WHITE PAPER

GNSS Signal Spoofing

How to Evaluate the Risks to Safety-Critical and Liability-Critical Systems

KEYSIGHT

Introduction

Signal spoofing was once considered a niche and unlikely risk for commercial users of global navigation satellite systems (GNSS). Transmitting fake GNSS signals to force a receiver into reporting an inaccurate time and position could only be done by radio frequency (RF) experts and needed expensive equipment. For that reason, almost all spoofing incidents documented prior to 2015 were conducted either for academic research or for nation state-level electronic warfare.

Since 2015, however, the emergence of low-cost, software-defined RF signal generators, combined with a growing awareness of spoofing as a powerful disruption technique, has seen the number of incidents increase. At the same time, commercial organizations are becoming more reliant on GNSS-based positioning, navigation, and timing (PNT) systems, making spoofing a growing threat to safety-critical and liability-critical operations.

This paper will review the threat to users of commercial GNSS receivers from spoofing at the RF level. It will set out how developers and integrators of GNSS receivers can assess the risks to their products and to their end-users' operations and will provide advice on implementing and testing spoofing detection and mitigation measures.

A sample test will show how a receiver's vulnerability to spoofing can be assessed in the lab. Finally, the paper will explain how Keysight can help with any aspect of spoofing vulnerability testing.

Review of Current Threats

Overview

At the DEFCON hacker conference in Las Vegas in 2015, Huang Lin and Yang Qing of antivirus firm Qihoo 360 demonstrated a low-cost, easy-to-use GNSS signal spoofer built with a software-defined radio (SDR) and open-source code downloaded from the internet. Overnight, it changed the threat landscape for commercial users of GNSS receivers. Spoofing was no longer a difficult and little-known technique for manipulating civilian GNSS signals. Now, anyone with a couple of hundred dollars and an internet connection could build a working spoofer.

From 2016 onward we started to see increased general awareness of GNSS spoofing, particularly with the advent of location-based smartphone games like Pokémon GO. Attempts to manipulate the game evolved in just six weeks from very primitive spoofing (rotating cell phones on ceiling fans) to much more sophisticated techniques employing RF constellation simulation.

Other recent spoofing incidents have ranged from localized attempts by criminals to outwit law enforcement, to large-scale, almost certainly state-sponsored initiatives like the spate of incidents reported in Moscow in 2016 and the Black Sea in 2017. In 2019, ships entering the Port of Shanghai found their positions being spoofed onto the radius of a circle — a new and as-yet unexplained pattern that has since also been observed in Iran and the United States.

Depending on the equipment used, the range of a spoofing attack can be very wide — many miles in some cases. This creates a high risk of collateral damage, with unprotected receivers easily being disrupted or disabled by an attack intended for a different target. For that reason, receiver developers and integrators should give serious consideration to the possibility of collateral damage when assessing the risks of spoofing to their products and end-users.

Spoofing Equipment

It is important to understand the types of equipment that can be used to conduct GNSS spoofing attacks. Spoofing equipment can range from cheap and widely available SDRs typically used by low-level hackers, to highly sophisticated RF signal generators more often used by nation states.

An example of the kind of spoofing equipment that can be built with basic, off-the-shelf components is shown in Figure 1.

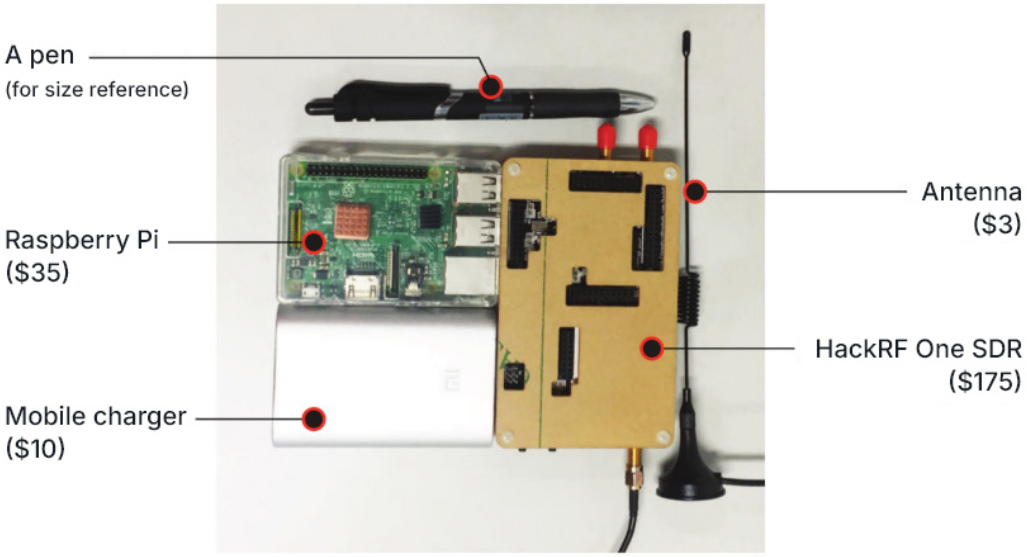


Figure 1. A low-cost spoofer based on SDR architecture made by Virginia Tech for their spoofing investigations

Similarly, code and instructions for creating an RF signal generator using an SDR are easily accessible online, as Figure 2 shows.

