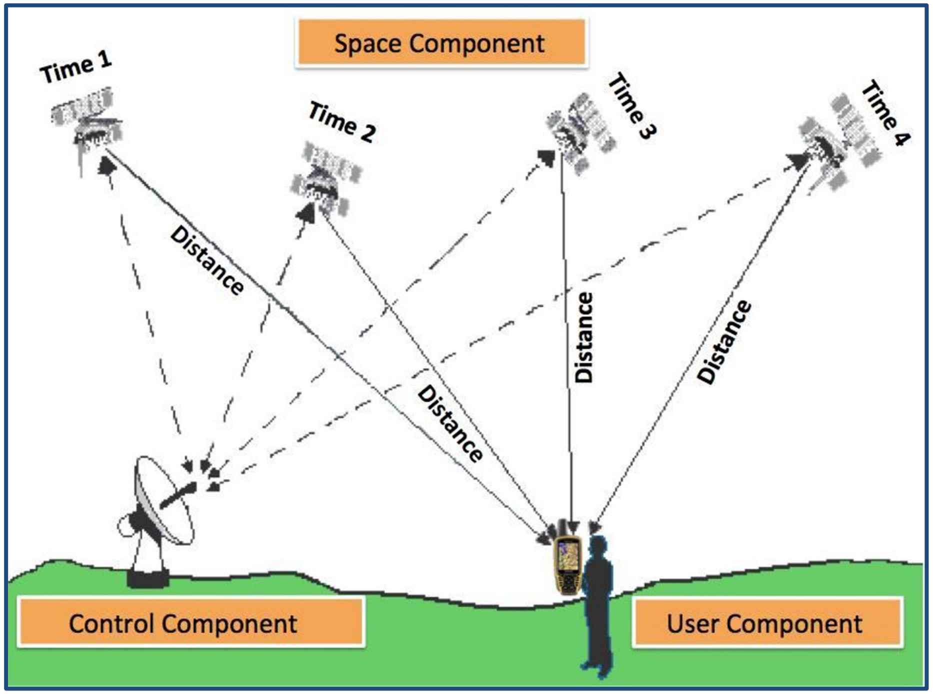
Global Positioning System Security - Manipulating Receivers

Matthew Miles, Peter Zhang

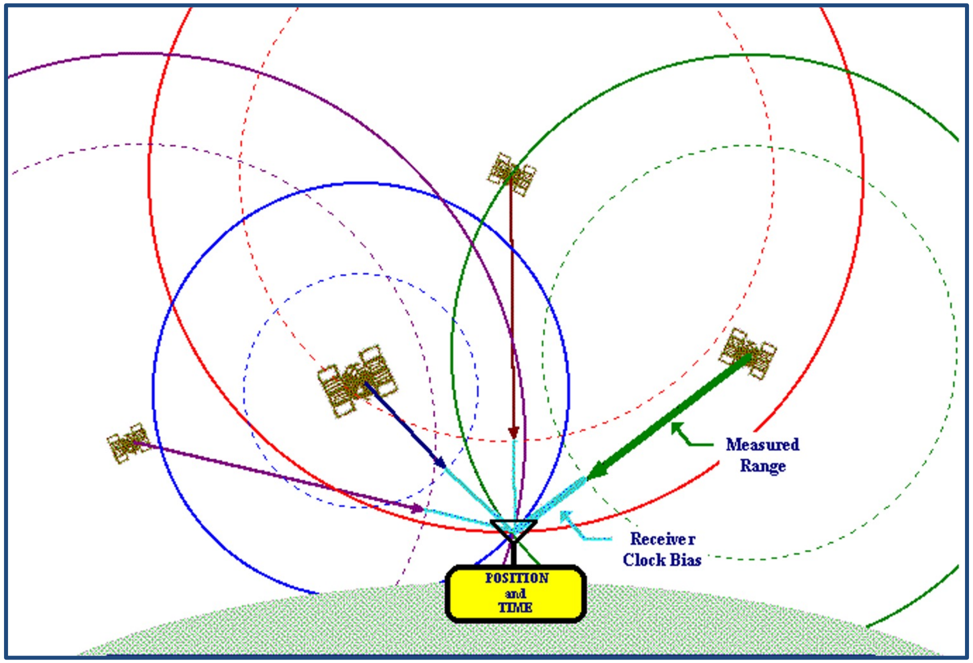
Overview

The Global Positioning System (GPS) is a U.S. owned utility that provides users with positioning, navigation, and timing (PNT) services. This system consists of three segments: the space segment, the control segment, and the user segment. The U.S. Space Force develops, maintains, and operates the space and control segments.



