GPS spoofing and time

Aril Johannes Schultzen

August 16, 2016

Contents

1 Global Positioning System: A short introduction

The Global Positioning System (GPS) is a utility owned by the United States that provides its user with positioning, navigation and timing services. At the end of 60's, the U.S Navy was developing the Polaris missile, a missile capable of being launched from a submarine. One of the requirements for launching the Polaris missile was exact knowledge of the submarines position. The problem led the Navy and The Applied Physics Laboratory at Hopkins to develop the Transit system, the earliest predecessor to the GPS system [**SteJ**].

Today, roughly 40 years later we are surrounded by GPS technology. In fields like emergency response, search and rescue, fleet management and even agriculture, it has become a vital tool of utmost importance to everyday operation. Satellite navigation can be found in most new cars and few phones are today sold without an internal GPS receivers. The European Space Agency estimated that there were 2 billion GPS enabled devices by 2012 [**ESA**]. What started out as a navigation tool for the U.S navy is now used by millions, if not billions of users both civilian and military all over the globe. A common misconception (that is often reinforced by Hollywood action movies) is that the GPS satellites track *you* by communicating with your GPS receiver. It actually works the other way around. You are, with your GPS receiver, tracking a set of satellites in order to establish your own position. At any given time, there are at least 24 GPS satellites each in its own orbit at about 11,000 nautical miles above your head [**GPSGOVSS**]. In order for a GPS receiver to determine its position and obtain correct time, it will need 4 GPS satellites within line of sight [1]. The method used by your GPS receiver to determine its position is called *trilateration*. Trilateration is used in geometry as a process of determining the location (absolute or relative) of point by measuring distance. It is often

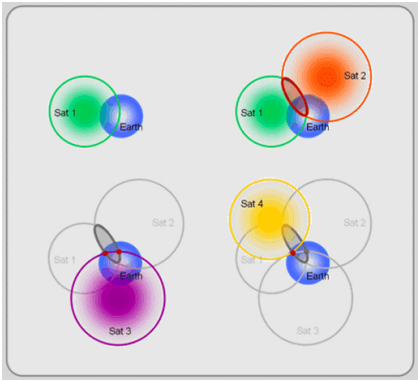

*Figure 1: Figure showing how GPS satellites are used to trilaterate to determine a GPS receivers position. Source: [***GISTRILATERATE** *]*

[1] The line of sight requirement might seem unreasonable, but by the time the signal has reached earth, is has degraded to a minimum of -160 dBW [**NATINT**]

confused with triangulation which instead of distance, uses angles. Measuring the distance from the GPS satellites to a given position on earth is quite simple when using the equation:

$$Distance = Rate \times Time \tag{1}$$

The equation is simple to solve, first we need the rate. In this context, the *rate* is how fast the signals travel. This is equal to the speed of light (299,792,458 m/s). The time the signal has used traveling from the satellite to earth can be obtained by analyzing the signal itself. A simple and slightly inaccurate description is the signal contains a "time stamp" of when the signal was sent. By comparing this time stamp with the current time, one can calculate the age of the signal and therefore how long it has spent traveling. This is explained in greater detail under (3) [**GPSGOVTE**].

2 Clocks

What does a $10 wristwatch and a $100 000 atomic clock have in common? They don't stay accurate forever. This phenomena known as *frequency drift*, is when a clock no longer runs at the exact same speed as a reference clock and they drift apart.

This property is a result of how they track time. In essence, all clocks work in the same way. They have a part that oscillates, a way to count the number of oscillations and a way to show the count. If we transfer this analogy to the typical "grandfather clock", the pendulum would be the oscillator, the counting mechanism the clockwork and the clock face and dials would be the display. In a typical wristwatch, the oscillator is a quartz crystal powered by a battery. The frequency of which the crystal oscillates is then divided down to a single Hertz by simple electronics. The purity of the crystal is among the decisive factors determining the accuracy of the clock. [**CSMG**]. Although a completely different beast, the same principles apply to the atomic clock which uses the microwave radiation that electrons in atoms emit when they change energy levels. One of the most commonly used elements in atomic clocks,

*Figure 2: High pure Caesium crystals in ampule under argon. Source: [***DENCES** *]*

is *caesium-133*, an isotope of caesium.[2] [**HP**]. Bear in mind that this is of course an extremely limited explanation.