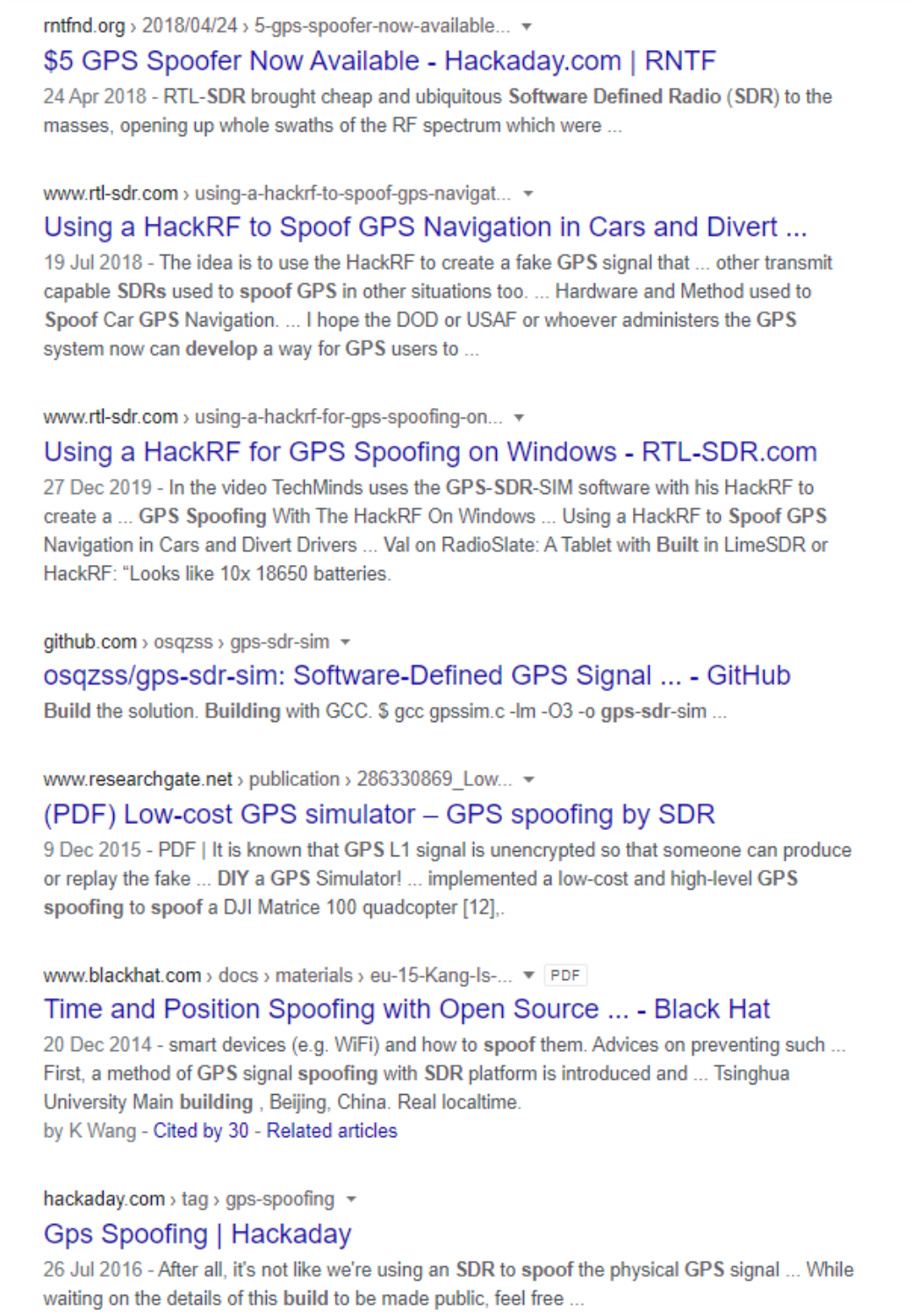


Figure 2. A few of hundreds of search results for "building an SDR GPS spoofer

Types of Spoofing Attack

A GNSS spoofing attack can be carried out in a number of different ways, depending on the intentions of the attacker, the equipment and knowledge at their disposal, and the financial resources available to them. The five primary types of attack are as follows:

Meaconing: The re-transmission of authentic GNSS signals to a target receiver. If the meaconing attack is successful, the target receiver will report the position contained in the re-transmitted data rather than the true position. Legitimate use of GNSS repeaters and pseudolites can result in unintentional transmission of spoofed signals if the devices are not sufficiently isolated, making meaconing the only way that spoofing can occur unintentionally.

Code / carrier attack: The attacker replicates GNSS signals using an RF signal generator. The aim is to align the replica signals to the authentic signals being received by the target receiver before increasing the power to take control of the target receiver tracking loops.

This power level adjustment is critical to the detection of spoofing attacks, as abrupt power level changes are usually a good indicator that untoward activity is occurring. Once the receiver's tracking loops are locked onto the replica signals, an attacker can manipulate the fake code and carrier signals to force the target receiver to report an incorrect position (see Figure 3).

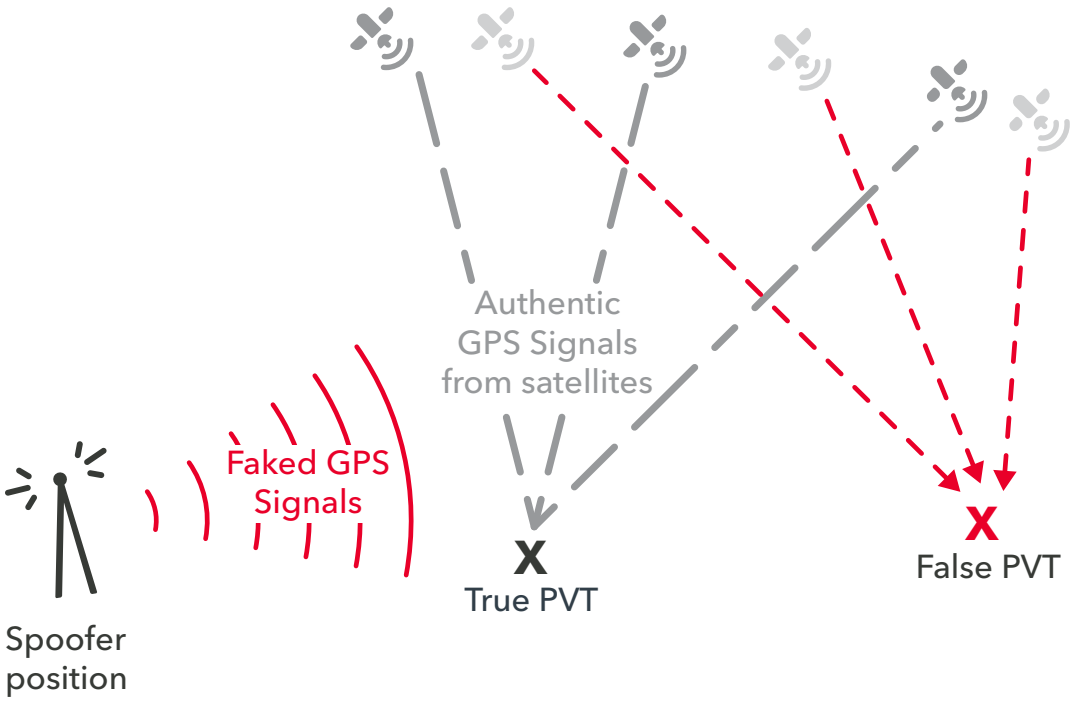


Figure 3. A GPS spoofing attack showing how faked GPS signals can force a receiver into reporting inaccurate position and time