Functionality

GPS satellite installations (~31 in total) transmit a unique signal* to the user segment. The receiver decodes the signal and calculates satellite location. By tracking overlapping satellite signals and comparing changes of frequency from the doppler effect, a position can be determined via trilateration.



Philosophy

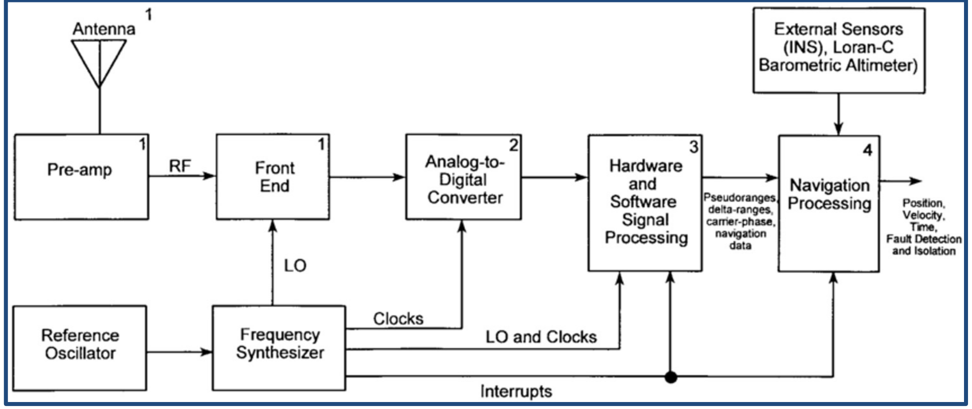
We will focus on the User Segment for the sake of our security analysis. Control and Space Segment functionality is separate from GPS User Segment. One way connection.

- Can stay functional separate from GPS functionality: isolated and tamperproof; access, similar to other restricted systems government regulated, is restricted and non-bypassable, etc

Conversely, the User segment security depends on the receiver. Often designed with little consideration for security as it only pings the Space Segment with minimal functionality → the relay can be tricked with relative ease.

Left: Generic GPS receiver block.

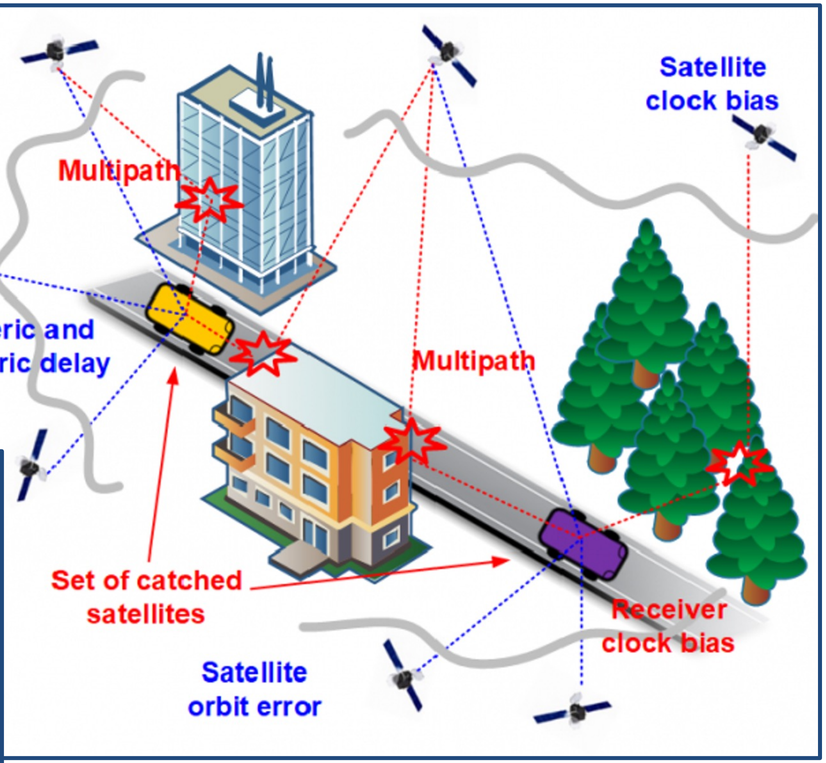
- 1) Antenna passes specific signal
- 3) satellites tracked in separate channels
- 4) Sensory data is integrated externally


