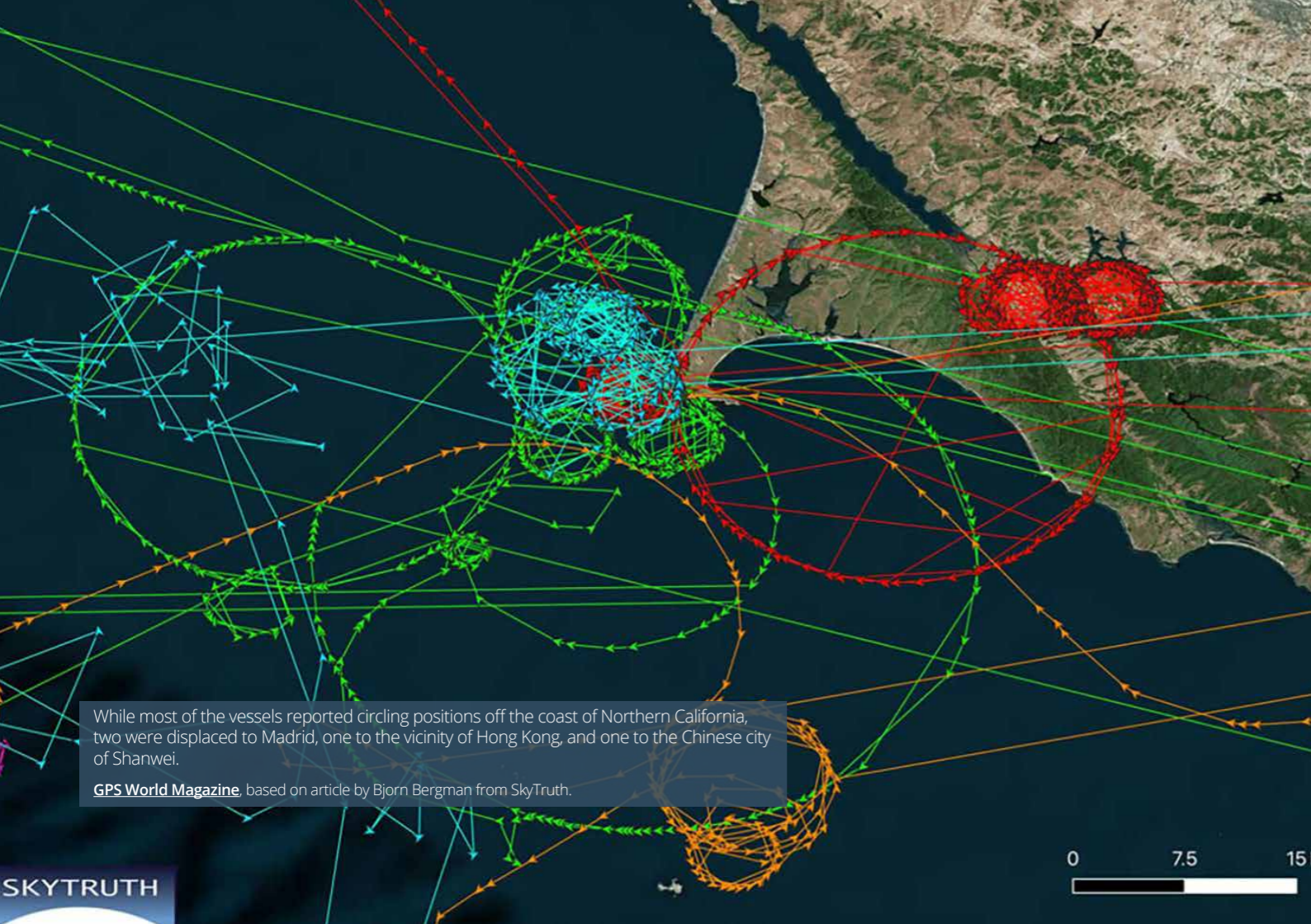




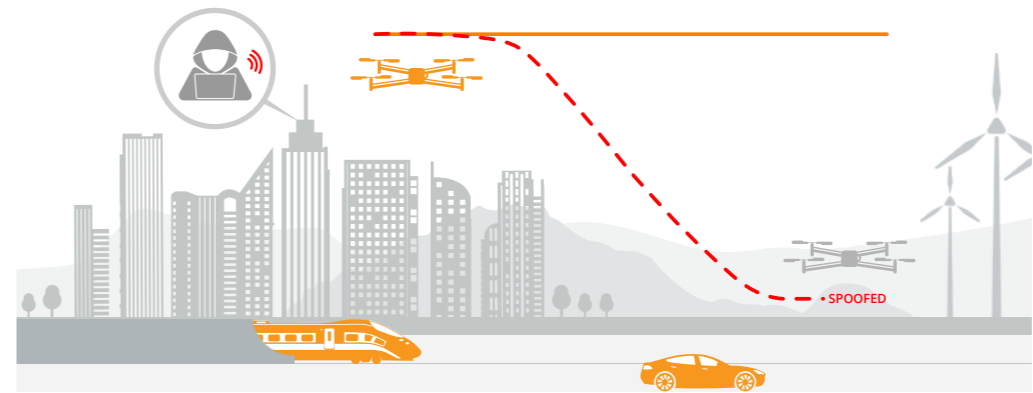
# GNSS Spoofing



While most of the vessels reported circling positions off the coast of Northern California, two were displaced to Madrid, one to the vicinity of Hong Kong, and one to the Chinese city of Shanwei.

GPS World Magazine, based on article by Bjorn Bergman from SkyTruth.

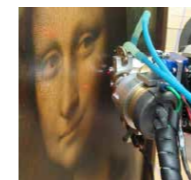
## GPS spoofing: what is it and why is it a concern?



A spoofer misleads a target GPS receiver and takes over positioning or time of the whole system. For applications such as autonomous vehicles as well as critical infrastructure, this poses a serious vulnerability.

### False signals result in false positions

During a spoofing attack, a nearby radio transmitter sends fake GNSS signals to the target receiver, fooling it into believing it is at a false location. By the time signals from GNSS satellites reach the Earth they are quite weak and can easily be overpowered by signals in the same frequency range transmitted from nearby.



Faking a GNSS signal is not much different to making a fraudulent painting, it looks very similar to the real thing, but can be uncovered by experts who know what to look for.

### All you need to know about GNSS spoofing

This brochure explains the following concepts in a simple and visual way:


- Which applications are most vulnerable to GPS spoofing and why
- What are the different ways to spoof a GPS receiver
- Latest detection and mitigation mechanisms
- Building resilient sensor fusion systems in a cost-effective way