Note that it is extremely difficult to align the fake signals and authentic signals perfectly, due to signal delay between the spoofer and target receiver while the fake signals are re-transmitted.

Navigation data attack: This uses the same equipment as a code / carrier attack, but instead of manipulating the replica signal code and carrier, the attacker only adjusts the navigation message content on one or more of the faked signals. The aim is to cause denial of service or to produce gross errors in the target receiver. An attacker could set a satellite's status to unhealthy, broadcast hacked ephemeris information, or broadcast false clock correction messages.

To exploit this attack to its full potential, the hacker would generally have knowledge of the target receiver: at a minimum the make, model, and software configuration. However, the rewards are high, as this sort of attack often leaves the receiver requiring a hard reset, even after the attacker has turned off the spoofer and withdrawn from the scene.

Application-level spoofing: The National Marine Electronics Association (NMEA) specification used to transmit data from GNSS receivers to PNT systems is unencrypted, making it vulnerable to man-in-the-middle type attacks. This can be exploited to force systems to report incorrect time and location data with no need for any of the equipment or techniques associated with RF spoofing attacks. (Note that this kind of attack is out of scope for this paper, which focuses on RF-level attacks.)

Multi-method attacks: Sophisticated attacks involve a combination of the above methods, and may also use equipment such as antenna arrays, high-powered transmitters and even low Earth orbit (LEO) satellites. This kind of attack is usually limited to nation states with significant resources and motivation for electronic warfare.

A sophisticated attack will often start with a GNSS receiver in acquisition mode. Many multi-constellation, multi-frequency (MCMF) receivers acquire or re-acquire signals using the GPS L1 frequency alone. This makes them especially vulnerable as they will often lock onto the first signals they see, which could be replica signals generated by a spoofing device.

A receiver could be forced into re-acquisition using high-powered jamming interference or attacked as it exits an area where no GNSS signals were visible. The latter is especially attractive for sophisticated attacks, as the attacker has knowledge of a fairly accurate start position.

Effects of Spoofing on the Receiver

When a GNSS receiver is switched on, it goes through different processing stages before its position, velocity, and time (PVT) solution is computed. The impact of spoofing on a GNSS receiver depends on what stage the receiver was in when the spoofing attack was initiated.

The first stage, the acquisition phase, begins by identifying which satellites are in view and obtaining an estimate of the ranging signal parameters. These are then passed to the next stage, the tracking stage, for fine synchronization, leading to signal acquisition.

Once the signal is being tracked, the navigation data is read from the synchronized signals to determine the exact location of the satellites. The time delay for the ranging signal to travel from the satellite to the receiver is also computed and used to calculate the distance between the

receiver and the satellite. This information is then used to determine the position and velocity of the GNSS receiver and the GNSS time.

The receiver's acquisition stage depends on its initial conditions; that is, the type of acquisition-aiding data (almanac data, ephemerides, knowledge of time and frequency, etc.) available to the receiver when it is switched on.

There are four types of start condition:	
Cold start	The receiver does not have time or position information and no valid ephemerides or almanac data at the start of the acquisition process. If the spoofing attack is initiated during the acquisition stage in a cold start use case, the receiver cannot distinguish the spoofing signal from the real GNSS signal since the GNSS receiver has no a priori knowledge of time or its position. If the receiver does not have any anti-spoofing algorithms, the spoofing signals can mislead the GNSS receiver to compute an incorrect PVT solution, given that the spoofing data is internally consistent.
Warm start	The receiver has an approximate time and position, and a valid set of almanac data, but no valid ephemerides data. If the spoofing attack is initiated during a warm start use case, since the GNSS receiver only has an approximate time and position, it cannot distinguish the spoofing signal from the real GNSS signal. If the receiver has no anti-spoofing algorithms, the spoofing signals can mislead the GNSS receiver to report a wrong PVT solution, within the bounds of the information already available to the GNSS receiver.
Hot or assisted start	The time and last position are known, and the receiver has a valid set of ephemerides data and almanac data. If the spoofing attack is launched during an assisted start use case and the spoofing signal is aligned with the real signal that the GNSS receiver is receiving, the receiver can acquire and track it. If the parameters of the spoofing signals are gradually changed, this can cause the GNSS receiver's PVT solution to diverge as it tracks the spoofed signal.
Re-acquisition	The re-acquisition phase occurs when the GNSS receiver has lost one or more satellites (e.g., when the user goes into a tunnel or under a bridge) for a short period of time. If the spoofing attack is launched just before the re-acquisition stage, the spoofing signals can mislead the GNSS receiver to report an inaccurate PVT solution, given that the spoofing data is aligned with the receiver's previous information.

For a spoofing attack to be successful during the GNSS receiver's tracking stage, the spoofing signal will have to change in a manner that is consistent with the trajectory of the GNSS receiver as well as changes in its environment.

This type of spoofing attack usually results in a jump in the computed position of the receiver. It also causes some inconsistencies between the reported time before and after the spoofing attack, making this type of attack easy to detect if appropriate anti-spoofing algorithms are implemented in the GNSS receiver.

Risk Assessment and Mitigation

As spoofing becomes easier to carry out, unprotected receivers and GNSS-reliant systems are increasingly vulnerable to attack — whether they are the intended target of the attack or simply collateral damage.

