minutes or hours, depending on the ability of the holdover source, in order to reduce the potential for acquiring spoofing signals during reacquisition.

8) **Enhance anti-measurement spoof processing**. To the extent possible, the GPS receiver should be specified and developed to provide good anti-measurement spoofing—recognizing, rejecting, and reporting spoofing signals that cause the receiver to produce erroneous time of arrival measurements or frequency of arrival measurements. Upon recognition and reporting of spoofing signals, the unit should hand over to a backup sensor (precision clock, inertial sensors). Examples include:
   - Calculating and inspecting the cross-ambiguity function (CAF) between the input waveform and each true signal in order to detect the presence of spoofing signals. This processing can happen during acquisition and also periodically during tracking. This CAF computation should cover the ITU and IFU over which valid signals are expected.
   - Inspecting the combination of RF power levels and reported C/N_0 levels or, if possible, received signal power levels to identify anomalous values or changes in signal power levels.
   - Inspecting RF power levels to identify either sequential or concurrent knockoff jamming.

- Implementing acquisition processes such as, keeping the ITU and IFU ranges as small as possible, guided by holdover from high-quality time and frequency sources (larger ranges can be searched for the presence of spoofing signals).
- Narrowing the time and frequency dimensions of tracking loop pull-in regions as tracking loops converge.
- Implementing multipath mitigation, such as narrow early-late spacing, correlation function shape tests, double-delta and related processing, and multipath-mitigation techniques based on parameter estimation, to discriminate against spoofing signals— even when spoofing signals are spaced close to true signals in delay.
- Inspecting position and time outputs using measurements, as available, for anomalous values or changes.
- Exploiting characteristics of specific receivers: For stationary timing receivers using GPS signals, take advantage of the repeating ground track of GPS satellites to store received power levels from each satellite over time and comparing newly received power levels to the reference values. Unless there has been a change or anomaly in the satellite or receive antenna, very tight correspondence should be obtained to facilitate the detection of spoofing signals received at distinctly different signal power levels.
- Using measurements from multiple antennas that are spaced on the order of 10 wavelengths apart to detect that different signals are arriving from the same direction and thus are likely to be spoofing signals. (Where feasible in mission-critical applications,)

Algorithms that recognize and reject measurement spoofing may need adjustment if employed on a receiver protected with a horizon-nulling antenna. Here, signals from satellites at low elevation angles may not be available at adequately high C/N_0. Even so, it may be useful to attempt to calculate position and velocity solutions even in position hold mode. The resulting positions and velocities, computed only when enough satellites are in view, would not be output by the receiver, but could be employed within the receiver to help detect measurement spoofing.

9) **Implement anti-data spoofing**. Receiver software should be modified to implement anti-data spoofing using whitelists that describe valid message contents. Anti-data spoofing should inspect data message contents before the message is used. If it is not possible to implement anti-data spoofing in the receiver software, it is highly desirable that the receiver provide data message segments at its output so that an integration processor can then perform anti-data spoofing. In either case, the anti-data spoofing software should recognize, report, and reject illegal and invalid message contents, and recognize and report with suspicious state information. No data should be stored, output, or used until it has passed the anti-data spoofing inspection. Upon recognition and reporting of data spoofed signals, the timing unit should temporarily stop processing signals and outputting PVT information and, if possible, hand over to a backup device for a prudent period of time. While suspicious information should be recognized and reported, deciding how to respond to this information must be determined based on the specific application and the availability of backup devices. Government reference software that implements whitelist checking should be used to guide implementation and to verify operation of anti-data spoofing.

10) **Use more GPS signal types.** Modernized civil GPS signals are more robust than the L1 signal and should be leveraged for increased resistance to interference, jamming, and spoofing. By the end of calendar year 2015, the GPS L2C signal was transmitted by more than half the GPS constellation, making at least one L2C signal typically available continuously everywhere on earth. The GPS L5 signal will also be available within a few years. The GPS L1C signal will start being broadcast by 2017. There is much less chance that accidental interference will affect all signals on multiple carrier frequencies. Jamming and spoofing are also made more

complicated for attackers as long as the signals are properly used in the receiver. The forward error control and data demodulation error protection using cyclic redundancy checks, available in all these modernized GPS signals, also make data spoofing more difficult, while the wider root-mean-square (RMS) bandwidths of L5 and L1C facilitate multipath mitigation, which can assist in detecting and discriminating against measurement spoofing. While this step is listed as a development strategy, it must be paired with the extended whitelist work described in Appendix B and with techniques that exploit consistency across multiple signals in mitigating measurement spoofing.