3 GPS signals and Time

During the introduction of this essay the properties of GPS as a tool for navigation was made apparent. This is however not the only use of GPS, it is also used for timing. The GPS satellites transmits a *Coarse/Acquisition (C/A)* code and a restricted *Precision (P)* code. The C/A code is freely open for everyone and is transmitted at the L1 carrier frequency (1575.42 MHz) and the P code is transmitted at both L1 and L2 (1227.60 MHz) and is reserved for the military. The C/A code is a 1023 bit pseudo random code that is transmitted at 1.023 Mbit/s, which means it repeats itself every millisecond. Each satellite transmits a different pseudo random code, codes that does not correlate well with each other. This is important because it makes it possible to separate the satellites from each other. The way the receiver calculates its position was briefly mentioned during the introduction and is better explained here. The receiver calculates the distance from itself to the satellites by comparing the pseudo random code received from the satellite with an identical one it generates itself. The receiver "slides" these codes over each other further and further until they match up. The signals travel time is determined by how far the codes had to be slided before the matched. This is what is called *Code-phase GPS* and it has got some problems. Since the codes have a wide cycle width, almost a microsecond, there is a lot of slop and at the speed of light, a microsecond wrong is roughly 300 meters wrong. What many receivers do is that they start with the code-phase and moves on to using measurements based on the carrier frequency. Since the frequency is much higher, the slop decreases and the accuracy increases dramatically. This is whats known as *Carrier-phase GPS*.

Alright, but what about time? We have already established that the key to GPS is measuring the travel time of a radio signal, but considering the consequences of a couple of microseconds of slack when dealing with light-speed, it is really putting some pressure on the GPS receivers internal clocks. As previously mentioned, all your receiver needs to do to find its position in a three dimensional space, is three GPS satellites. If the GPS receivers internal clocks where perfect, the three satellite ranges would intersect at a single point, your position. But in the real world our clocks is everything but perfect. One could use atomic clocks in the receivers but that would make the receivers too expensive (even though chip scale atomic clocks (CSAC) are

[2] 1 second equals 9,192, 631,770 cycles of the Cs-133 transition

becoming increasingly affordable 5.2.9) for anyone to buy. The solution is to make a fourth measurement from a fourth satellite. This measurement will not intersect with the first three when using an imperfect clock. The receiver can then try to find a correction factor it can subtract from its timing measurement in order to make the measurements intersect. By doing this, it also brings the receivers clock back to sync with universal time. With the correct time, it can also make correct and precise positioning. [**TRIMBLETIME**]

4 Phasor Measurement Units

An example of an application relying on GPS derived time is a PMU (phasor measurement unit).A PMU analyzes the waves on the electrical grid and uses a common time source for synchronization. This synchronization allows for real-time measurements between multiple points in the grid by multiple PMU's. The common time source (and why PMU's are relevant) is often obtained by using GPS. [**YLJRNR**] The value of such a device is understood clearer by recognizing that the power grid is a complex, interconnected, interdependent network. In other words, errors and abnormalities in one part of the grid will have an effect on operation elsewhere and in some cases lead to whole spread blackouts [**EVPMUGA**].

5 Threat Models and countermeasures

The thread models and countermeasures presented in this paper are based on the article *Reliable GPS-Based Timing for Power Systems: A Multi-Layered, Multi Receiver* by L. Heng, D. Chou and G. Xingxin Gao (2012). The only exception is our proposed countermeasure under 5.2.9.