# GNSS Spoofing: a real and increasing threat


The timeline below shows various spoofing events from around the world which have come on the news over the last years. Unfortunately, as technology advances, spoofing events are becoming increasingly common. The risk of spoofing varies depending on the GNSS use case, and it is up to the integrator to balance the risk and protection technology. For different use cases, different types of protection may be suitable.



## Some hazards posed by spoofing





**Drones** are often pre-programmed to land if they enter a restricted zone (geo-fencing). By making the drone believe that it is at an airport, the drone can be landed and stolen.



**Data centers.** internet, and financial institutions rely on GNSS time, which can be spoofed in a similar way to positioning, causing network interruptions or inaccurate timestamping of financial transactions.

**Container yards** are located close to ports and ships and may be affected by direct or indirect spoofing, which can cause operational interruption or wrong tracking data.


As seen in numerous cases of AIS (Automatic Identification System) data, spoofing GPS receivers which are aboard **ships** can bring vessels off course or even cause collisions.




**Autonomous shuttles** transport people around busy places. Any deviation from the route can have serious repercussions.




**Autonomous haul trucks** are used in mines to increase safety. If they are manipulated to go off course, this can result in serious damage or loss of life.



**Ground robots** working around valuable infrastructure or people can be taken off course or out of their geofenced area.