11) **Instrument receivers capture data**. To support both debugging and forensic analysis, receivers should capture data when they detect anomalous situations. Currently, many receivers capture and provide little or no information when anomalous situations occur, making identification of the anomaly and its cause a guessing game unless the anomaly is repeated when instrumentation is available. Demodulated data message bits, measurements or observables, and RF power levels can be continuously stored in nonvolatile memory, then overwritten after several minutes unless an anomaly has occurred. If a software anomaly is automatically detected and operation is returned to a known good state (see Development Strategy 4, Return to known good state), the characteristics of this anomaly and other relevant information should be captured. While the capacity may not exist for recording waveform information in a receiver, it may be possible to capture some spectral and power information that could be used to characterize jamming attacks.

Research Opportunities

The following topics explore areas where further research is needed to develop techniques and strategies to enhance resilience efforts in civilian use of GNSS signals for PNT-related operations.

1) **Extended whitelists and associated government reference software**. Additional whitelists need to be developed beyond the existing whitelist for the C/A signal's LNAV message. There are additional ways to confirm consistency over time and among satellites in order to aid recognition of illegal and invalid entries, as well as incorrect states. Corresponding whitelists should be completed for Satellite-Based Augmentation System signals, as well as for the modernized GPS signals: L2C, L5, and L1C. Open signals from other GNSS systems (GLONASS: L20F, L3OC, and in the future L1OC and L2OC; Galileo: El OS, E5a, E5b; BeiDou: B1I, B2I, B1C, B2a, B2b) are to be used for diversity, and whitelists need to be developed for each of them. In addition, whitelists are needed for standard data interfaces to receivers. Finally, there are significant benefits to development of government reference software implementations of these whitelists to expedite adoption and implementation of anti-data spoofing techniques, while lowering developers' risk and nonrecurring costs.

2) **Generalize blocking antenna polarization**. Initial development and assessment of blocking antennas has emphasized the rejection of interference, jamming, and spoofing signals that have right-hand circular polarization, just like GNSS signals. However, recent testing indicates that in some cases the blocking antennas are less able to reject undesired waveforms with other polarizations, including the commonly used linear polarization. Developing and assessing blocking antennas that provide enhanced performance against waveforms that are elliptically polarized or linearly polarized with any orientation, and even left-hand elliptically or circularly polarized, would be a considerable benefit. Preliminary designs have been evaluated and determined to be promising.

3) **Exploit other sources of data messages**. Alternative sources of clock and ephemeris data should be sought for use in crosschecking or replacing the digital data modulated onto the broadcast signals. Several options have been identified and still need to be explored and refined. One such option is obtaining trusted ephemeris

or data messages directly from the GPS control segment. Another approach would be to obtain assured long-term ephemeris that is produced by nongovernment organizations, including providers of assisted GNSS services or the International GNSS Service. An attractive option for some applications may be the nine-day GPS ephemeris currently offered by the National Geospatial Intelligence Agency. Available and assured data can be used either to verify correctness of values in data messages read from the broadcast signals, or to replace information read from broadcast data messages. In either case, research is needed to mature and harden such capabilities, to handle unexpected changes in status of signals or satellites, to identify and address other such anomalous situations, and to mature the assured provision of this information to receivers. There would be significant benefits, in terms of developer cost and risk as well as time to market, from government reference software that exploits other selected sources of data messages.

4) **Reduce latency in recognition and reporting of interference, jamming, and spoofing**. If a receiver is misled by an attack before the attack is recognized and reported, then backup devices may be corrupted by the receiver before hand over. Developing and testing low-latency approaches, as well as strategies for a clean handover before backups are corrupted, are important topics to pursue. As one example, in a sensor/blocker there are benefits to inspecting data message bits as they are demodulated, rather than waiting for the entire word to be demodulated. This way, spoofing signals can be more quickly blocked from the protected receiver.

Summary

This guidance document identifies 22 specific recommendations for receivers and equipment today and existing techniques that can be inserted into new products. These installation and operation strategies and development opportunities described herein can significantly enhance the ability of GNSS receivers and associated equipment to defend against a range of interference, jamming, and spoofing attacks.

