infiniDome
NAVIGATION RESILIENCY

GPS Jamming:
How it Works, Methods of Prevention

The Vital Necessity of GPS

In recent times, GPS has become a mainstay for not just communication technologies, but also a wide range of commercial activities as well as homeland security. Ship and cargo truck fleets rely heavily on accurate and reliable GPS data for navigation and tracking, with their operations remotely monitored by control centers. In the field of defense, GPS has become critical for everything from UAVs and loitering munitions to military ground vehicles.

The Vulnerability of GPS

GNSS receivers, which use GPS signals (as well as GLONASS, Galileo and other constellations – hence the name "GNSS" – Global Navigation Satellite System), are notoriously vulnerable. This is due to the nature of the signals themselves, which emanate from orbiting satellites located 20,000km above the Earth's surface. Reception for this very weak signal is challenging, but is still possible – provided there is no interference. Besides the vast distance the signals have to travel, the satellites themselves have limited energy. Signal disruption can be the result of a) physical barriers between the receiver and the satellites, such as mountains, buildings or a roof (when indoors or in a tunnel), b) unintentional jamming (an adjacent frequency used, such as Ligado, which overlaps with GPS) or c) intentional jamming – which is the focus of this white paper.

The Threat of GPS Jamming

Intentional interferences such as GPS jamming have become a major problem in recent years, due in no small part to the widespread availability of cheap jamming devices. For defense applications, disruptions in critical PNT data (Positioning, Navigation and Timing) mean loitering munitions that never find their targets, multi-copter or fixed-wing UAVs that get lost or crash to the ground, and ground vehicle fleets that cannot be monitored and managed (with all IFF – Identification of Friend or Foe – capabilities impaired). GPS jammers have also become the weapon of choice for criminals engaged in cargo theft and drug trafficking, with Mexico reporting the use of jammers in an astonishing 85% of all documented cargo truck thefts.[1] Furthermore, along the U.S.-Mexico border, drug cartels use jammers on border surveillance drones to hide their operations from the U.S. government.[2]

GPS jamming can even present a threat to civilians. In China, drone light shows are all the rage in recent years. But in the central city of Zhengzhou, a drone light show over a mall quickly turned into a nightmare, when dozens of drones began falling from the sky and smashing into buildings and vehicles on the ground, endangering the 5,000 onlookers.[3] Several other crashes and accidents have been reported at drone shows across the world.

All that an attacker needs to do to create a potentially catastrophic Denial of Service attack of GPS for everything around him, is to overpower the GPS signals by emitting a signal at the same frequency, just slightly more powerful than the original (extremely weak) signals. And today, this attack could be carried out with a $20 jammer bought online. In the fields of electronic warfare and communications there is a concept called "J/S" (jamming to signal ratio), which is used to evaluate the susceptibility of a system to jamming. J/S is a measurement of how powerful the jamming signal is compared to the power of the original GNSS signal. With normal J/S (i.e. under "normal" conditions), there is no jamming signal. A higher J/S ratio indicates that the jamming signal is stronger, making it more difficult for the receiver to detect the desired signal.

Types of Jamming Attacks and Signals

GPS jamming attacks typically involve the use of an RF (Radio Frequency) signal that overwhelms the receiver, making it impossible to detect the satellite signal amidst the noise. The receiver's resistance to interference signals depends on its synchronization status, but there is always a threshold beyond which the jamming signal will be successful in causing the receiver to lose the satellite signal. To achieve this, the jammer must emit a signal that reaches the receiver's antenna with greater power than the receiver's threshold. If the jamming signal is directed towards the receiver's antenna, the receiver will require more transmission power from the satellite to maintain the same level of reception (which is, of course, impossible as the satellite signal power levels are constant).

Continuous Wavelength (CW) is the most straightforward method of jamming for attackers. The benefit of a CW is that the full power of the jamming signal is concentrated into a single frequency. Almost anything transmitted in the same frequency as the GPS signal will lead to it being blocked. A sinusoidal wave is the simplest signal to transmit so as to create a single frequency CW attack. So for example, an attacker can transmit a sinusoidal wave on the L1 frequency signal (1,575.42 MHz) and it will successfully block a GPS signal in the same wavelength. However, there are receivers that know how to overcome a CW attack. The best receivers on the market today have the capability of creating a "notch filter," which can attenuate or filter out a specific, very narrow-band signal to very precise measures, in such a way that the desired satellite signal can still be received around this notch.

Narrow band refers to signals established through a narrow range of frequencies (a range of around 2MHz). The problem here is that the power (Watt) is spread and diluted throughout the different frequencies making up the band. Here one could do a sweep modulation – transmit several CW's one after the other, always alternating the frequency. This would improve one's ability to emit a signal at a much higher power. There are also jammers that create a series or burst of narrow-band signals, transmitting one shortly after the other. This is referred to as a "barrage."