5.1 Threats

5.1.1 Jamming

By emitting a high-power signal at the frequencies used by GPS satellites, one can interfere with the signals received by the GPS receiver, effectively denying GPS receivers use of these signals. These signals are already weak considering their travel from space. Such an "attack", although effective, is pretty naive and easily recognized by the jammed party. If your equipment is operational and you don't have a signal, you are probably being jammed.

5.1.2 Signal-level Spoofing

Signal-level spoofing is when an attacker causes a receiver to loose lock on an authentic GPS signal by overpowering it with a false signal. This can be achieved by using a GPS simulator that matches the authentic signals phase, code delay and encoded data [**SGRCOOPMU**]. Knowing the signal that the victim is receiving is important in order to successfully spoof it. To anyone with access to the military-grade GPS signals, this is less of an issue since their signals are encrypted and harder to spoof, the civilian frequencies on the other hand are publicly known and readily predictable. Shepard, Humphreys and Fansler (2012)[**EVPMUGA**] describes in their paper *Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks*, a way to successfully spoof a GPS signal used by a PMU. They describe how they "introduce" the counterfeit signal to the victim by adjusting the power of the signal below the victim receivers noise floor and then gradually raises it until it surpasses the authentic signals strength. Once the victims receiver locks on, the attacker has gained full control.

5.1.3 Data-level Spoofing

In data-level spoofing, the contents (data) of the GPS signal are manipulated. GPS signals includes ephemeris data used to solve the positions of each satellite in orbit and also the time and status of the satellite constellation. By altering this data, the receiver solves incorrect velocity, location and most important in this context, clock offset.[**SGRCOOPMU**]

5.1.4 Replay spoofing

Replay spoofing (or *meaconing*[3]) is a technique where GPS signals are intercepted and rebroadcasted. The rebroadcast can be delayed and used to confuse navigation or to cause delay in applications relying on GPS signals for time.

5.1.5 Malfunctions

Just like any tool or device, a GPS receiver is prone to failure. This threat may not be posed by an external party, but is still a threat to normal operation. The ability to differentiate between an attack and a malfunction is important when deciding how to respond to such an event.

[3] *Meacon* is portmanteau of *Masking Beacon*

5.2 Countermeasures

5.2.1 Monitoring Signal Power

In any kind of attack, jamming or spoofing, a counterfeit signal must overpower the authentic signal in order for the receiver to lock onto it or in the case with jamming, denying access to the authentic signal. By monitoring the strength of the signal and detecting a spike or rise in signal power, a possible attack can be identified. This is a low-cost, low-complexity and independent (in contrast to for example using other receivers as a reference) countermeasure. It is however because of the unpredictable nature of signals, not considered to be a detection confident countermeasure and should therefore only be used along side other countermeasures.[**HengChouGao14**]

5.2.2 Checking solved position against known position

By checking the position solution against the known position of the receiver, both receiver errors (5.1.5) and a replay spoofing (5.1.3) attack can be detected. It does however fall short when more sophisticated techniques like Data and Signal-level spoofing (5.1.3,5.1.2) are used. These kind of attacks when done properly (unless it's done with intention), will not alter the solved position. It is important to note that this only relevant when only using *one* receiver. If the position solution from multiple receivers deployed in the same area are cross-checked, this countermeasure can still be considered effective. Consider the following scenarios when using 3 receivers:

- **None of the receivers are spoofed:** Each receivers solved position matches their respective known position. They all solve the same time.
- **One or two receivers are spoofed:** The spoofed receiver(s) solve(s) different time compared to the receiver(s) not being spoofed.
- **All the receivers are spoofed:** As long as they are spoofed by the same spoofer, they will solve the same time but also the same position which again makes it possible to detect the attack.

