

The significance of GNSS spoofing for OME

Introduction

This report is going to cover the use of Global Navigation Satellite Systems (GNSS) in the Ordnance, Munition and Explosive (OME) environment. It will briefly cover basics of the engineering, physics and mathematical principle used in GNSS, the different variants in use around the globe but primarily focusing on the Global Positioning System (GPS). It will cover how GPS is used in the OME and weapons environment including both current and future applications. This report will also cover the vulnerabilities the system has such as Jamming and Spoofing and countermeasures to these types of attacks.

Concept

GNSS is a generic term used to describe any satellite-based means of providing Positioning, Navigation and Timing (PNT) data to a device or system for the purpose of navigation in a global or regional basis [1]. Whilst GPS is the most prevalent system and will be the main focus of this report, there are several systems around the world in global and regional use.

System	Country	Type	No. of Satellites*
GPS	United States	Global	32
GLONASS	Russia	Global	27
Galileo	European Union	Global	30
BeiDou	China	Global	22
QZSS	Japan	Regional	7
NAVIC	India	Regional	7

Table 1:Types of GNSS systems [2]

*Approximate number of operational satellites.

GNSS and more specifically GPS is made up of three segments, these are Space segment, Control segment and User segment. Together they work to provide navigational information to the user's device.

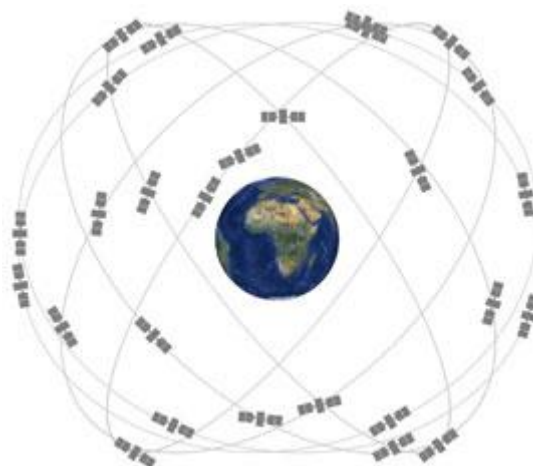


Figure 1: 24-Slot satellite constellation [1]

- **Space segment** – Consists of the satellites orbiting in mid-earth orbit (20,000 KM) twice a day in constellations. A constellation consists of four satellites orbiting around the globe and spaced apart from other constellations by 60 degrees, as depicted in Figure 1 above. This allows for at least four satellites to be visible from any point on the planet [3].
- **Control Segment** – This consists of earth-based monitoring locations, control stations and ground-based aeriels. Their role is to monitor all the satellites and provide correctional data to keep the system accurate during their orbits [3].
- **User segment** – This segment is the GPS receivers that interact with the satellites. The GPS receiver convert the signals sent by the satellites into PNT data which is then used to accurately find the GPS receiver's position [3].

In a simplified way a GPS system works by a satellite sending its location data and time, to the GPS receiver and the GPS receiver uses this data to determine how far away from the satellite it is. With one satellite the GPS receiver knows how far away it is from the source, but this could be anywhere in a sphere around the satellite. When a GPS receiver gets a signal from a second satellite it can determine its location against two possible points (where these spheres intersect). With a third satellite it can then use the point at where all three satellites intersect to determine its location (see figure 2) [4].

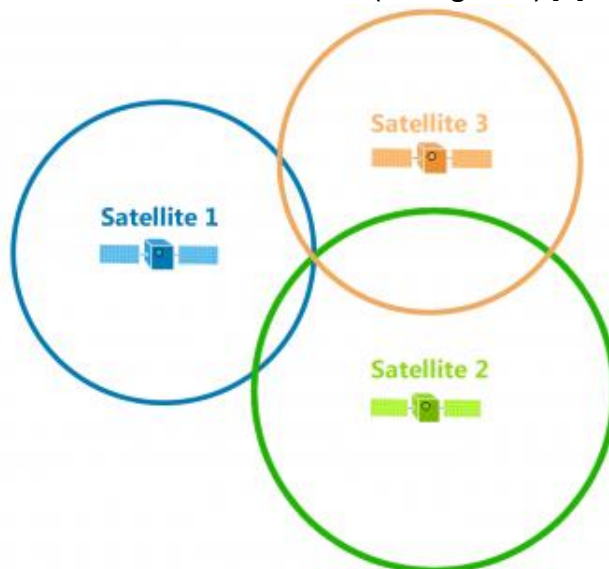


Figure 2: Three satellites on a 2D plane [4]