Since the power of signal transmission is diluted through the different frequencies, one way jammers can try to improve their attacks is by directional precision – by aiming directly in the target's direction. There are jamming devices on the market that even resemble a gun and which use a directional transmitting antenna, designed to be precisely aimed at a specific target or in a specific vector.

Jammers can also use various types of **modulations** in their attacks. For example, in **Frequency Shift Key (FSK)** modulation, a signal is transmitted by switching between two different frequencies, one represented by a binary "0" and the other by a binary "1." However, this is a relatively slow method. By using two bits at a time instead of just one (00, 01, 10, 11 – instead of just 0 or 1), it is possible to represent four states and use four frequencies to transmit the signal. As a result, information is transmitted twice as fast. In FSK8, 3 bits are used, resulting in 8 unique symbols representing 8 different frequencies.

Phase Shift Keying (PSK) is another method of wave modulation for transmitting data. In PSK, the phase of the carrier wave (its position in time relative to a specific reference point) is varied to represent certain information. The variations in phase can be used to transmit data like a binary signal, with the advantage that it is more robust to noise and interference than its amplitude-based counterparts. In PSK, the phase of the frequency is modulated to one of four possible positions or values: 0 degrees, 90 degrees, 180 degrees, or 270 degrees. Each phase change represents a different piece of information, in

this case one of four different frequencies. In this way, PSK allows the signal to carry more information compared to FSK with the same bandwidth.

An important thing to note is that the size of jammers is determined by its power. A small jammer, around the size of a pack of cigarettes, is usually around 1W. A larger box, the size of an old VCR, can reach 10-100W in transmission power. The huge jammers used in Ukraine, for example, in hostile war conditions, are usually around 1KW and about the size of a truck.

Different Approaches to Protecting GPS

Various anti-jamming approaches and technologies exist to protect GPS-reliant devices. With **beam steering**, an array of antennas is pointed in specific direction(s) where their performance will be more effective. This method can be used when one has the ability to control the directions or vectors from which the signals are emitted. With **beam forming**, by manipulating the direction and amplitude of the antennas in the array, one creates nulls and beams in many directions. For example, with a signal from a certain direction hitting just two antennas in the array, both antennas will receive the signal at the same intensity at different angles. But one can turn them to the point where they will receive the signal at the same angle, which then cancels out the signal. Instead of cancelling it out, one can also combine the signals and have a more powerful or sensitive antenna.

With **null steering (digital/analogue or RF)**, we create a null in the direction or vector of interference (instead of creating a beam in a certain direction as we did with beam forming), in such a way that any signal from that vector is attenuated, while protecting signals received from anywhere but that vector. This is the commonly used approach for protection against jamming. The number of nulls you can create is always n-1, where "n" is the number of antennas in the array.

Some approaches consist of a combination of both null steering and beam forming. **Mechanical approaches** are another option, whereby anti-jamming antennas automatically "know" the direction of the jamming signals, thereby protecting themselves more efficiently. For example, antennas mounted on the roof of a building could efficiently protect from a jammer below.

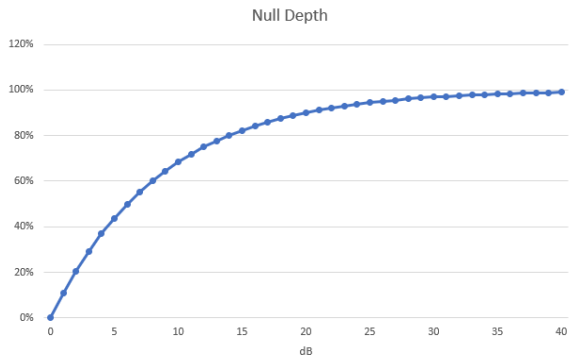

Figure 1: Mitigation of jamming signals at varying protection levels.

Figure 1 above shows the effectiveness of different levels of protection in dB for mitigating jamming signals. The x-axis represents the system protection strength in dB (null-depth), while the y-axis represents the percentage of jamming signal mitigation achieved relative to each level of protection. The graph shows, for example, that when employing a 20dB null anti-jamming protection system the jammer will only be effective to a tenth of the original proximity (10m vs. 100m).