References

1. New York State Enterprise Information Security Office, “Cyber Hygiene with the Top 20 Critical Security Controls,” at https://its.ny.gov/newsletter/cyber-hygiene-top-20-critical-security-controls, accessed 6 April 2016.
2. Jared Ablon and Drew Buttner, "Global Positioning System (GPS) Receiver Software Assurance Best Practices," The MITRE Corporation Document, 29 September 2015.
3. Frank Amoroso, "Adaptive A/D Converter to Suppress CW Interference in DSPN Spread-Spectrum Communications," IEEE Transactions on Communications, Vol. 31, No. 10, pp. 1117-1123.
4. Ryan Dougherty and Timothy Kurp, "GPS Spoofing Detection for Resource-Constrained C/A Code Receivers, Part 2: Practical Implementations for Stationary Receivers," The MITRE Corporation Technical Report MTR150145V2, November 2015.
5. Blanch, Juan, et al., "Advanced RAIM User Algorithm Description: Integrity Support Message Processing, Fault Detection, Exclusion, and Protection Level Calculation," Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, September 2012, pp. 2828-2849.
6. E. McMilin, et al., "Single Antenna, Dual Use: Theory and Field Trial Results of Anti-jam and Spoof Detection," lnsideGNSS, September/October 2015, pp. 40-53.
7. J. D. Parsons, The Mobile Radio Channel, Second Edition, Wiley, 2000.
8. William C. Stone, "Electromagnetic Signal Attenuation in Construction Materials," NISTIR 6055, NIST Construction Automation Program, Report No.3, October 1997.
9. Eustace K. Tameh and Andrew R. Nix, "The use of measurement data to analyze the performance of rooftop diffraction and foliage loss algorithms in a 3-D integrated urban/rural propagation model," IEEE Vehicular Technology Conference, May 1998.
10. National Space-Based Positioning, Navigation, and Timing Systems Engineering Forum (NPEF), Follow-on Assessment of LightSquared Ancillary Terrestrial Component Effects on GPS Receivers, 6 January 2012.

Appendix A Observations from Site Visits with Critical Infrastructure Owners and Operators

A.1 Background:

- This appendix summarizes observations and findings from a series of site visits and conversations with critical infrastructure owners and operators who used GPS in communications, electric power generation and transmission, and various aspects of financial operations.

These engagements focused on installation and use of PNT equipment, although additional insights were obtained concerning the need for information derived from GNSS signals, and the effect of incorrect or missing GNSS signal-derived information. Visits with owners and operators only observed reception of the GPS coarse/acquisition (C/A) signal, rather than other GPS signals or signals from other GNSS systems.

A.2 Observed Common Themes:

Owners and operators of the critical infrastructure facilities visited have varying degrees of awareness concerning the capabilities of GPS and GPS-related vulnerabilities and mitigations. Since owners and operators are not GPS experts, they depend heavily on suppliers of the equipment they purchase and install for such awareness. The following are common themes from these site visits:

- There is widespread use of GPS for timing, with current timing accuracies for most applications on the order of milliseconds (10^{-3}) or larger, over local extent in some cases and global extent in other cases. In the future, timing accuracy needs may approach or be less than one microsecond (10^{-6}). However, the ability to provide such accuracy without GNSS-provided PNT data over the needed geographical extent varies. It is unclear how or whether graceful degradation will occur in the absence of such time accuracy.
- Current GPS installation and operation strategies can be improved. Limitations on current practices are generally due to lack of awareness since owners and operators are interested in improving current practices.
- In most cases examined, if GPS receivers are unable to provide time for critical applications, holdover or fallback capabilities can continue to provide adequate time for days or weeks as long at the holdover or fallback device is functioning appropriately.
- Owners and operators experience GPS outages (if only due to equipment failure) and have successfully operated through GPS outages.
- The effects of losing GPS appear to be gradual and not catastrophic; loss of GPS produces degraded capabilities and eventually denial of service rather than erroneous outputs. Localized impacts would likely precede effects over a wider geographic area.
- Much more attention is paid to interference and jamming and their effects than to the full spectrum of spoofing attacks.