Due to the signal emission around the satellites are spherical, to accurately find our position in a 3D environment we require the use of a fourth satellite to provide us with the data required to find our position in the vertical axis.

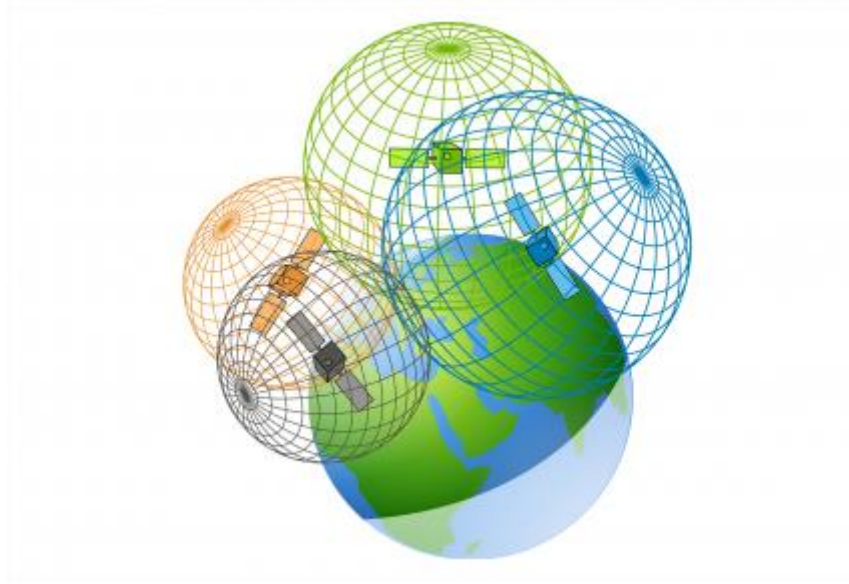


Figure 3: Four satellites in a 3D environment [4]

The process described above is known as trilateration, this is a mathematical technique used to determine the user's location (both horizontally and vertically) as well movement of the user. This is done by the GPS receiver employing the geometry of circles, spheres, and triangles to calculate the exact distance from each satellite [5].

Part of the signal received from the satellites contains a precise time reference which all the satellites are sequenced to (the job of the Control segment). It calculates this by working out the latency between receiving all 4-time stamped signals from the satellite and the receiver's internal clock [7]. The receiver's internal clock is then synchronised with that of the satellites. The receiver does this by calculating a correction factor that it can apply to all the signals. With this correction factor applied it can work out how far away from each satellite it is, with these four distances applied to the known location of each satellite the receiver can determine its PNT data. The basic formula the receiver uses to calculate its PNT data is [8]:

$$\begin{aligned}
 D1 &= C \cdot t_i + \sqrt{(X - X_1)^2 + (Y - Y_1)^2 + (Z - Z_1)^2} \\
 D2 &= C \cdot t_i + \sqrt{(X - X_2)^2 + (Y - Y_2)^2 + (Z - Z_2)^2} \\
 D3 &= C \cdot t_i + \sqrt{(X - X_3)^2 + (Y - Y_3)^2 + (Z - Z_3)^2} \\
 D4 &= C \cdot t_i + \sqrt{(X - X_4)^2 + (Y - Y_4)^2 + (Z - Z_4)^2}
 \end{aligned}$$

Equation 1: Trilateration

Where:

C= Speed of light

t_i = Time correction factor

(X, Y, Z) = Position to be solved

(X₁, Y₁, Z₁), (X₂, Y₂, Z₂), (X₃, Y₃, Z₃), (X₄, Y₄, Z₄) = Locations of the satellites

D1, D2, D3, D4 = Distance of satellites from receiver.