The Challenge: Form Factor

Current solutions that employ null steering technology use a lot of digital signal processing, which results in them being very heavy and bulky in size. Since they also require high-end A2D components (Analog to Digital) to operate, this results in them being extremely expensive and power-hungry as well. Digital null steering

solutions also add a substantial amount of latency to the signal (RF) path. In addition, the number of calculations and possible nulls for jamming protection increases (exponentially) with each additional antenna. Consequently, the size of the anti-jamming unit (due to the quantity of electronics needed) directly correlates to the number of nulls and complexity of calculation. Despite all this, it is possible to create optimal anti-jamming solutions which are scalable, and which, especially when combined with high-quality yet off-the-shelf antennas (with or without inherent horizon-blocking AJ capabilities), and multi-constellation, multi-band resilient receivers with high processing gain (with or without AJ notching capabilities), can still support a very good J/S ratio for the system while adhering to minimal SWaP (Size, Weight, and Power) constraints.

How infiniDome Tackles the Problem

infiniDome uses null-steering technology, creating nulls in the directions or vectors of the jamming signals' exact angles of attack. But that's far from the full story. Its solutions are designed to place specific emphasis on how the signal is received at the antennas themselves. Instead of working with fixed antenna arrays (as required by competing solutions in the market), infiniDome's patented algorithms allow the antennas to be almost freely deployed on the vehicle (at least 10cm apart), autonomously analyzing the deployed geographical structure of the antenna array and its orientation, thereby allowing it to analyze the direction of attack. By adding to the calculation the direction relative to the structure and orientation of the antenna array, and running optimization algorithms to find the optimal direction of the nulls for attenuating the jamming signals, infiniDome solutions are able to isolate and attenuate the attack.

Once the direction of the jamming signal is isolated, two essential techniques are employed to maintain protection. The first is the general null steering approach: taking the signal, down-converting it to a lower frequency on all antennas, transforming it to the **frequency domain*** (using **Fast Fourier Transformation – FFT**), then calculating and implementing the null steering algorithm itself. (*The frequency domain is a way of analyzing signals by looking at the frequency components that make up the signal, rather than looking at the signal over time.) The second technique requires sampling the Radio Frequency (RF) channels, performing similar Fourier transform, calculating the required phase and amplitude shift for each of the four signals and performing this signal modification on the RF signal itself.

infiniDome implements down-conversion only if a jamming signal is recognized. This means that the nominal power consumption can be reduced even further. If a jamming signal is detected (after down-conversion), infiniDome solutions sample the Intermediate Frequency (IF) using all four antennas. These samples are analyzed (using FFT) and a null-steering algorithm is applied to calculate the required phase and amplitude changes for each of the four antennas. These results are transferred to a proprietary RFIC which modifies the RF signals according to the solution of the calculations, which then frees the digital processor up to allow it to analyze other frequencies (thereby ensuring minimal latency of less than 100 nanoseconds).

infiniDome's GPSdome is capable of attenuating a jammer at a 20dB null depth in a single direction, while its GPSdome2 solution employs 35dB protection against up to three simultaneous directions of attack in each of the 2 protected frequencies.

Real-Life Application

infiniDome conducted tests in the Golan Heights along the Israel-Syria border, where Russian GPS jamming has become a common occurrence, used by the Syrian military to disrupt Israeli defense operations, homeland

security and even commercial activities (such as GNSS-dependent, precise agriculture). The goal was to "hunt down" jamming events and record them, comparing GNSS performance side-by-side for an unprotected GNSS u-blox M8N receiver versus an identical receiver protected by infiniDome's GPSdome. In a video of the tests, the receiver protected by GPSdome can be seen maintaining the GPS signal along the border, enabling uninterrupted navigation. In contrast, the unprotected GNSS receiver lost the GPS signal during the attack, which could have easily resulted in a drone being completely jammed, aggressively drifting and eventually crashing to the ground. An analysis of the jamming attack showed that it was a slightly more sophisticated signal than a regular "brute force" jamming attack, causing the receivers to "see" something that looks like real satellite signals (which were in fact, generated by their smart jammer), but to not be able to synchronize the receiver to their signals and track them. The receiver protected by GPSdome was able to distinguish between the real GNSS signals and the more powerful jamming signals, with GPSdome attenuating the jamming signals sufficiently to enable continuous tracking of the real GNSS signals while reporting the attack via its dedicated alert output.[4]

For more details of the Golan Heights tests and the full reports, including links to the video recordings, please visit this page.

Additional test reports for other jamming scenarios are available. For more information, please contact infiniDome directly: info@infinidome.com

[1] Source: https://rntfnd.org/2020/10/30/gps-jammers-used-in-85-of-cargo-truck-thefts-mexico-has-taken-action/
[2] Source: https://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/
[3] Source: https://www.vice.com/en/article/z3xp38/drone-light-show-failure-china
[4] White paper: "infiniDome Records GPS Jamming and Its Mitigation at the Israel-Syria Border", 2022.