- These findings indicate the needs for increased time accuracy are evolving along with methods of achieving that increased accuracy. In anticipation of these needs, there appear to be opportunities to not only make PNT-related operations more secure and resilient, but also ensure that timing accuracy requirements do not exceed what can be securely and effectively provided. Further, strategies should be put in place to ensure that, when these tighter timing accuracy requirements are not met, there is gradual, rather than sudden, degradation of capability.

Appendix B Operational Benefits of Blocking Antennas for Civil GNSS Applications.

B.1 Background

For many years, GNSS receive antennas have been developed and evaluated to block or attenuate undesired radio frequency (RF) waveforms, whether interference or jamming waveforms, or spoofing signals.
Since the received power of desired GNSS signals is significantly less (typically at least 10 dB lower) than the noise power in a receiver front end, any input whose power is greater than this noise power is undesired and potentially harmful. The simplest blocking antennas conceptually are horizon-nulling antennas that attenuate all inputs from lower elevations. These are most suited for stationary timing receivers that need signals from only one or several satellites that can typically be found at high elevations. More sophisticated blocking antennas include adaptive antennas that use an array of multiple antenna elements (commonly known as a controlled reception pattern antenna, or CRPA), combined with sophisticated signal processing of the array outputs, to attenuate input waveforms whose power exceeds the noise power. These can be used in applications where the receiver is moving, and also in positioning applications where it is desirable to receive true signals from lower elevations. Other blocking approaches, such as [10], are also available for specific applications.
Blocking antennas provide different levels of attenuation, depending on a number of factors, including their design, the polarization of the interference, their ability to function in one or more frequency bands, and various geometry factors. In some cases, in addition to the attenuation provided by a blocking antenna, additional attenuation may be provided by buildings, fences, or other structures shadowing the undesired waveforms.

B.2 Propagation Models

RF propagation behaves very differently at different frequencies and in different environments. For the L band signals considered here, a classic reference on propagation models is [11]. Extensive data on excess attenuation from building materials is provided in [12], while foliage attenuation and other effects are discussed in [13]. This appendix does not examine the effects of building materials, structures, and foliage.

While the calculations in this appendix are frequency-dependent, showing different results at different L band carrier frequencies, real-world uncertainties caused by other considerations dominate the variations due to different L band frequencies, so all results are provided at the most commonly used GNSS carrier frequency, 1575.42 MHz.

Both for simplicity and because of the context, this appendix focuses primarily on conditions that could lead to relatively low propagation losses producing larger levels of undesired RF power at the receiver. Of course, an attacker trying to insert undesired RF signals must either know the exact propagation conditions and receive antenna gain, or provide additional power margin to overcome propagation losses that can be much larger than predicted here, particularly in urban conditions and when antennas are near the surface of the earth.

The standard propagation loss model is based on a free-space assumption, where the electromagnetic waves propagate through a vacuum from the source to the receive antenna, interacting with no objects along the path. An alternative propagation model is based on the assumption of Earth as flat and conductive, assessing the interaction between two propagation paths—the direct path and the reflection from the Earth's surface. Results from this two-ray model depend upon the height of the transmit antenna and the receive antenna. Real-world results, such as [13], show that propagation loss between terrestrial transmitters and receivers can be as small as predicted by these two models, while also being significantly larger sometimes. Thus, it seems prudent to use the free-space and two-ray models for these conservative assessments.

Figure C-1 shows propagation loss using the free-space and two-ray propagation loss models for several different conditions. Free-space losses depend upon frequency, vary smoothly with the square of range, and only apply when transmit and receive antenna heights are not relevant. Two-ray propagation losses can be both larger and smaller than predicted using the free-space model, but are never smaller than 6 dB less

than free space. When either or both of the antennas are elevated from the ground, the two-ray losses fluctuate significantly with small changes in range, as the two rays constructively and destructively interfere. When both antennas are close to the ground, the two-ray propagation loss is independent of frequency and varies smoothly with fourth power of range. Other models for terrestrial propagation would predict greater propagation losses than shown here.