Antenna
1
External Sensors (INS), Loran-C Barometric Altimeter)
Pre-amp
1
RF
Front End
1
Analog-to-Digital Converter
2
Hardware and Software Signal Processing
3
Pseudoranges, delta-ranges, carrier-phase, navigation data
Navigation Processing
4
Position, Velocity, Time, Fault Detection and Isolation
LO
Reference Oscillator
Frequency Synthesizer
Clocks
LO and Clocks
Interrupts

Impact on Reliability

Though originally drafted for military use, and thereby having bedrock security architecture in mind, the expanded use of GPS patching → less security focused. Issues satellite works to fix

- Receiver Quality (clock timing)
- Poor Satellite Positioning
- Physical Impediments



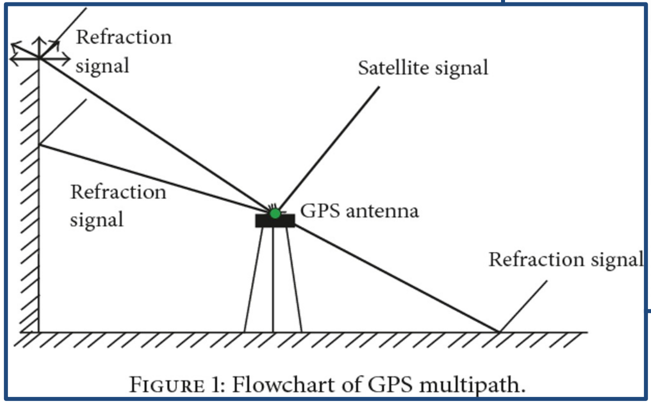


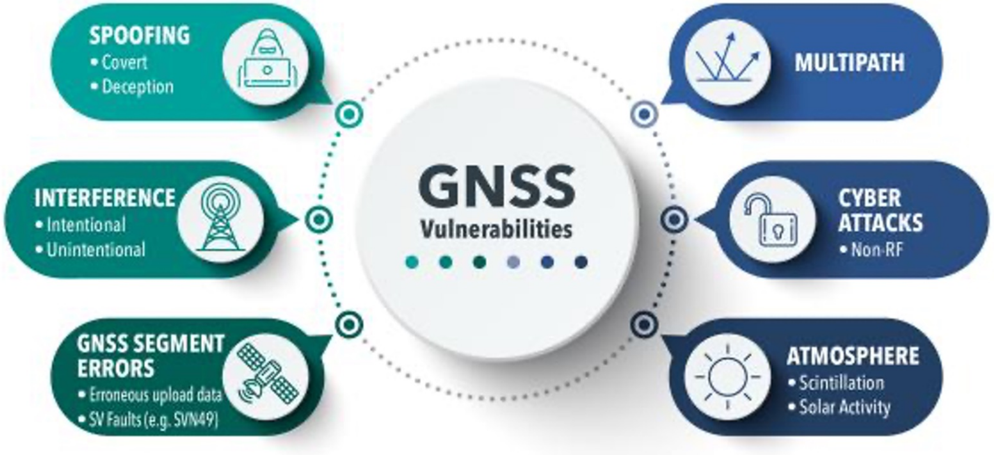
FIGURE 1: Flowchart of GPS multipath.

Threats

Third parties actively attempt to compromise the integrity of GPS time in the form of actions such as:

GPS spoofing: Someone broadcasts a fraudulent GPS signal and transmits it at high power to overwhelm the client receiver

GPS jamming: The transmission of noise in the same frequency range used by civilian GPS to stop receivers from obtaining and holding a lock on a signal



Threats - GPS Spoofing

GPS spoofers overpower weak GNSS signals, which helps them hack the system and display the wrong coordinates. There are two types of GPS spoofing:

1. Rebroadcasting GNSS Signals (Meaconing): This takes an existing signal (which may have happened in another place and another time) and rebroadcasts it.
2. Modifying Satellite Signals: This takes an existing signal, modifies, and transmits it.

Used to confuse or mislead users.