A possible way to for a attacker to avoid detection would be to use one spoofer per receiver. These spoofers would need to be synchronized and their signal power fine tuned to make sure that they only spoof their respective receiver. It is believed that such an attack would be too complex and costly to be considered practical. [**HengChouGao14**]

5.2.3 Checking time solutions against receiver clock statistics

By comparing statistics created by monitoring the receivers clock with the time solution, one can detect spoofing (5.1.2,5.1.3) as well as malfunctions (5.1.5). This is because the time solution is unlikely to be consistent with the statistics in event of an attack. Since this countermeasure relies on the receivers clock which can be described as both unpredictable and stochastic, it should only be used along side other countermeasures.[**HengChouGao14**]

5.2.4 Cross-checking navigation data among receivers

When under a data-level spoofing attack (5.1.3), the navigation data is modified. By comparing one GPS receivers navigation data with another, both data-level spoofing and malfunctions (5.1.5) can be detected. This countermeasure can also prove useful during jamming attacks (5.1.1) because a jammed receiver could use the data from other receivers in the event that is unable to correctly decode navigation, but still able to track satellites. This may enable the receiver to continue operation during an attack. [**HengChouGao14**]

5.2.5 Comparing navigation data and reverse-calculated satellite positions

The PMU GPS receivers are never moved and their position is known. By using their pseudorange measurements, the satellites positions can be reverse calculated by using trilateration. Since the reverse-calculated positions only match the positions calculated from the navigation data when both pseudorange and navigation data is correct, one can effectively detect replay spoofing (5.1.4) and malfunctions (5.1.5). Its also worth noting that this countermeasure increases the difficulty of both signal and data-level spoofing (5.1.3,5.1.2) because it narrows down the possible valid (seemingly) spoofing signals. [**HengChouGao14**]

5.2.6 Cross-correlating P(Y) code

This countermeasure assumes two receivers with at least 1 km distance from each other that tracks a signal from a satellite visible to them both. It is also based on the assumption that the encrypted military P(Y) code cannot be forged by a spoofer. The receivers use the C/A code phase and timing relationship to the P(Y) code to obtain two samples from the same time frame of the received P(Y) code and then correlate the two samples.

Even though the samples will be encrypted, noisy and perhaps distorted by narrow-band RF front-ends, a high correlation peak should be created when a cross-correlation is conducted as long as the receivers are not spoofed. A key conclusion of the research made by L. Heng (2013) as referenced by L. Heng *et alia* (2014) was that the probability of detection errors using this method decreased exponentially with the length of the samples made from the P(Y) code and the number of receivers used as reference. This method has therefore proved itself effective against spoofing attacks (5.1.3,5.1.2), but ineffective against replay spoofing because the rebroadcast uses authentic GPS signals with correct P(Y) code. It is important to note that the implementation of this countermeasure relies on the GPS receivers ability to output baseband samples and these samples ability to be transfered over a data network. Because the sampling rate of the samples are fairly high, it is recommended that the spoofing detection is done periodically instead of continuously. [**HengChouGao14**]

5.2.7 Position Aided (PIA) Tracking loops

Vector tracking is a receiver architecture that combine the tasks of signal tracking and position/velocity estimation into one algorithm. This is a contrast to the traditional way where the tracking methods track satellites independently as well as the position/velocity solution independently. Even though this requires more computing power, it increases immunity to interference and jamming. The vector tracking is aided by the fact the we know the PMU GPS receivers true location. The tracking robustness can be further improved by using a Kalman filter. Since a PMU and its GPS receiver remain stationary, the parameters of the tracking loops can be chosen to narrow the loop filter bandwidth which reduces noise and the effective radius of a potential jamming attack (5.1.1). Replay spoofing attacks will also fail since the PIA vector tracking depends on the knowledge of the GPS receivers true position. In the event of such an attack, the result would be that the vector tracking will fail to function. [**HengChouGao14**]