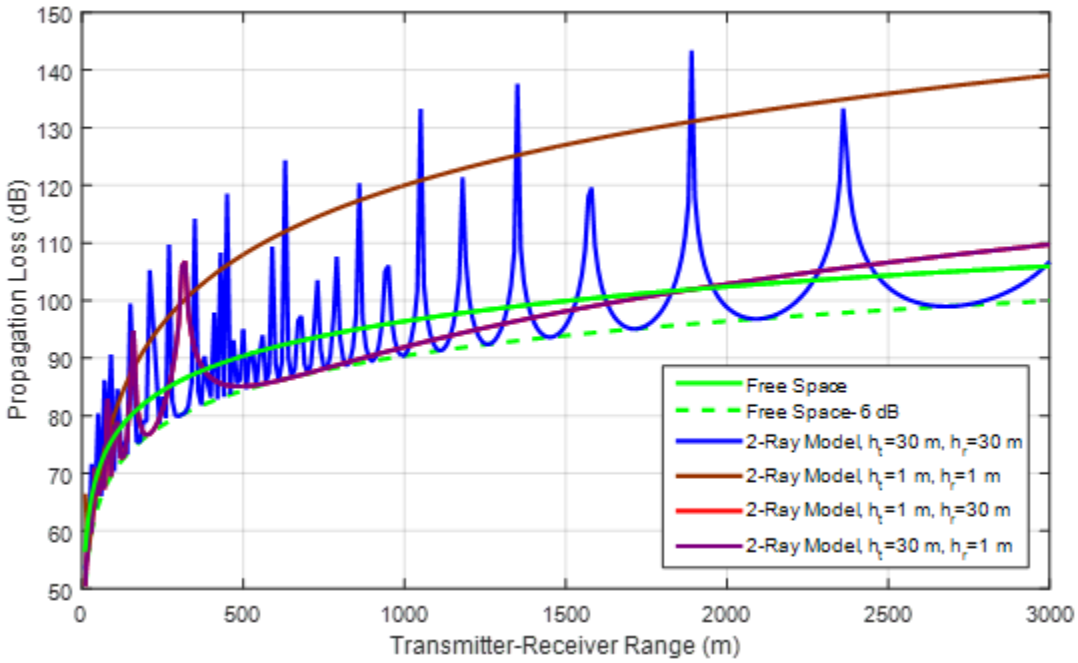

Figure B-1. Comparison of Propagation Losses Computed Using Free-Space Model and Two-Ray Model for Different Transmit Antenna Heights, h_t, and Receive Antenna Heights, h_r.

Based on these results, the performance predictions in subsequent sections employ the free-space propagation loss model. It is important to remember, however, that losses may be somewhat less than predicted, producing up to six dB greater received power than predicted using this model. At longer ranges than shown in Figure C-1, however, it would be rare for conditions involving terrestrial transmitters and receivers to be well modeled by any of these results, and greater propagation losses would typically be observed.

B.3 Blocking for Mitigation of Interference and Jamming

It is commonly stated that interference or jamming having received power 24 dB greater than the received power in desired signals can deny operation of a C/A signal receiver. In reality, such a conclusion depends on the power spectral density (PSD) of the interference or jamming, the specific receiver processing techniques used, and the mode in which the receiver is operating (e.g., acquisition, code tracking, carrier aided code tracking, data demodulation). Once receivers have acquired and are tracking signals, many modem receivers can tolerate interference and jamming almost 30 dB greater than the received signal power, and some high-sensitivity receivers can maintain track even with considerably higher power interference and jamming than this.

In addition, while the minimum specified received power for C/A signals is -158.5 dBW, this power is specified under worst case conditions. Often the signal is transmitted at higher power than minimum, undergoes less propagation loss and polarization loss than worst case, and may benefit from some receive antenna gain.

For illustrative purposes, consequently, this appendix uses received signal power of -155 dBW and a tolerable jamming threshold 25 dB higher than that, or -130 dBW. As noted above, some C/A signal receivers in some

operating modes may be able to tolerate -120 dBW or more of interference power.

Blocking antennas can produce two distinct effects. One effect can be gain in the direction of desired signals. The other effect can be attenuation in the direction of undesired waveforms such as interference, jamming, or spoofing. The blocking ratio quantifies the ratio between the blocking antenna's gain in the direction of undesired waveforms and the blocking antenna's gain in the direction of desired signals. In most applications involving interference, jamming, or spoofing, the blocking ratio is a useful metric, relating the amount that undesired waveforms are attenuated relative to desired signals. In some cases, however, when received signal or waveform power must be related to the thermal noise power spectral density, the gain itself must be considered. In the remainder of this appendix, the blocking ratio is used as if the gain toward desired signals is 0 dBi, and received power of undesired waveforms is attenuated by the blocking ratio.