Threats - GPS Spoofing

GPS spoofing on android, iOS, Linux, Windows, and macOS is dangerous as it allows fraudsters to fake their location and commit crimes. We know that military GPS spoofing is used for legal purposes. However, it also encourages the practice of deception and crimes.

1. Global businesses use geo-blocking techniques to limit the usage of their services within specific territories. However, GPS spoofing can bypass these restrictions, causing losses to the companies.
2. Gaming industry: Pokemon Go as a example. Players spoof their location to gain unfair advantages against other players.
3. Companies like Uber and Doordash are heavily reliant on GPS locations. Their drivers/delivery people could fake their location and make money off of it. Detrimental to their brand image and customer retention rate.

Threats - GPS Jamming

The transmission of a noise signal across one or more of the GPS/ GNSS frequencies to raise the noise level or overload the receiver circuitry and cause a loss of lock.

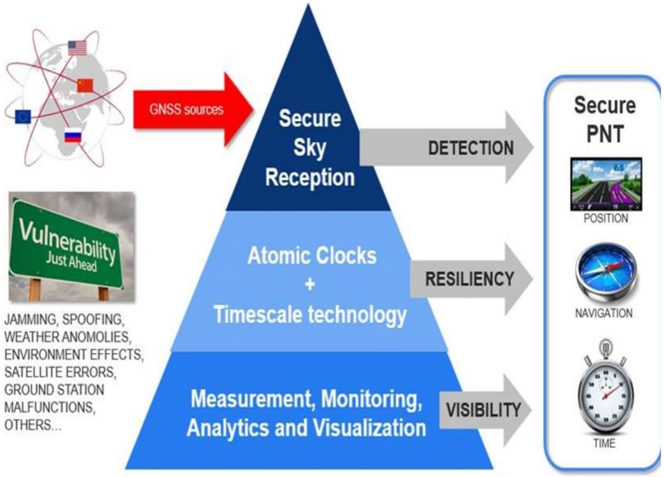
1. Commercial jammers, which might be used by car thieves, those keen to avoid road tolls, and commercial drivers not wanting to be tracked by their bosses
2. In January 2007. Technicians jammed radio signals on two Navy ships in San Diego during training exercise. GPS services were significantly disrupted throughout San Diego. Impacts included Naval Medical Center emergency pagers stopped working, the harbor traffic-management system used for guiding boats failed, airport traffic control used backup systems and processes to maintain air traffic flow, cell phones users had no signal, and bank customers trying to withdraw cash from ATMs were refused.

Spoofing Mitigation Techniques

GNSS receivers need to *detect* spoofed signals out of a mix of authentic and spoofed signals. Once a satellite signal is flagged as spoofed, it can be excluded from positioning calculation.

Various countries invest in spoofing resilience by building security directly into their GNSS satellites. With OS-NMA (Open Service Navigation Message Authentication), Galileo is the first satellite system to introduce an anti-spoofing service directly on a civil GNSS signal.

OS-NMA is a free service on the Galileo E1 frequency. It enables authentication of the navigation data on Galileo and even GPS satellites. Such navigation data carries information about satellite location and if altered will result in wrong receiver positioning computation.


GNSS sources
Vulnerability
Just Ahead
JAMMING, SPOOFING, WEATHER ANOMOLIES, ENVIRONMENT EFFECTS, SATELLITE ERRORS, GROUND STATION MALFUNCTIONS, OTHERS...
Secure Sky Reception
Atomic Clocks + Timescale technology
Measurement, Monitoring, Analytics and Visualization
DETECTION
RESILIENCY
VISIBILITY
Secure PNT
POSITION
NAVIGATION
TIME

Anti-Spoofing Rules

1. Obscure antennas: Install GNSS antennas in areas where they are not visible to the public.
2. Install decoy antennas: Put up clearly visible decoy antennas far enough from real ones that spoofing attacks won't interfere with legitimate signals.
3. Carefully choose antenna locations: Antenna location should have a clear view of the sky.
4. Add redundant antennas: Two or more antennas at different ends of a building or a ship to allow an organization to spot problems and switch to backup navigation systems.
5. Use backups: Rubidium or Cesium clocks can serve as backup timing systems and inertial sensors can help determine position until GPS reception is restored.
6. Practice good cyber hygiene: Organizations should consider keeping GNSS receivers and associated equipment offline whenever network connectivity isn't required.