Developers and integrators of receivers used for safety-critical and liability-critical systems should seek to understand the impact of all types of spoofing on the operation of the receiver and evaluate the secondary risk to functional safety and business liability.

If vulnerability to spoofing is found to be a material risk to the receiver and its end-users, developers should seek to build in mitigation measures commensurate with the level of risk. Measures typically fall into three categories: protect, toughen and augment.

Protect: Operational procedures are put in place that protect users and equipment from the effects of a spoofing attack — such as ensuring users do not rely entirely on the output from the receiver but also maintain vigilance as to their current position.

Toughen: The receiver is hardened against spoofing attacks through the use of attack detection and automated response — such as sounding an alarm or rejecting the spoofed signals.

Augment: The receiver is complemented with additional / alternative positioning technologies — such as inertial sensors, Wi-Fi / cellular positioning or holdover clocks (for timing applications).

Detection of Spoofing Signals

Both the toughen and augment approaches call for the onset of a spoofing attack to be detected by the receiver. Several techniques can be used for this, as follows:

Antenna-aided techniques: These techniques exploit the advantages of an antenna array and are based on the wide spatial correlation that the satellite signal has with respect to the spoofing signal during a spoofing attack. Techniques include:

- Angle of arrival (AoA) detection with multiple antennas or synthetic arrays
- Beamforming techniques that entail steering or shaping the antenna beam pattern to mitigate the spoofing signals

Signal power monitoring techniques: A spoofing signal is normally louder than the real GNSS signals. In most GNSS receivers that offer protection against spoofing, an attack is detected by monitoring the power and variations in power of the received input signal. The detection of a jamming or spoofing attack is normally performed with the receiver's automatic gain control (AGC).

During a spoofing attack, the presence of a spoofing signal results in an increase in the receiver's noise floor due to the presence of more cross-correlation signals between the spoofing signals and the locally generated replica signals. The increase in noise floor can be used to detect the spoofing attack.

These signal power monitoring techniques can be used in addition to other anti-spoofing methods to detect a spoofing attack.

Evaluation of the correlation properties of the received signal: In the GNSS receiver, signal quality monitoring algorithms can be employed to continually monitor the shape of the correlation function of the received GNSS signals and its locally-generated replica in order to detect distortions in the correlation function. Changes to the shape of the correlation function can be used to detect the presence of a spoofing signal at the acquisition and tracking stages of the GNSS receiver.

PVT consistency checks: GNSS receivers employ different PVT consistency check algorithms to detect and mitigate spoofing signals. Some algorithms compare different attributes of the signal parameters — such as the pseudorange measurements from each of the GNSS satellites that feature in the navigation solution — to detect faults, isolate faulty satellites, and, where necessary, compute protection levels.

Most algorithms work best when more satellites are visible to the receiver than are used in the navigation solution, allowing a valid comparison of the received measurements. Measurements that differ significantly are excluded from the computation. This may be used to exclude spoofed signals from the PVT calculation, as well as to indicate that a spoofing attack is in progress.

Some PVT consistency checks employed in GNSS receivers include:

- Sudden jumps in calculated position fix
- Sudden jumps in time
- Velocity and acceleration changes that are impossible for the particular application
- Consistency of Doppler frequency and code phase measurements
- Consistency of range (pseudorange) or range rate measurements
- Checks using receiver autonomous integrity monitoring (RAIM) algorithms
- Comparison between the single GNSS constellation PVT solutions
- Consistency between data from different GNSS systems
- Consistency with other navigation systems and non-GNSS systems
- Time consistency between the different GNSS system times
- Checks using satellite augmentation data

Navigation message checks: In the navigation data demodulation phase, algorithms can check that the decoded data messages are real. These algorithms may, for example, include checks to ensure that the navigation data messages change when scheduled and that the parameters that change conform to the model of the satellite orbits.

Mitigation of Spoofing Signals

While authorized military users can protect against spoofing attacks by using encrypted signals like the GPS L2 P(Y) code and Galileo's Public Regulated Service (PRS), commercial users must find other ways to protect GNSS receivers and GNSS-reliant systems.

Both toughen and augment approaches can be taken to spoofing mitigation. Toughen options include signal authentication or sounding an alarm. Augment options involve handover to alternative time and navigation sensors.

Signal authentication: New GNSS signals will use hash-type encryption architectures to generate satellite signals that the receiver can differentiate as being authentic. While this is a significant step forward for GNSS security, it does not eliminate the risk of meaconing. The handling of authenticated signals in a PNT system must also be carefully assessed: for example, if there is a failure of the authentication mechanism at the transmitter, what are the consequences of signal rejection for the system's behavior and for the end-user?

Alarms and thresholds: If the receiver detects suspected spoofing signals, it can be programmed to sound an alarm. However, thresholds must be carefully set to avoid alarm failures or false alarms (which can lead to alarms being turned off or ignored). It is therefore critical to decide on appropriate receiver parameters to monitor and then set an alarm threshold on that parameter with enough statistical evaluation of the probability of 1) alert failure and 2) false positive alert.

Handover to alternative navigation sensors: Once a spoofing attack has been detected, the most common mitigation technique is a fallback to an alternative source of position or time. These alternative sources may include:

- Augmentation systems such as inertial measurement units (IMUs) or "dead reckoning" sensors integrated into the system such as gyroscopes and accelerometers
- Approximate position sourced from a different location or connectivity system, such as cell ID or Wi-Fi, to check the computed GNSS position
- Stable holdover clocks in the system (for timing applications)

What to Test

The first step in any test activity that involves spoofing should be an assessment of risk to the operation. This should involve understanding the most important performance parameters of the equipment necessary to meet operational requirements.

For some applications, for example, the timeliness of a position fix may be more important than the accuracy. If the system is providing precision time services, it may be more important to understand how the pulse per second (PPS) behaves under spoofing conditions.

For safety- or liability-critical applications, this analysis should include alarm threshold levels, time to alarm, and the impacts that a spoofing attack (or collateral effects of a spoofing attack) could have on the system.