All of which looks complicated on the surface but, the equation is essential calculating the distance using time and speed.

$$Distance = Speed \times Time$$

Equation2: speed distance time triangle

We know the speed of the radio waves as they travel at the same speed of light [6] which is $3 \times 10^8 m/s$, we then require the time it took the radio waves to travel the distance from the satellite to the receiver to complete the equation. The receiver calculates the time by comparing the time stamp in the signal from the satellite to the time on the receiver system. With the time and speed factors the receiver can then calculate the distance.

Passive Radio Frequency (RF) trilateration is the most common used form of trilateration for satellite navigation. The signal sent by the satellites to the GPS receiver are L-band radio signals in the 1GHz to 2GHz frequency. The advantage of using this frequency band is it allows the signals being sent to be insensitive to most weather conditions. The receiver needed is inexpensive and easy to produce and it is a passive device. Meaning the receiver does not have to transmit any signal for it to operate. As with any sort of radio wave it has its limitations, it can easily be affected by space weather (waves emitted by the sun) causing signal distortion for example. The radio waves do not propagate well through materials such as underground or in water meaning the system is only suitable for above ground navigation. Due to the low power of the receivers and lack of encryption used in most civilian GPS device they are very susceptible to interference such as jamming and spoofing [6]. This is something which will be covered in detail later in the report.

GPS in OME platforms

GPS has a multitude of uses and has been integrated into various household items from smart phones, smart watches, Farming, and vehicles just to name a few. One key area GPS has been used widely is in the defence sector with the constant desire for more precise location and tracking for vehicles, weapons, and personnel.

Throughout recent history the worlds military have constantly searched for more accurate weapon systems. The use of carpet bombing from the likes of WW2 and Vietnam to achieve a military goal is no longer desired due to their indiscriminate nature and destroying everything in its path including military targets and civilian areas nearby. Although the use of carpet bombing will severely affect the moral of the enemy, the high number of civilian casualties will severely affect the support of the country's population doing the bombing [9].

One of the first breakthroughs for precision munitions was the use of laser guided bombing but despite the high level of accuracy they still suffered from limitations. The launch aircraft would have to stay in the vicinity of the target to guide the munition to target and it is also severely susceptible to the weather conditions, low hanging clouds for example [10]. One way to combat this and to allow a wider range of munitions to be used for precision attack is the integration of a GPS module into the weapons [11]. For more complex weapons such as air to ground missiles and cruise missiles the weapon systems use a combination of GPS and Inertia Navigation System (INS) for high degrees of accuracy [11]. These sorts of munitions

are now in widespread use across the world's militaries. With the increase in accuracy the impact on the civilian population of a war zone has been reduced. Before bombs would fall wherever they were dropped hitting anything that happened to be in their way but now the ability of commanders to precisely choose as target can reduce the amount of munitions needed to achieve the same results as "dumb" bombing [11].

The future of guided munitions will have a high degree of accuracy whilst also being able to have guidance updates mid-flight and network enabled communications with other guided weapon systems [12].

Limitations

Like any system there are limitations associated with GPS, two of the main limitations for GPS are Jamming and spoofing. Due to the unencrypted nature of the signal sent between the Satellite and the receiver it is left open to jamming or spoofing attacks [13].

Jamming is achieved by overpowering the receiver with a stronger unusable signal preventing it from accessing the correct signal from the satellite [6]. Due to the weak signal received from the satellite due to atmospheric interference it is easy for even a small jamming device to cause a widespread denial area [6]. Due to the cheap and straightforward design of jammer devices its not too difficult for someone with a basic knowledge of electronics to make a GPS jammer, and with a simple search on the internet you can find endless jamming devices available for purchase.