Suppose the receive antenna does not attenuate the received interference or jamming at all, so the blocking ratio is 0 dB. (For reference, some commercial antennas approach this characteristic even at the horizon.) Then the received interference or jamming power is shown in Figure C-2, assuming free-space propagation. A small 1 mW transmitter produces received power exceeding -130 dBW out to almost 1,500 m range, and even a 0.1 mW transmitter produces this received power at ranges closer than 500 m, if the propagation loss is similar to that of free-space propagation.

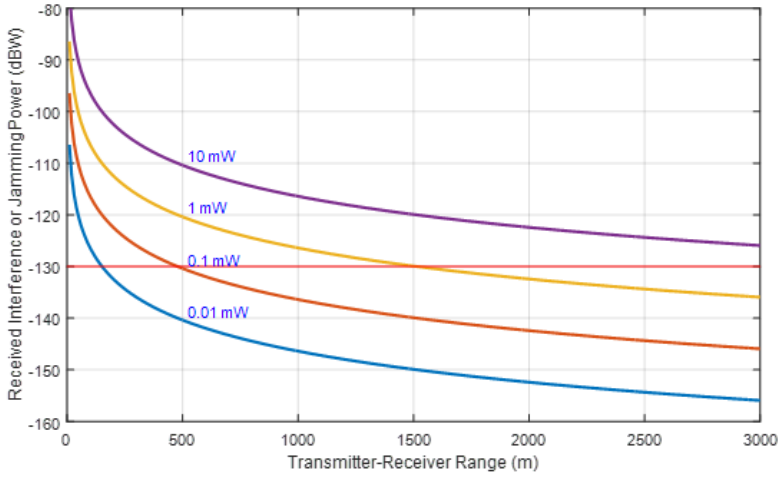

Figure B-2. Received Interference or Jamming Power with 0 dB Blocking Ratio, Assuming Free-Space Propagation

With -30 dB blocking ratio, the received interference or jamming power is greatly reduced, as shown in Figure C-3. Even a 10 mW transmitter produces received power exceeding -130 dBW only at ranges of several hundred meters, and lower power transmitters must be very close—perhaps within a physical security boundary. While it would not be difficult to transmit at power levels higher than 10 mW, a transmitter designed in anticipation of a 0 dB blocking ratio antenna might not have that power, or might not be operated close enough to the target receiver.

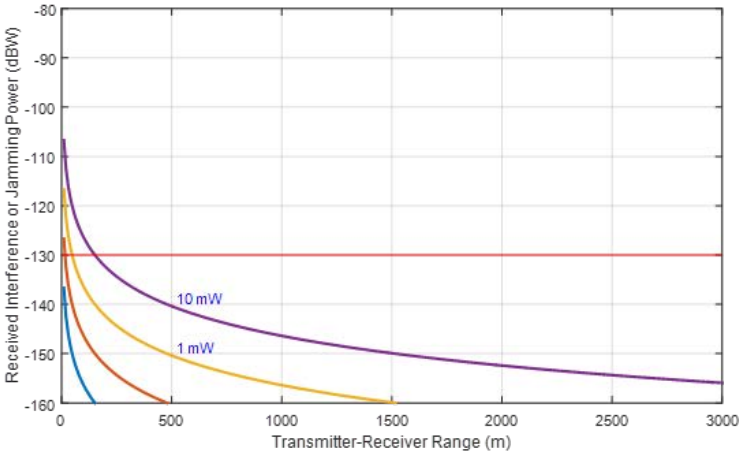

Figure B-3. Received Interference or Jamming Power with -30 dB Blocking Ratio, Assuming Free-Space Propagation

It may not be possible to obtain a -30 dB blocking ratio. Figures C-4 and C-5 show equivalent results for blocking ratios of -20 dB and -10 dB, respectively. Although the -130 dBW threshold is crossed at larger ranges than with -30 dB blocking ratio, with -20 dB blocking ratio the source of interference or jamming must be one-tenth the range (compared to a 0 dB blocking ratio antenna) to produce the same received power. To operate at the same range, the interference or jamming source must have 100 times the transmit power, but this is still a relatively small value.