A risk assessment and analysis will inform several important testing decisions. Does the antenna need to be tested independently? If so, testing may need to be conducted in an anechoic chamber or even on a live range. If testing is to be conducted in a laboratory environment, will simulated signals be sufficient or will it be necessary to introduce authentic live-sky signals?

In most cases, the primary characteristic to test will be the receiver's horizontal positioning error (HPE) versus the power level of the spoofing source at different distances from the source. As the most likely real-world spoofing scenario is accidental exposure to a meaconing device, this should be the primary test case. A sample test is documented in section 7 below.

Further scenarios might be more dynamic in nature, including the receiver operating in acquisition or re-acquisition mode, as well as in tracking mode. For devices where deliberate hacking is a risk, test scenarios should include navigation data attacks where an attacker might hack the contents of the NMEA messages to induce unexpected behavior in the target receiver.

Test Requirements, Methods, Equipment and Scenarios

Defining the Test Requirements

It is important to define the requirements in detail before investing in test instruments and other equipment. Gathering the requirements may encompass knowledge of the following:

Purpose of the testing (current and future)	Testing could be required for one or more purposes, including: • Internal quality control and qualification procedures • Benchmarking and vendor selection for receivers and antennas equipped with spoofing detection / monitoring or mitigation capabilities • Understanding and quantifying possible operational impacts resulting from a spoofing attack or the collateral effects from an attack • Carrying out a risk assessment of real-world threats including resilience / robustness against spoofing • Setting appropriate alarm / alert thresholds Any future changes in requirements should also be considered, to avoid incurring extra costs. This is especially relevant when considering tests for robustness / resilience, as spoofing equipment and resources have become much cheaper and more widespread, so the nature of spoofing attacks has evolved and will continue to evolve rapidly.
Scope of the testing	Should the antenna be tested along with receiver and other hardware-in-the-loop (HIL)? This will determine whether over-the-air (OTA) tests are needed as well as conducted tests.
Geographic location(s)	Should the simulations be carried out for more than one location, or is simulation for a single location sufficient?

Satellite geometries	Do tests need to be repeated with identical satellite geometries?
Vehicle motion	Are the device under test (DUT) and spoofing source stationary, or is there any relative motion?
GNSS application objective	Is the provision of precise timing data more important than precise positioning?
Spoofing vector profile	This will encompass: • Profiles for relative power, code / carrier phase and Doppler offsets of spoofing signals with respect to authentic signals • Code / navigation data attack: A selection of likely target messages has to be made (e.g., SV health status, clock correction messages, ephemeris data) • Pseudorange ramp: At what pace should the spoofer move the position from truth? (If done over a long period of time, this type of attack can deceive the receiver and "sneak under" alarm / alert thresholds) • Radio frequency interference (RFI) profile if "jam then spoof" attacks need to be considered: ◦ Boundary power level conditions ◦ Gradients of change and simulation iteration rate (e.g., 1 ms) ◦ Power resolution (e.g., 0.1 dB) ◦ Waveform type (e.g., continuous wave or chirp)
Spoofing power profile	This will encompass: • Boundary conditions (e.g., min / max spoofer power levels) • How rapidly the spoofer power levels change (e.g., the slope of a first order power ramp) depending on the dynamic output range and update rate of the test instrument (e.g., every 1 ms) • The power resolution (e.g., at least 0.1 dB) • Supported bandwidths: For GNSS receiver testing it is essential to support the GNSS frequency bands (e.g., L1, L2, and L5 for GPS) as well as the adjacent bands, which may affect the DUT performance • Accuracy required (e.g., calibrated power levels, static and run-to-run biases, non-linearities). Note that there are inherent trade-offs in any signal generator between supporting a wide effective bandwidth against the achievable power level magnitude and accuracy. This trade-off must be well understood before investing in vulnerabilities testing equipment. For example, some manufacturers re-purpose generic SDRs for testing within the GNSS frequency bands. Although these generic SDRs can generate waveforms over a wide spectrum of frequencies (e.g., cellular, digital TV, Wi-Fi), they essentially sacrifice performance in terms of calibrated power level, signal fidelity and spectral purity.
DUT and spoofer transmitter testing states	This is very important to ensure test repeatability, especially if testing is conducted in chronically divided phases, or by different operators. Typically, the DUT is cold-restarted between test runs, erasing any previous data stored in the volatile memory, but invoking the testing state configuration parameters (e.g., last-used, user-saved, or factory-set) from the non-volatile memory. These configuration parameters contain essential information (e.g., which atmospheric model the Rx may employ) or whether to enable or disable any multipath / interference mitigation algorithms.
Receiver benchmarking	A packaged subset of scenarios can be used as the basis for a receiver benchmarking scheme. Users can compare test results from a wide range of devices and choose the most appropriate receiver for their intended application.

Choosing a Test Method

Once the test requirements are known, a decision can be made as to the most appropriate test methodology. There are two fundamental methods of testing a receiver:

Over-the-air (OTA)	Testing on an open-air range or in a properly shielded environment such as an anechoic chamber. OTA testing allows for the testing of antenna systems as well as the target receiver. This may be necessary if the antenna system will help to mitigate the effects of spoofing, or to understand the effects of spoofing on the antenna system as well as the receiver.
Conducted testing	This is easily conducted in a laboratory environment by introducing signals directly into the receiver via coaxial cable. It is limited to the target system from the RF input point, which is normally the receiver.