**Drones** and machines operating near conflict zones can be captured or diverted, by a spoofing attack.



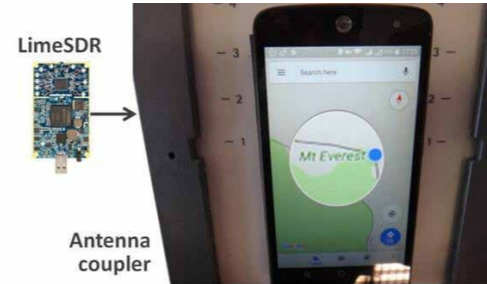
**Energy grids, telecom towers** and broadcast equipment are synchronized with GNSS time. Call drops and blackouts can be the result of tampering with these time sources.

## Why is spoofing becoming more commonplace?

### We all depend on GPS

Today so many of our devices, machines and critical infrastructure rely on GPS positioning or time. Spoofing can have serious repercussions in terms of safety and costs, and that is why spoofing is actually illegal in most parts of the world. Yet unfortunately spoofing incidents are still on the rise.

*"For cheating at Pokemon Go with a HackRF and spoofing, [one player] used the off the shelf GPS-SDR-Sim software, which is a GPS Spoofing simulator tool to be transmitted by SDR's like the HackRF and USRP radios" - [rtl-sdr.com](http://rtl-sdr.com)*



In the picture above a cheap LimeSDR is set-up with open-source software to transmit fake signals into the GPS of a mobile phone, making it believe that it is on Mount Everest.

### GNSS Spoofing, not rocket science any more

Increasingly available software and hardware allows for easier and quicker spoofer set-up. Open-source software for generating fake satellite signals is readily available online nowadays. Transmission of these fake generated signals can be done by an SDR (Software Defined Radio), which can easily be purchased online for under 150 Dollars/Euros.

## More sophisticated spoofing on the rise



### Advanced attacks require advanced countermeasures

While simple spoofing devices are becoming trivial to set-up, more sophisticated spoofing techniques use advanced GNSS simulators (as shown above) and transmission techniques. These sophisticated attacks are more difficult to detect and counteract and so require more advanced countermeasures.

*"GNSS Spoofing has been a concern in the defense domain for many years, but it's now starting to impact commercial and civilian users too. As more devices and autonomous systems rely on GNSS, and as spoofing know-how and equipment are now relatively easy to acquire, we'll see more unprotected systems fall victim to spoofing attacks."*  
*- [Guy Buesnel](#), PNT Security Technologist*

### Jamming goes hand in hand with spoofing

Spoofing is often accompanied by jamming, which disables GNSS signals by overpowering them with "white noise" interference. Jamming breaks the lock of receiver and GNSS signals making it more likely for the receiver to lock on to the fake signals. Jamming other signals during a spoofing attack, removes the possibility for a receiver to fall back on other signals. Thus, the first line of defense against spoofing is having good anti-jamming technology built into the receiver, such as [AIM+](#) Advanced Interference Mitigation.

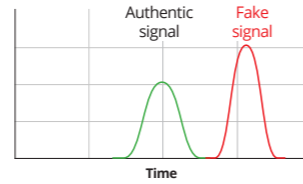


# Different forms of spoofing

There are various methods of spoofing with increasing levels of sophistication. The more sophisticated methods are also more difficult to detect and mitigate.

## Non-Coherent attack: the most basic method

This form of attack is fairly easy to set up with a cheap SDR and open-source software. Often non-coherent spoofing is preceded by jamming, to first break the "lock" with the real signal. The spoofing signal is not precisely synchronized with the authentic signal, however many receivers will acquire on it since it is more powerful.