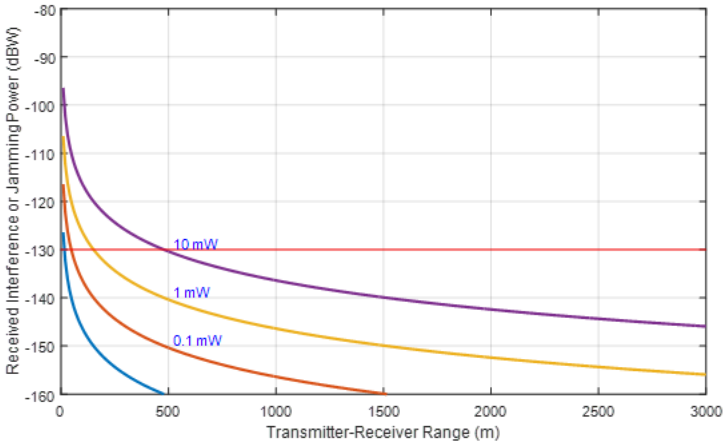

Figure B-4. Received Interference or Jamming Power with -20 dB Blocking Ratio, Assuming Free-Space Propagation

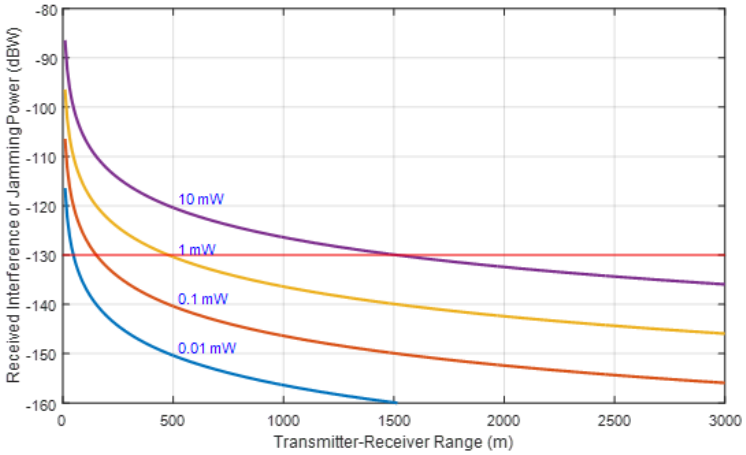

Figure B-5. Received Interference or Jamming Power with -10 dB Blocking Ratio, Assuming Free-Space Propagation

A very sophisticated blocking antenna might achieve a -40 dB blocking ratio. Even with this exquisite performance, a 1 W transmitter would still produce greater than -130 dBW of received power at a range of 500 m. Thus, it is clear that blocking antennas do not constitute, by themselves, an adequate defense against interference or jamming. Many combinations of reasonable transmit power levels and ranges to the receiver can still cause incapacitating levels of received interference or jamming.

However, there are still benefits of blocking antennas. With 20 dB of additional blocking ratio and free-space propagation, the radius of damage from a given interference or jamming source is reduced by a factor of 10. For example, the reported 0.5 W of interference in the GPS band from a Navy ship in San Diego harbor on January 22, 2007, would have caused harmful interference to many fewer (perhaps only 1%) GPS receivers had they been protected by antennas having -20 dB blocking ratio. Further, attackers intending to do harm to GPS reception might not provide enough power in their transmitters or operate close enough to receivers to have an effect. In addition, attackers that provide higher power transmitters in response to blocking become an easier target for spectrum enforcement. Clearly, blocking antennas can contribute to a layered defense-in-depth strategy against interference and jamming, but are not a panacea.

B.4 Blocking for Mitigation of Spoofing Signals

Spoofing signals must be accepted by the target receiver processing as valid before they can affect the receiver or its PVT solution. Not only must they use an appropriate signal format (such as center frequency, spreading modulation, spreading code, data message format, etc.), but they are also most likely to be accepted by a receiver as valid signals when they are received at values of delay, frequency shift, and signal-to-noise ratio close to those of true signals.

If the spoofing signals are accompanied by simultaneous knockoff jamming to deny reception of the true signals while maintaining realistic C/N_0 of spoofing signals, then the results in Section C.3 apply. Otherwise, it is expected that spoofing signals should be received at slightly higher power than that of the true signals, but not at high enough power to be rejected by receiver logic or to be incompatible with receiver processing (saturating analog components or exceeding the dynamic range of digital processing). Acceptable received power levels for each spoofing signal, when unaccompanied by simultaneous knockoff jamming, might be in the range of -150 dBW to -130 dBW.