Spoofing is different to jamming, instead of saturating the environment with unusable radio signals spoofing tricks the GPS receiver into thinking it is somewhere else [6]. As mentioned in the jamming attacks the signal from satellites are weaker than locally generated signals, so all a spoofing system must do is broadcast a stronger signal and the receiver will pick this up. A spoofing device mimics the signals from the four satellites and provides a fake signal for the receiver to use to calculate its location [6]. For a military application this can be particularly useful and in recent years it has reported been used by Iran to capture a United States drone [14]. Iran claims they achieved this by spoofing the GPS signal to the drone into thinking it was near its homebase and made it land at one of their airfields.

Jamming and spoofing protection

Jamming and spoofing protection as a civilian user is limited due to the simplistic nature of most receivers available to the civilian population. Naturally, the military powers of the world have invested heavily in Jamming and Spoofing protection for its equipment. For this report, we will be focusing on the military Jamming and Spoofing mitigations in weapon systems.

For small weapons like artillery shells that use a GPS module such as BAE Systems Navfire [15], a small unit with a high G resistance allowing for it to be fired from an artillery cannon. This system uses a process such as digital nulling which in simple terms means the receiver only recognises signals coming from an authentic direction (known location of a satellite), the system essentially filters out the jamming signal due to the location it arrives from [16].

For more complex weapons such as cruise missiles they can have a wider range of mitigation systems built in. As well as digital nulling mentioned above there could also be an INS built into the missile. This is where a series of gyroscopes and accelerometers can measure the movement of the missile in flight without any external input. For this system to work it can use the last known good GPS location as a starting point and using time, speed and orientation to deduce where it has travelled from the last known position, it knows where it is [6]. But this system has its drawbacks as it becomes more unreliable the longer it is in use due to drift in the gyroscopes. GPS jamming can also be mitigated using laser designators to paint the target with a laser beam for the missile to acquire. The main drawback to this mitigation is you need to maintain line of sight to the target be it by aircraft or boots on the ground. Combining all three mitigations above would provide widest means of jamming mitigations. The GPS system could guide the missile to the target location where it can null the jamming signal until the jamming signal becomes too powerful for the nulling effect to work. At this point the INS would take over the navigation of the missile to the target area. If the jamming area were small the INS could see the missile through to impact, if the jamming area were on a larger scale the INS could allow the missile to travel to proximity of the target where a drone or a man on the ground could paint the target for the missile to locate. This method would also work to mitigate against spoofing attacks.

Spoofing attacks as mentioned above involve the introduction of a fake satellite into the Trilateration equation (Equation 1 above), it essentially replaces one or more of the genuine satellite signals with a false signal. A way to combat this is using signal encryption, all civilian receivers are unencrypted and only acquire one signal from the satellites orbiting above. Military receivers use the regular civilian signal as well as a second encrypted signal known as M-code [17]. This mitigation is difficult to get around due to the secretive nature of the key to the encrypted signals. As mentioned in the paragraph above digital nulling will also help mitigate against spoofing signals.

Spoofing is particularly a type of attack that needs to be mitigated in the weapon system world, due to the possibility of a spoofing attack being used to make a missile impact an overly sensitive area such as a school or hospital. If an aggressor country were able to carry out such an attack, they could use it to gain support for their own cause and tarnish the reputation of the country launching the missiles. For countries such as the UK using spoofing attacks to cause damage to civilian infrastructure (such as hospitals and schools) is highly unlikely due to the way the UK's armed forces are confined by the Geneva convention which prevents such actions. One way the UK could implement a spoofing attack for example would be to spoof a vessel of interest into entering UK controlled waters where it could then use the encroachment into UK waters to conduct a boarding operation and seize control of the vessel.