There are two methods of testing a receiver for robustness and resilience to spoofing:

Testing with simulated live-sky signals	The DUT receives replica live-sky signals generated by a simulator. Spoofing signals, usually generated by the same simulator, are then combined into these representative live-sky signals. The test can be OTA or conducted. Testing with simulated signals is far easier to implement because both the real and fake signals are generated by the simulator, making it very easy to align spoofing pseudoranges with the real ones. It should be noted however, that tests carried out in this manner are very much a "worst case," as it would be difficult for a real-world attack to be as well synchronized and aligned. As the live-sky signals are simulated, it means testing is fully repeatable and can easily be carried out in more than one geographical location. Another advantage is that the test can be carried out in a sealed (secure) laboratory environment.
Testing with authentic live-sky signals	The DUT receives the authentic live-sky signals and the spoofing signals generated by the simulator are coupled into the environment. Testing with authentic live-sky signals is more complicated. The real signals are subject to atmospheric errors, multipath, and even RFI, if any is present. To conduct a realistic test under these conditions, the setup must allow relative power levels to be well balanced so that spoofer power levels can be accurately controlled. This makes it harder for the test spoofing attack to succeed, as real ephemeris data must be simulated and the first epoch of the simulator must usually be closely aligned for a spoofing attack to be successful — at least at power levels that do not swamp the correlators. In many ways this is the very best test case for a receiver. This method does have disadvantages, however. Tests are not repeatable due to the constantly changing geometry — for GPS satellites with an orbital period of 11 hrs 58 s, this could mean waiting almost 24 hours (a sidereal day) for a repeating geometry. It also makes testing at different locations and in different environments very difficult or impractical to carry out.

Selecting a Simulator

When selecting a radio frequency constellation simulator (RFCS) for vulnerabilities testing, the following features are key:

Signal accuracy	The signal generator must be more accurate by at least an order of magnitude than the DUT, otherwise it may mask the DUT performance. It is important to generate a test input signal eliminating artifacts, by ensuring maximum specs for the following key parameters: • Signal fidelity: The RF output represents faithfully what has been configured in the simulated scenario • Spectral purity: Eliminating spurious signals, harmonics and other products that may occur in the process of generating the GNSS RF signal output, as well as providing sufficient isolation between signals of different frequencies • Low noise floor: Ensuring that the RFCS inherently generated noise (which is additive to the ubiquitous environmental thermal noise) is kept to a minimum, at least an order of magnitude less than the DUT one, is conducive to a realistic representation of real-world signals, as if the test was taking place under live-sky conditions • High jammer / signal (J/S) ratio (when spoofing tests also incorporate jamming): The ratio of interference power over the nominal GNSS signal power, typically measured in dB. Usually, -130 dBm is the reference power level that corresponds to the interface control document (ICD) GPS L1 frequency C/A code. J/S is a commonly used parameter to benchmark the performance of a DUT in the presence of interference. An RFCS must provide maximum J/S (ensuring low noise floor specifications are maintained)
Accurate signal and error models	The nominal GNSS signals must truthfully represent the live-sky signals (as defined in their respective ICDs), spoofing signals and any ensuing errors (e.g., errors due to multipath, atmospheric interference, or potential signal-in-space (SIS) failure modes). Both the implementation of ICDs and error models can be highly complex, requiring advanced expertise. It is therefore important to invest in testing equipment that is calibrated to an accredited standard, with performance verified by experts in industry-leading organizations.
Flexibility to add new test cases	To maximize its value, the RFCS should be able to expand to accommodate future test requirements (e.g., by adding advanced spoofing generation and monitoring capabilities; multipath interference simulation tools for the specific operational environment of the DUT; remote motion input for HIL testing configurations; or integration of generated GNSS RF signals with emulated inertial sensors for simulation testing of inertial navigation system (INS) / GNSS equipment).
Automation capabilities	If vulnerabilities testing becomes a regular part of ongoing operations, it is essential for the RFCS to support internal or external automation control tools (e.g., via sharing a public application programming interface [API]). Automation can help to maximize the return on the initial RFCS investment.

Further reading

For more information on how to characterize simulator performance, read our eBook: How to Choose a GNSS Simulator.

Configuring the Test Equipment

The equipment and configuration required for a basic test may encompass:

- A GNSS RF constellation simulator (RFCS)
- Calibrated cabling / adaptors, connecting the GNSS RFCS to the antenna DUT
- The Ax / Rx under test
- Monitoring equipment for data collection and analysis, typically via the Rx control user interface or other custom / third-party tools interfacing the Rx output

In some configurations, the RFCS may be replaced by an RF record and playback system (RPS). The RPS can record real-world signals and spoofing signals from a chamber or live-sky test. This recording of the RF test environment can then be replayed in the lab, rather than generating the signals in real time from first principles.

It should be noted that any RPS used should have a sufficiently high dynamic range to capture effectively both real and spoofed signals, and to represent realistically to the DUT the spoofed-to-real signal power ratio that occurred at the time of the recording.

Defining Appropriate Test Scenarios

Receivers and systems should be tested using scenarios that are highly representative of real-world meaconing and spoofing conditions. Their responses will indicate what kind of mitigation techniques may be necessary to allow them to function as expected in the real world. The broadest possible range of scenarios should be tested to minimize the risk of unexpected effects in the field.

Testing should reflect the static and dynamic elements of the chosen scenario. For example, in a meaconing attack the spoofer is likely to be in a fixed location, while the target DUT may be in a moving vehicle, perhaps exiting a tunnel. On the other hand, a timing receiver at a data center is static while the spoofer may be situated in a moving vehicle.

Example Test: Receiver Vulnerability to Meaconing

Scenario

For this sample test, we have chosen a meaconing scenario based on the well-recorded incident in 2010 at Hannover Airport in Germany, where GPS repeaters were installed to test the avionics of business jets in a hangar close to the runway threshold.

If the repeaters were in use when the hangar doors were open, aircraft close to the runway threshold experienced problems with instrumentation that relied on GPS. Several pilots reported that the displayed position of their aircraft shifted to coincide with the position of the hangar.

This scenario can be used to test GNSS receivers along with any hardware dependent on the precise positioning or timing data output from the receiver. As a spoofing scenario it is quite basic, but it serves as an excellent start point for any investigation into the effects of GNSS spoofing on a system.

What Does the Test Measure?

This test assesses a receiver's robustness to a spoofing attack (i.e., the degree to which it is impacted by the attack). The receiver's resilience (i.e., its ability to recover from the attack) can also be assessed by the ability of the DUT to return to its original position once power to the spoofer is reduced at 40:00 minutes into the scenario.

Test Method

The scenario detailed here uses simulated live-sky signals. It can be adapted easily for use with authentic live-sky signals, which requires the use of a synchronization utility.