The results shown in Section C.3 indicate that low-power transmitters can produce received power levels of -150 dBW to -130 dBW even at relatively long ranges. Even if 10 spoofing signals must be transmitted, raising the total transmitted power by 10 dB over that for each signal, the total transmitted power levels need simple amplifiers and transmit antennas.

These small received power levels are similar to or less than the thermal noise power at a receiver input (depending upon receiver noise figure and precorrelation bandwidth). For example, a receiver with thermal noise power spectral density of -201.5 dBW/Hz and 4 MHz precorrelation bandwidth experiences thermal noise at the input of -135.5 dBW. Consequently, adaptive antennas designed to place antenna nulls in the direction of interference and jamming typically would not recognize and react to spoofing signals whose received power levels are less than -135 dBW. Horizon-nulling antennas, however, would continue to mitigate these spoofing signals, if they are transmitted from near the ground, since these antennas attenuate all RF waveforms received at low elevation angles.

Blocking antennas that attenuate spoofing signals can provide a distinct benefit. Attackers may desire to provide spoofing signals at received power levels close to those for true signals. If the attacker is unaware of the existence of a blocking antenna, then the attacker may transmit the spoofing signal at too low a power level for it to have an effect on the target receiver. Even if the attacker is aware of a blocking antenna, unless the blocking ratio is known, the attacker may transmit the spoofing signal at too high or too low a received power level for the spoofing signal to have an effect on the target receiver. Here again, the blocking antenna is not a panacea, but can contribute to defense in depth.

B.5 Blocking's Benefits to Sensing

Now suppose another layer in the defense in depth is a sensor that detects interference and jamming waveforms, as well as spoofing signals. A detection could lead to several actions, including:

- Immediately blocking the RF input to a protected receiver, causing that receiver to fall back to another PNT technology such as an atomic clock or IMU;
- Alerting a local or remote entity that interference, jamming, or spoofing have been detected;
- Capturing and storing data that characterizes the interference, jamming, or spoofing signals for forensic analysis.

Using a standard antenna, rather than a blocking antenna, for the sensor leads to a very beneficial situation. If the attacker takes steps to deliver higher power in order to overcome the blocking antenna's blocking ratio and achieve the desired effect on the target receiver, then the sensor will observe the interference, jamming, or spoofing signals at 10, 20, or 30 dB higher power than the power entering the target receiver. At that elevated power, the sensor can more reliably recognize the interference and jamming waveforms, or spoofing signals, and capture high-fidelity data for forensic analysis. Thus, a blocking antenna makes associated sensing much more reliable and capable.

B.6 Summary and Additional Considerations

This analysis shows that blocking, by itself, cannot be relied upon to defeat interference and jamming waveforms, or spoofing signals. Even when the blocking antenna has a large blocking ratio, modest levels of transmit power at modest range to the target receiver can overwhelm the effects of a blocking antenna.
However, blocking antennas do contribute to a layered defense in depth. Blocking antennas can greatly reduce the range at which receivers are affected by unintentional interference; if widely used, they would significantly lower the number of receivers affected by this interference. Further, receivers would be less affected by some jamming events, such as personal privacy jammers in vehicles on a nearby road or highway.
When an attacker is targeting a receiver, if the attacker is unaware of the presence or performance of a blocking

antenna, the transmitted power of the jamming or spoofing signals may be insufficient to affect the targeted receiver. If the attacker is aware of the blocking antenna, overcoming the additional attenuation causes the attacker to transmit at higher power, or closer to the target receiver's antenna. These reactions to the blocking antenna can make it easier to detect, locate, and apprehend the attacker.

List of Figures

Appendix C. Acronyms

CAF	Cross-Ambiguity Function
CRPA	Controlled Reception Pattern Antenna
C/A	Coarse Acquisition
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IFU	Initial Frequency Uncertainty
ITU	Initial Time Uncertainty
LNAV	Legacy Navigation
PNT	Positioning, Navigation, and Timing
PSD	Power Spectral Density
PVT	Position, Velocity, and Time
RF	Radio Frequency
TRAIM	Timing Receiver Autonomous Integrity Monitoring