Cost of equipment & effort need

Low

Likelihood of happening

High (intentional)

Set-up complexity

Low

Counter-methods (details on the next page)

Heuristics: continuity monitoring for time, power and positioning

Cryptography

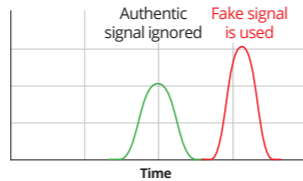
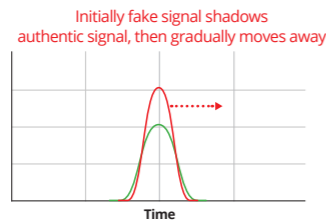
Spoofing sophistication  
Mona Lisa analogy



The quality of the Mona Lisa painting shows that this fake is easier to make, but it is also easier to detect. For example, checking for coordinate jumps can alert the system to this attack.

## Coherent attack: more complex

This type of attack first aligns the spoofing signal to a less powerful authentic GNSS signal and gradually delays it in time to take over receiver tracking. An attacker uses a simulator or similar equipment to create the spoofed signal. If highly advanced equipment is used and set-up is done well, it can be very challenging to detect.



High

Low (intentional)

High

Heuristics

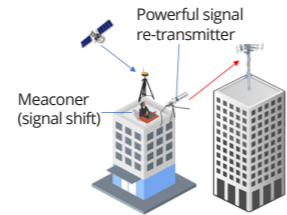
Cryptography



The fake Mona Lisa quality is improving, and one needs to look closer to see if something is wrong.

## Meaconing: signal re-transmission

This method intercepts and rebroadcasts recorded satellite navigation signals. This aims at making the receiver believe it is at the location of the antenna used to intercept the signal.



Low

Medium (intentional or unintentional)

Medium

Detection is difficult

Heuristic algorithms can detect this type of attack based on timing information

Polarized antenna



Meaconing is not very complex to set-up and is used for equipment testing. That is why meaconing can cause unintentional positioning disturbance, if the re-transmitted signals escape the test area. Meaconing detection is difficult because the spoofed signal is the same as the authentic signal. The Mona Lisa is actually a copy, but still separate from the original painting.

## Protecting receivers on many levels

These approaches can work together for a stronger protection or exist on their own. The first 3 approaches harden the GNSS receiver, while the 4th adds to a complete system protection.

### Multi-frequency GNSS: enhanced detection and mitigation



Having access to a multitude of signals such as GPS L1, L2, L5 and Galileo E1 and E5 enables the receiver to make thorough signal comparison and consistency checks. The spoofer would need to account for all these signals, to fool such receivers.

#### Falling back on other signals

The more “fallback” signals are available to the receiver the better quality of positioning will be once the spoofed signals are excluded. This means that even during spoofing the receiver could continue reliable operation.

### Heuristics: data analysis for inconsistencies

The receiver analyses data and uses algorithms to look for signal anomalies and inconsistencies. These sophisticated integrity algorithms require a vast amount of real-world data for accurate calculation of classification thresholds.

#### Built on data and experience

Similar to heuristics, art historians need to analyze replicas of paintings in detail to look for forgery. Heuristic algorithms are usually IP protected and vary in sophistication depending on receiver manufacturer.



**Septentrio technology protects receivers from spoofing on all levels**

### Cryptography: signature check for authenticity

By using cryptography and a digital key the signal can be “signed” by GNSS satellites, just as artists sign their own paintings. To check for authenticity this signature is then verified on the receiver side upon signal reception.