The DUT is connected to the RFCS, which provides the combination of simulated live-sky GNSS signals along with the signals generated by the spoofer. The spoofing signal broadcasts a location 50 metres east of the initial truth location.

The power of the spoofing source is increased slowly in stages so that the robustness of the DUT is evaluated against the carefully controlled power level of the spoofed signal.

(Note that in the real-world case, the transmitted power level of the meaconing signal was at a fixed level.)

NOTE: Keysight uses the designation "vehicle" for the sources of both authentic and replica signals as it is possible for both the source and the spoofer to be simulated in dynamic or static environments.

Equipment Required

- Keysight RF Constellation Simulator (either PNT X or PNT GSS7000)
- 1RF, n-Vehicles license feature
- Multi-constellation license feature (for nav data spoofing scenarios only)
- Receiver under test

What Does the Test Do?

In this scenario, Vehicle 1 (V1) transmits the truth position, while Vehicle 2 (V2) is located 50 meters east of V1 and acts as the spoofing signal. The signal generated at V2 comes on 10 minutes into the scenario at an increasingly high power as described in the table below.

Time into run (minutes: seconds)	Action
00:00	Start of scenario: V1 ON at default power
10:00	Spoofing starts: V2 ON at default power -10 dB
11:00	V2 power starts increasing by 1 dB every minute
30:00	V2 power at +10 dB
40:00	End of scenario

Table 1. Description of the test

Figure 4 below shows how the power level of the spoofing signal is varied over the course of the simulated scenario. The 2D position error of the DUT is obtained through the GGA NMEA messages sent from the receiver.

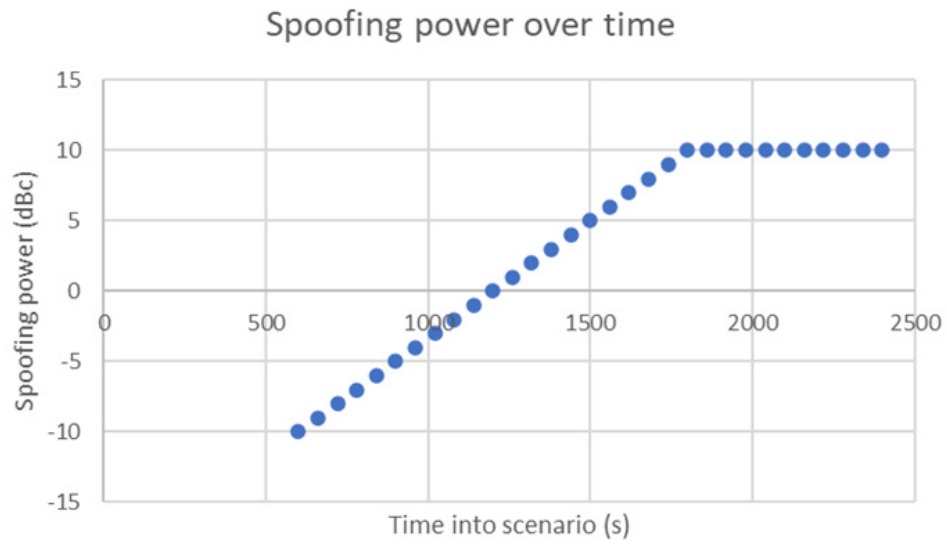


Figure 4. The power level of the spoofing signal is varied over the course of the test

Expected Results

If the DUT is impacted by the spoofer, its position will slowly shift to the new spoofed position 50 meters away as the spoofing power increases. If its HPE is being measured, it will increase as the receiver position is shifted.

Observed Results

A plot of the results from two test receivers subjected to this scenario is shown below in Figure 5. In this case, both receivers are affected by the spoofed signals — with both gradually shifting to report positions consistent with the meaconing signal rather than the truth signal.

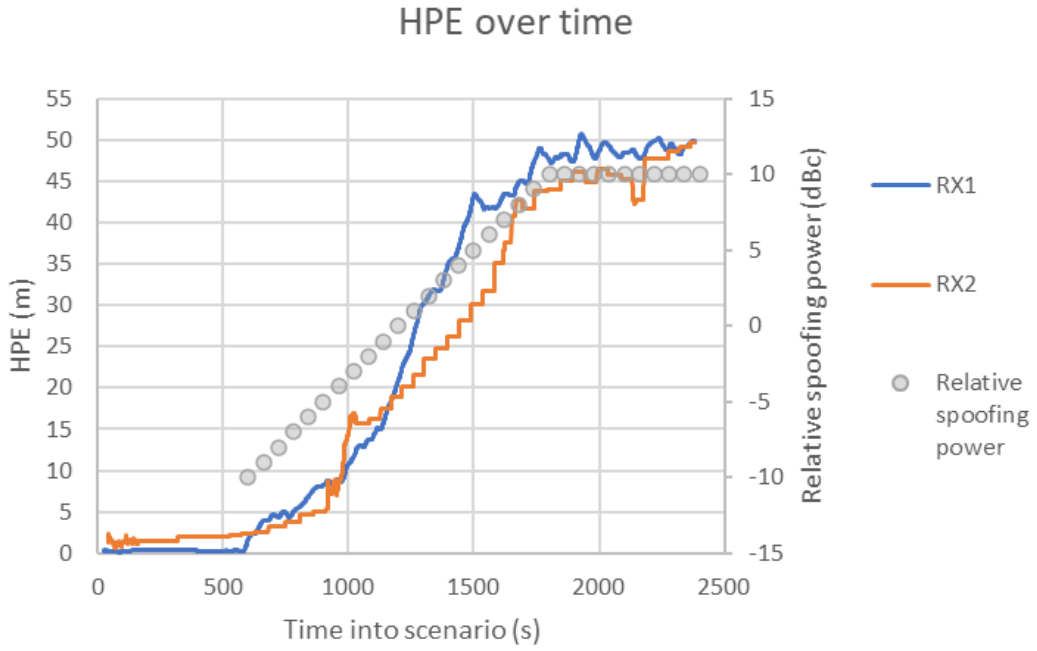


Figure 5. Observed impact on HPE of two receivers under test as the spoofing power increases over time

Conclusion

Testing a receiver's response to GNSS spoofing has traditionally been seen as challenging and as a "nice to have" rather than a test fundamental. This was because spoofing attacks were once considered esoteric in nature and very unlikely to occur in the real world.