Conclusion

GNSS and more specifically GPS have many applications both in the civilian and military use and as we have covered, they have their vulnerabilities. With information warfare developing into a new aspect of warfare with ever more requirements for battlefield commanders to have instant information on their forces locations, GPS has and will be

integrated into a wide array of equipment, vehicles, and weapon systems. As with any form of warfare an arms race will always take place between offensive means such as jamming and spoofing and the defensive technology to counter these threats. Attacks will continue to get more sophisticated as well the means to counter them. Until a new form of PNT which does not rely on satellites can be developed and implemented this arms race will continue, then a new way of service denial (such as jamming and spoofing) will be developed, where the cycle will start again. As with anything new coming from the military sphere when a new PNT system is implemented, eventually it will trickle its way into civilian use just like GPS has.

References

- [1] "GPS: The Global Positioning System," U.S Government, [Online]. Available: <https://www.gps.gov/systems/gnss/>. [Accessed 15 Nov 2022].
- [2] M. Choudhaey, "Geospatialworld," 20 Nov 2019. [Online]. Available: <https://www.geospatialworld.net/blogs/what-are-the-various-gnss-systems/>. [Accessed 15 Nov 2022].
- [3] J.-F. Pascual-Sánchez, "Introducing relativity in global navigation satellite systems," *Annalen der Physik*, vol. 519, no. 4, pp. 258-273, 2007.
- [4] "GIS Geography," 31 May 2022. [Online]. Available: <https://gisgeography.com/trilateration-triangulation-gps/>. [Accessed 15 Nov 2022].
- [5] F. Zahradnik, "Life Wire," 28 Aug 2021. [Online]. Available: <https://www.lifewire.com/trilateration-in-gps-1683341>. [Accessed 15 Nov 2022].
- [6] I. Botkin, Director, *Why Everyone Needs a GPS*. [Film]. United States of America: T.Rex Arms, 2022.
- [7] D. K. T. & D. C. Chatterjee, "ecoursesonline," [Online]. Available: <http://ecoursesonline.iasri.res.in/course/view.php?id=53>. [Accessed 15 Nov 2022].
- [8] J. & D. B. W. P. Dr Y. JADE MORTON & Dr FRANK VAN DIGGELEN & Dr JAMES J. SPILKER, *Position, Navigation, and Timing Technologies in the 21st Century*, Wiley, 2021.
- [9] T. E. o. Encyclopaedia, "Britannica," 21 Jul 2016. [Online]. Available: <https://www.britannica.com/topic/carpet-bombing>. [Accessed 16 Nov 2022].
- [10] "Precision guided munitions and the historic roles of GPS," PCTEL Connected solutions, 2015.
- [11] P. G. Gillespie, *Weapons of choice: The development of precision guided munitions*, Tuscaloosa: University of Alabama, 2006.
- [12] L. C. F. Esposito, "Precision-guided munitions of the future," *Joint air power competence centre*, vol. Spring/Summer 2019, no. 28, pp. 28-33, 2019.
- [13] G. Mori Gonzalez, I. Petrunin, R. Zbikowski, K. Voutsis and R. Verdeguer Moreno, "Vulnerability Analysis of GPS receiver software," in *International Conference on Localization and GNSS*, Nuremberg, 2019.
- [14] L. G. P. K. (Retd), "SP's Aviation," 1 Feb 2021. [Online]. Available: <https://www.sps-aviation.com/experts-speak/?id=513&h=GPS-Circle-Spoofing-and-Electronic-Attacks#:~:text=Iran%20is%20the%20first%20nation,used%20it%20to%20great%20advantage.&text=In%20December%202011%2C%20Iran%20captured,drone%2C%20which%20was%20publicly%2>. [Accessed 17 Nov 2022].
- [15] "NavFire GPS receiver," BAE Systems, 2020.
- [16] M. Jones, "GPS World," 12 Apr 2017. [Online]. Available: <https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/>. [Accessed 21 Nov 2022].
- [17] S. Cole, "Military embedded systems," 30 Nov 2015. [Online]. Available: <https://militaryembedded.com/comms/encryption/securing-military-gps-spoofing-jamming-vulnerabilities#:~:text=How%20secure%20is%20military%20GPS%3F,be%20spoofed%2C%20Fischer%20points%20out..> [Accessed 21 Nov 2022].