5.2.8 Multi-receiver tracking loops

Building on the idea from *PIA Tracking loops*(5.2.7) one can benefit from the networked nature of the GPS-timed PMU. In a multi-receiver vector tracking loop, many receivers process information in collaboration. A key conclusion of the research made by A. Soloviev *et alia* as referenced by L. Heng *et alia* (2014) showed that acquisition and tracking performance under low signal-to-noise ratio conditions was improved under multi-receiver signal

accumulation. Multi-receiver phased arrays also improved the robustness against both jamming (5.1.1) and spoofing attacks (5.1.2,5.1.3) by *"Forming beams to satellites and steering nulls in the direction of attacking transmitters"* (L. Heng *et alia* (2014), p.41). In addition to the increase robustness, it increases the ability to detect malfunction (5.1.5). A faulty receiver will usually not be consistent with other correctly functioning receivers. As with the countermeasure based on cross-correlating P(Y) code (5.2.6), this implementation also requires that the GPS receivers are able to output baseband samples. In this implementation, the samples need to be transmitted continuously among the receivers which requires a capable data network such as a typical LAN. [**HengChouGao14**]

5.2.9 Spoof proof CSAC SMACC

We propose to use a smart miniature atomic clock controller(SMACC) that controls a CSAC (chip scale atomic clock). Playing the role as the SMACC will be a Raspberry Pi running Linux with software that implements the following countermeasures:

Figure 3: Symmetricom SA.45s CSAC. Courtesy Symmetricom.

- Checking solved position against known position (5.2.2)
- Checking time solutions against receiver clock statistics (5.2.3)
- Monitoring Signal Power(5.2.1)

In theory, any atomic clock would suffice for our application. This would however be highly unpractical and also very expensive. We therefore propose to use the Symmetricom SA.45. This is a CSAC measuring only 16cc with 1 pulse per second (PPS) output and 1 PPS input (for disciplining) as well as a RS-232 interface. The SA.45's strength is it's low power consumption (less than 120mW) and low price [**SADS**]. It is important to note that the properties of the SA.45 is what makes our proposal feasible, not the manufacturer or the model. A CSAC with similar properties and specifications would of course also work for our proposal.

It is also important to note that this approach doesn't really do anything with the fact that you are being attacked, it simply tries to eliminate the effects of it. In a scenario where you are under attack weeks at a time, you