*La Vinci*

#### OSNMA from Galileo and other authentication services

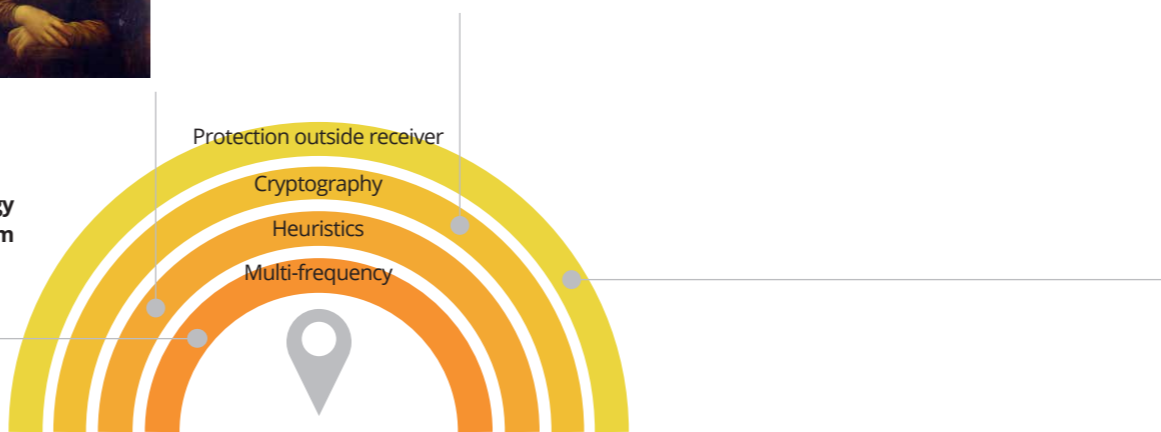
The European Galileo constellation is currently testing OSNMA (Open Service Navigation Message Authentication), which is planned to be operational soon. The GPS system will have a similar authentication service called Chimera. Galileo will be offering CAS, a Commercial Authentication Service for extended authentication access and control. Cryptography algorithms are CPU intensive and require powerful processing capabilities to run simultaneously with positioning/time algorithms.



### Protection outside of the receiver

Components, checks and services external to the receiver can be used to overcome spoofing:

- Navigation sensors like IMU, LiDAR or camera and checking their output against GNSS positioning
- Continuity checks (vulnerable to “pull-away attacks”)
- Anti-spoofing antenna like the dual-polarized antenna
- Services that provide additional information from satellites to authenticate all GNSS constellations, such as Fugro AtomiChron
- Anti-spoofing devices can be coupled with GPS receiver, but these can be expensive and could have side effects such as latency



## Spoofing resilience starts at the receiver core

For the most secure and cost-effective system protection, anti-spoofing should be designed-in from the start, and best at the receiver core. Adding anti-spoofing components and algorithms as an afterthought is less effective and more expensive. Just like anti-virus software, continuous improvements and upgrades of receiver firmware are needed to maintain a high level of security.



### Most efficient and cost-effective protection at receiver core

Anti-spoofing protection on the receiver level is the most effective approach. Built-in protection technology such as Septentrio AIM+ operates on signal level, performs checks which can not be done afterwards and can handle sophisticated attacks. The costs of other sensors and additional hardware components is avoided.



### Security on various system levels for enhanced protection

Depending on the application and the risk of spoofing, additional checks and/or components can be added to an already hardened multi-frequency receiver. However, these add-ons are costly and do not offer sufficient protection on their own.

## AIM+ Anti-spoofing protection

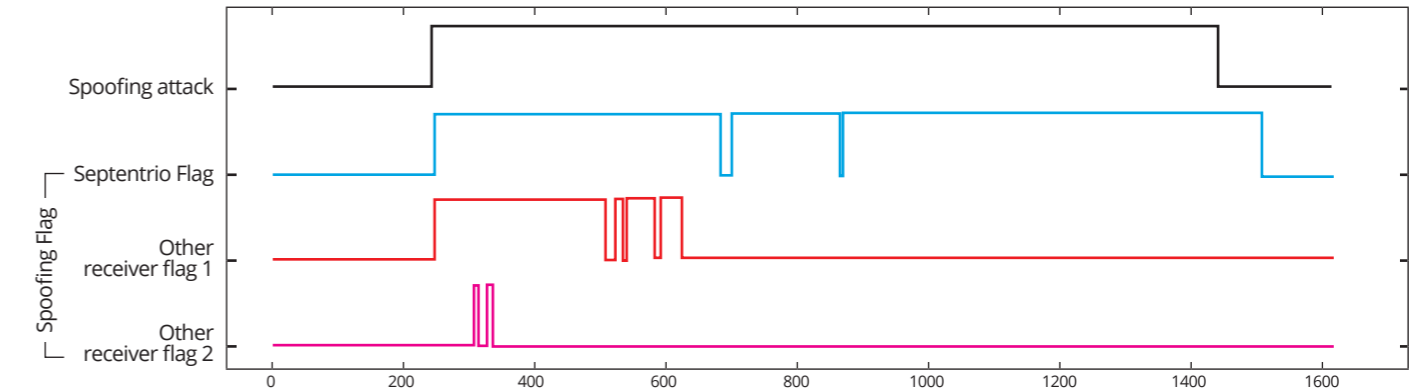
AIM+ anti-jamming and anti-spoofing technology is built into Septentrio receivers to protect them from false signals at the core using multi-frequency, heuristic and cryptographic approaches. Data collected over 20 years of operation ensures truthful spoofing flags. Spoofing is mitigated by discarding the false signals from positioning calculation and falling back on the multitude of other signals available, thanks to the multi-constellation triple-band technology.