Jamming Mitigation Techniques

1. Vestigial Signal Detection method

Used for spoofing mitigation, subtracts the local code and carrier replicas from buffered samples of composite received signal and then repeats the acquisition in order to detect and acquire suppressed signals from GPS satellites.

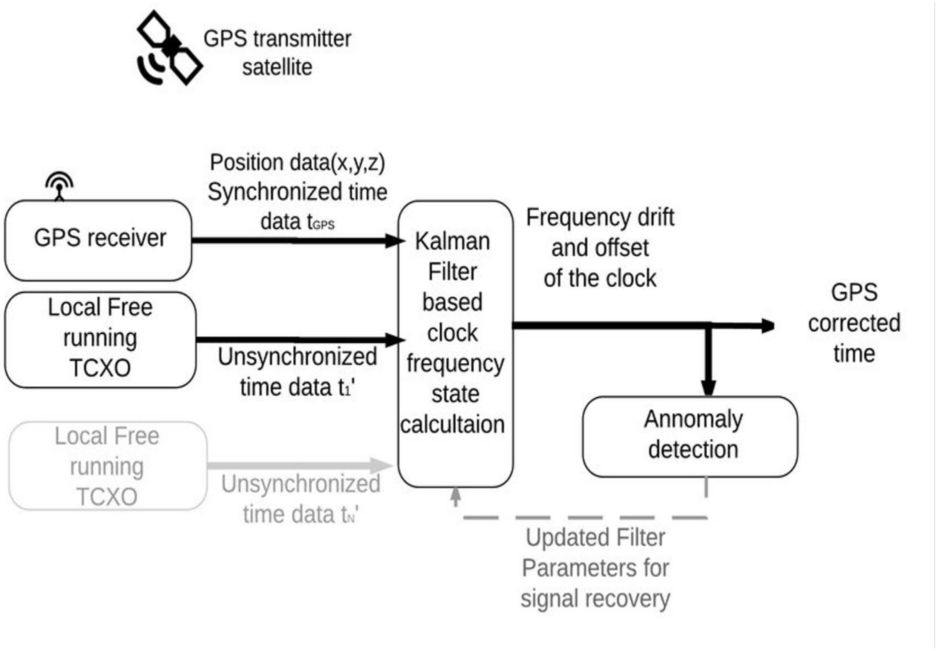
1. Anti-Jamming Device

GPS Anti-Jamming protects GPS receivers from interference and intentional jamming. By the time the GPS signal reaches the Earth's surface is weak and is susceptible to being overcome by higher power Radio Frequency (RF) energy. Even a small jammer of about 10 Watts power can disrupt an unprotected C/A Code receiver for about 30 kilometres (line of sight). GPS Anti-Jamming uses power minimization to reduce the effect of interference and jamming so that the GPS receiver can continue to operate correctly.

On-Board Spoof Protection Integration

Design of a proposed secure GPS receiver with on-board spoofing detection.

- Single (or multiple) free running temperature controlled oscillator(s).
- Time from each free running oscillator can be used for generating a stable virtual clock.
- Anomalies in the frequency drift and offset of this single clock (or the low noise virtual clock) calculated with respect to the GPS signal can reveal spoofing attacks on GPS signal.
- Updated filter parameters can help to reconstruct the approximated true time-offset during a spoofing attack.


GPS transmitter satellite
GPS receiver
Position data(x,y,z) Synchronized time data t_{GPS}
Local Free running TCXO
Unsynchronized time data t_1'
Local Free running TCXO
Unsynchronized time data t_N'
Kalman Filter based clock frequency state calcultaion
Frequency drift and offset of the clock
GPS corrected time
Annomaly detection
Updated Filter Parameters for signal recovery

References

- GPS Threat Mitigation: Why Network Time Users Should Care — Masterclock, Inc.
- GPS satellite over the Earth - The Global Positioning System
- How Does Global Positioning System (GPS) Work? » Science ABC
- https://www.microsemi.com/company/technology/gps-threat-protection-and-security\
- (a) Simplified BPSK DSSS transmitter block diagram. Points (a), (b)
- Design of the proposed secure GPS receiver with on-board spoofing... | Download Scientific Diagram
- Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing - ScienceDirect.
- How GPS Works (Step-by-Step) | Trakkit
- Everything You Need to Know About GPS Spoofing | EasyDMARC
- What is spoofing and how to ensure GPS security?
- What is GPS spoofing? And how you can defend against it | CSO Online