However, recent events have shown that this is no longer the case, with spoofing attacks being carried out more often and in more places. There have been many reports of collateral damage to receivers within range of an attack, with unprepared users experiencing unpredictable and disruptive behavior in their GNSS-dependent systems.

This paper has aimed to show that testing using an RF constellation simulator — either where authentic and replica signals are generated by the simulator, or where the authentic signals are obtained from the live sky and the replica signals are generated by the simulator — is relatively straightforward if a "system of systems" approach is applied to the test planning.

As we have shown, planning for a spoofing test should encompass the environment of the test, likely threats, the dynamics of the target and the spoofer, and the main performance metrics. Armed with a preliminary assessment of the test environment, test teams can then construct — or select — realistic scenarios that closely mirror real-world threats / circumstances.

How Keysight Can Help

Keysight can help with every aspect of PNT vulnerabilities testing, drawing on our deep experience developing and implementing GNSS and inertial testing solutions.

We continuously evolve our hardware and software to address the PNT vulnerabilities testing needs of leading organizations in the military, government, space, and industrial sectors. Our GNSS signals are generated implementing the latest ICDs, using dedicated hardware and software that is developed in-house for better support and maintainability.

Keysight mathematical models have been proven and optimized, working in partnership with the leading experts in the GNSS industry. Our simulated GNSS signals are generated from first principles, via full implementation of each relevant and current ICD, and fidelity is assured through verified mathematical modeling of the signal characteristics and errors as well as Rx behavior.

For spoofing testing in particular, Keysight offers the following hardware, software, and professional services:

Hardware

Keysight's multi-frequency, multi-constellation simulators offer full field upgradeability and on-the-fly reconfigurations, with support for all current and future constellations and frequencies, enabling developers to accurately evaluate receiver performance in a wide range of real-world conditions, including spoofing scenarios:

PNT X is a revolutionary PNT simulation system that supports the broadest range of NAVWAR test scenarios. With the option to generate over 600 individual signals or to utilize 10 individual RF outputs, and with the ability to generate all open and restricted GNSS signals, the PNT X is the ultimate partner for spoofing testing.

PNT GSS7000 is the class-leading simulator for civil and consumer applications, with up to 256 channels and 2 independent RF outputs.

Software

The embedded spoofing feature for the PNT X and PNT GSS7000 simulators comprises built-in and user-configurable capabilities to generate spoofing scenarios, such as trajectory spoofing, navigation data spoofing, and meaconing attacks. The user can define, amongst other parameters, the number of spoofer transmitters and their location (absolute or vehicle relative), the spoofer power levels, the false vehicle position (spoofed position) and the spoofing signal content, including navigation data and errors. The resulting spoofer RF signal will be automatically calculated based on user scenario settings, with the correct spoofer signal arrival angle and spoofer signal content.

Positioning Test Services

Keysight offers a portfolio of services to help with any aspect of PNT testing, including vulnerabilities testing. Services include:

Lab as a service: Keysight will test your device for spoofing vulnerabilities in our state-of-the-art lab, with testing conducted to your requirements and with a full report provided.

Test as a service: Experienced Keysight test engineers will join your team to conduct any aspect of your testing regimen, including setting up and managing spoofing tests.

Scenario provisioning: Choose pre-built spoofing scenarios from Keysight's comprehensive scenario database or ask us to build custom test scenarios for use with your Keysight simulator.

Additionally, Keysight offers a global technical support network, with experienced test engineers and consultants available to resolve any technical questions and advise on how to achieve and maintain the best calibrated performance from your system.

Contributors

Guy Buesnel, CPhys, MInstP, FRIN, RNTF

Guy has worked more than 20 years protecting GNSS receivers from emerging threats, having started his career as a systems engineer involved in the development of GPS adaptive antenna systems for military users. Guy is a specialist PNT security technologist covering the areas of PNT threats and mitigation. Guy holds a BSc honors degree in physics with atmospheric physics and a master's degree in communications engineering.

Guy is a member of the Institute of Physics, a Chartered Physicist, a Fellow of the Royal Institute of Navigation, and in 2019 was appointed as a member of the International Advisory Council for the Resilient Navigation and Timing Foundation.

Esther Anyaegbu, PhD

Esther completed a master's degree in data communications systems from Brunel University and subsequently earned her doctorate from the Institute of Satellite Navigation (ISN), University of Leeds. Her research focused on the processing of GNSS signals in the frequency domain.

Esther has expert knowledge of the GNSS receiver architecture and GNSS processing methodologies and has authored and co-authored many technical reports and publications.

Appendix: Glossary of Abbreviations

The following abbreviations have been used in this paper:

AGC	antenna gain control
AoA	angle of arrival
API	application programming interface
Ax	antenna
C/A	coarse / acquisition
DUT	device under test
GGA	Global Positioning System fix data
GNSS	global navigation satellite system
GPS	Global Positioning System
HIL	hardware-in-the-loop
HPE	horizontal positioning error
ICD	interface control document
IMU	inertial measurement unit
INS	inertial navigation system
J/S	jammer / signal
LEO	low Earth orbit
MCMF	multi-constellation, multi-frequency
NMEA	National Marine Electronics Association
OTA	over-the-air
PNT	positioning, navigation, and timing
PPS	pulse per second
PRS	Public Regulated Service (Galileo)
PVT	position, velocity, and time
RAIM	receiver autonomous integrity monitoring
RF	radio frequency
RFCS	radio frequency constellation simulator
RFI	radio frequency interference
RPS	record and playback system
Rx	receiver
SDR	software-defined radio
SIS	signal-in-space
SV	space vehicle (an individual satellite in orbit)

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

KEYSIGHT

This information is subject to change without notice. © Keysight Technologies, 2026, Published in USA, June 1, 2026, 3126-1206.EN