## Spoofing resilience starts at the receiver core

### Monitoring a truthful spoofing flag for reliable operation

Autonomous systems which rely on multiple sensors need to continuously monitor the quality of each sensor for reliable system operation. If spoofing is detected on one of the signals a spoofing flag can be used to notify the system control unit, while the erroneous signal is discarded from positioning. If spoofing is coupled with jamming and cannot be mitigated by falling back on other signals, then the spoofing flag should be set and no positioning should be provided.



Three different receivers and their spoofing flags are shown. It is clear that the Septentrio receiver at the top is the only one with a trustworthy flag, which gives sufficient notification to the system about the spoofing attack. Warning: Heuristic algorithms based on insufficient amount of data are prone to overreact and set false spoofing flags, disturbing system operation.

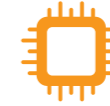
### Jump detection alone is not sufficient

To detect spoofing, many control system units and sensor fusion systems rely on an algorithm that checks for positioning jumps. However, this type of checks are vulnerable to pull-away attacks, where the spoofer gradually changes positioning information. It is extremely challenging to set the thresholds of such algorithms to effectively detect spoofing, while avoiding false positives.



Since IMUs rely on GNSS for initialization and absolute positioning, spoofing could have a serious impact on the system-level positioning or time in GNSS/INS systems.

## Why Septentrio?



Anti-spoofing security at the multi-frequency GNSS core, ensuring resilience of your whole system.



Leveraging cryptographic methods available on certain satellite signals, including [OSNMA](#).



Two decades of expertise and field implementation of anti-spoofing and anti-jamming technology.



Integrated anti-spoofing and anti-jamming, no additional hardware, calibration, or special antennas needed.



Continuous improvement of anti-spoofing technologies and secure communications.



Truthful spoofing flag set by proprietary algorithms, avoiding false positives.

Learn more about GNSS spoofing and jamming visit [septentrio.com/resilience](https://septentrio.com/resilience)







# septentrio<sup>o</sup>

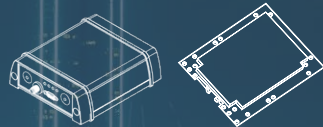
Accurate

Reliable

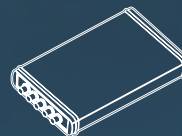
Available



**mosaic**  
GNSS receiver  
module



**AsteRx**  
OEM & enclosed  
GNSS receivers



**PolaRx**  
Reference  
receivers



**Software**  
GNSS software  
solutions

**EMEA**

Greenhill Campus (HQ)  
Interleuvenlaan 15i  
3001 Leuven, **Belgium**

Espoo, **Finland**

**Americas**

Suite 200  
23848 Hawthorne Blvd  
Torrance, CA 90505, **USA**

[septentrio.com/contact](https://www.septentrio.com/contact)

**Asia-Pacific**

Shanghai, **China**  
Yokohama, **Japan**  
Seoul, **Korea**

[septentrio.com](https://www.septentrio.com)



Septentrio Spoofing Brochure V1.

Specifications subject to change without notice.

Certain features and specifications may not apply to all models. © 2023 Septentrio