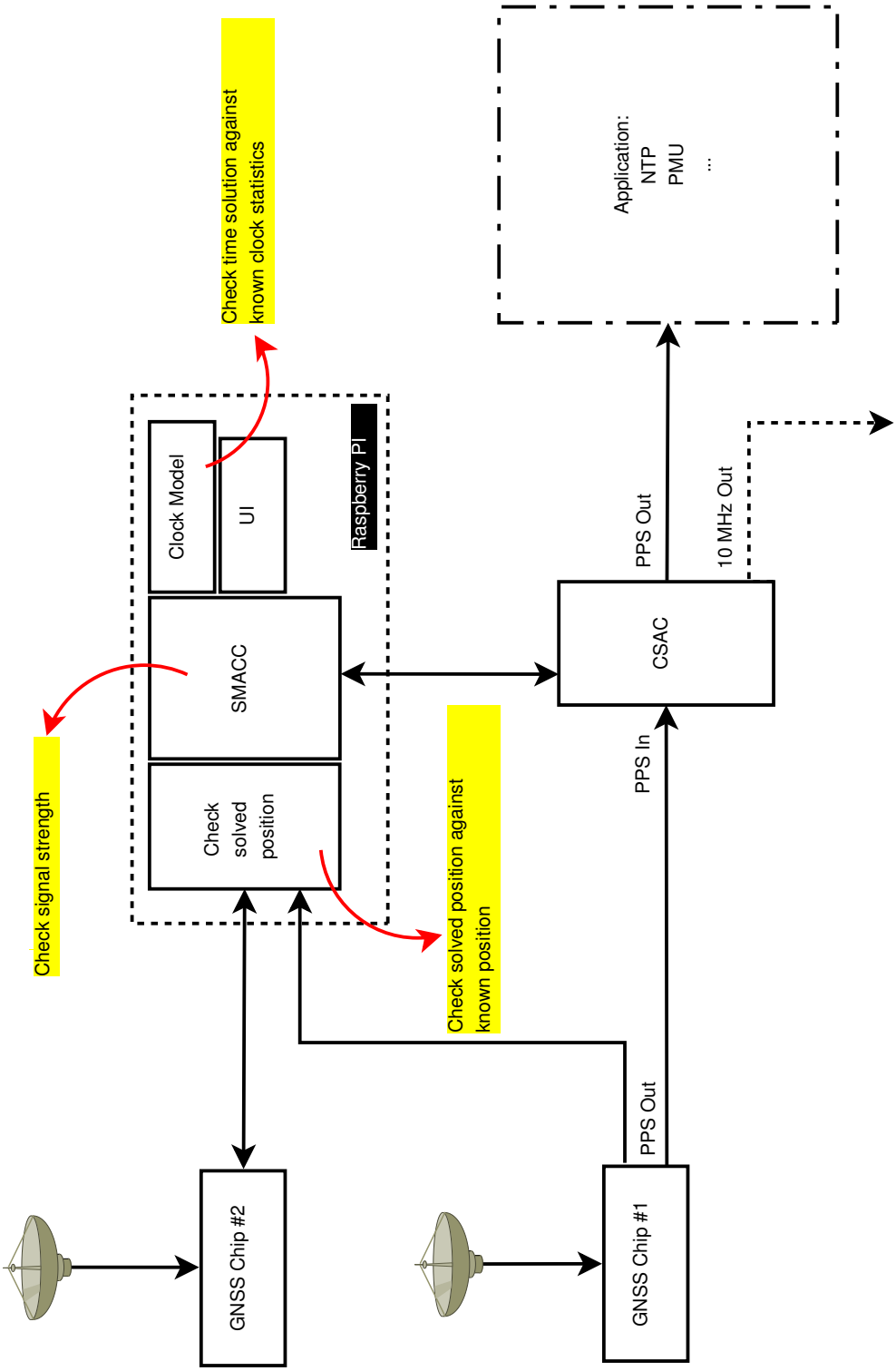

Figure 4: A block diagram of our proposed solution

will have to address the issue that you are under attack at some point. It is also important to notes that this countermeasure mostly apply to applications using GPS as a source of time. Having a stable clock during a jamming attack will not help you determine your position once you move (given that you are fully jammed).

5.3 Summary

The table (1) shows the different threat models and the effect of the countermeasures covered in this essay. Our proposed countermeasure is not yet tested, but is still included in the table reflecting the effect we believe it might have.

Table 1: The table shows the effectiveness of the covered countermeasures against threat models.

Counter Measures	Threat Models				
	JAM[4]	SLS[5]	DLS[6]	RS[7]	MF[8]
Monitoring Signal Power (5.2.1)	N	X	X	X	N
Check pos. solution (5.2.2)	N	Y	Y	Y	Y
Check time solutions (5.2.3)	N	X	X	X	X
Checking nav. data (5.2.4)	X	N	Y	N	Y
Reverse calculated sat. pos. (5.2.5)	N	X	X	Y	Y
Cross-correlating P(Y) (5.2.6)	N	Y	Y	N	N
PIA TL (5.2.7)	Y	N	N	Y	N
Multi-receiver TL (5.2.8)	Y	X	X	X	X
CSAC SMACC (5.2.9)	Y	Y	Y	Y	Y

Table 2: Legend for table (1)

Y	Effective	N	Ineffective	X	Auxiliary

[4]Jamming (5.1.1)
[5]Signal-level Spoofing (5.1.2)
[6]Data-level Spoofing (5.1.3)
[7]Replay Spoofing (5.1.4)
[8]Malfunctions (5.1.5)