GPS SPOOFING AND MITIGATION FOR PHASOR MEASUREMENT UNIT RECEIVERS

Houston Conley

Logan Rambert

June 2nd, 2022

Contents

Abstract

In this report, we describe our process and methodology for selecting a GPS Simulator to perform GPS Spoofing. The type of spoofing we would like to test is a technique to produce errors in the computed time-offset of the GPS receiver. The particular technique that we are interested in is to modify the GPS ephemeris in such a way that the spoofing attack is not detected, but a change in the computed time-offset is produced. To test this spoofing attack, we use a GPS simulator to modify the ephemeris and observe the time-offset at a receiver, through the use of a Software Defined Radio (SDR).

1. Introduction

Many large-scale systems, such as power-grids, make use of the high accuracy of GPS clocks to synchronize their systems. The area in which we are researching is GPS spoofing, where an attacker sends a hostile transmitted signal to a target receiver in hopes of tricking the receiving system into a different and inaccurate UTC time setup. This is done by altering the ephemeris of the receiver through overpowering the original signal by increasing the power of the hostile transmitted signal without being detected to change the position.

The purpose of researching this is to verify that the computed time offset of the GPS receiver can be spoofed by modifying the ephemeris. This research might be useful in the design of GPS security systems.

Through the contents of the upcoming chapters, we will discuss how we went about researching a GPS simulator, the methodology of how we verified our theories, the costs of our research, and our results from our research.

2. Methodology

In order to procure a GPS simulator appropriate for our research goals, we first needed to become familiar with the techniques used to perform the spoofing. Specifically, we needed to learn how the pseudorange calculations can be manipulated through the modification of the ephemeris. Several resources became particularly helpful in furthering our understanding of the pseudorange and ephemeris [1].

2.1 GPS Fundamentals

GPS (Global Positioning System) is a system that allows a receiver to determine its position on Earth by referencing GPS satellite locations. A total of four satellites is needed to compute the receiver’s location. In addition to location, a receiver also obtains time information. GPS satellites are equipped with highly accurate atomic clocks, and these clocks are used to compute position and time. The calculation of these values is obtained through the use of ephemeris data. This ephemeris data helps compensate for the various relativistic effects that influence computations such as position and time for orbiting bodies. These parameters are shown in Figure 1.

t_{0e}	Reference time of ephemeris
$\sqrt{a}$	Square root of semimajor axis
e	Eccentricity
i_0	Inclination angle (at time t_{0e})
Ω_0	Longitude of the ascending node (at weekly epoch)
ω	Argument of perigee (at time t_{0e})
M_0	Mean anomaly (at time t_{0e})
di/dt	Rate of change of inclination angle
$\underset{\cdot}{\Omega}$	Rate of change of longitude of the ascending node
$\mathbf{\Delta}n$	Mean motion correction
C_{uc}	Amplitude of cosine correction to argument of latitude
C_{us}	Amplitude of sine correction to argument of latitude
C_{rc}	Amplitude of cosine correction to orbital radius
C_{rs}	Amplitude of sine correction to orbital radius
C_{ic}	Amplitude of cosine correction to inclination angle
C_{is}	Amplitude of sine correction to inclination angle

Figure 1: GPS Ephemeris Data Definitions

The actual algorithm is shown in Figure 2. It produces an output necessary for pseudorange calculation, specifically x-y-z value coordinates. There are four pseudorange values computed, one for each of the four GPS satellites (shown in Figure 3). Along with each position location, a time offset t_u is computed. It is this time offset that our research is primarily concerned with.

(1)	$a = (\sqrt{a})^2$	Semimajor axis
(2)	$n = \sqrt{\frac{\mu}{a^3}} + \Delta n$	Corrected mean motion, $\mu = 398{,}600.5 \times 10^8 \ \ m^3/s^2$
(3)	$t_k = t - t_{0e}$	Time from ephemeris epoch
(4)	$M_k = M_0 + n(t_k)$	Mean anomaly
(5)	$M_k = E_k - e \ sin \ E_k$	Eccentric anomaly (must be solved iteratively for *E_k*)
(6)	$sin \ v_k = \frac{\sqrt{1-e^2} sin \ E_k}{1-e \ cos \ E_k}$ $cos \ v_k = \frac{cos \ E_k - e}{1-e \ cos \ E_k}$	True anomaly
(7)	$\phi_k = v_k + \omega$	Argument of latitude
(8)	$\delta\phi_k = C_{us} \ sin(2\phi_k) + C_{uc} \ cos(2\phi_k)$	Argument of latitude correction
(9)	$\delta r_k = C_{rs} \ sin(2\phi_k) + C_{rc} \ cos(2\phi_k)$	Radius correction
(10)	$\delta i_k = C_{is} \ sin(2\phi_k) + C_{ic} \ cos(2\phi_k)$	Inclination correction
(11)	$u_k = \phi_k + \delta\phi_k$	Corrected argument of latitude
(12)	$r_k = a(1 - e \ cos \ E_k) + \delta r_k$	Corrected radius
(13)	$i_k = i_0 + (di/dt)t_k + \delta i_k$	Corrected inclination
(14)	$\Omega_k = \Omega_0 + (\Omega - \Omega_e)(t_k) - \Omega_e t_{0e}$	Corrected longitude of node
(15)	$x_p = r_k \ cos \ u_k$	In-plane *x* position
(16)	$y_p = r_k \ sin \ u_k$	In-plane *y* position
(17)	$x_s = x_p \ cos \ \Omega_k - y_p \ cos \ i_k \ sin \ \Omega_k$	ECEF *x*-coordinate
(18)	$y_s = x_p \ sin \ \Omega_k - y_p \ cos \ i_k \ cos \ \Omega_k$	ECEF *y*-coordinate
(19)	$z_s = y_p \ sin \ i_k$	ECEF *z*-coordinate

Figure 2: Algorithm for Computing Satellite ECEF Position Vector

$$p_1 = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} + ct_u$$

$$p_2 = \sqrt{(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2} + ct_u$$

$$p_3 = \sqrt{(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2} + ct_u$$

$$p_4 = \sqrt{(x_4 - x_u)^2 + (y_4 - y_u)^2 + (z_4 - z_u)^2} + ct_u$$

Figure 3: Pseudorange Calculation for Each GPS Satellite

2.2 GPS Simulator Selection

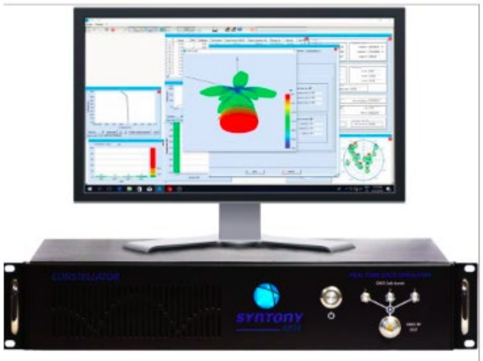
Researching the proper GPS simulator for our spoofing needs required knowledge of GPS fundamentals as discussed in the previous section. With this knowledge, we searched for GPS simulators online using the google search engine that would allow us to directly access the ephemeris data. Reading through many GPS simulator data sheets and requesting quotes from their respective companies, we eventually found five total GPS simulators that seemed to match our requirements.

The first GPS simulator we found was the CLAW from Jackson Lab Technology (JPL) [3]. This device was a miniature GPS simulator module that had a cost of approximately $3800. After reading through the user manual provided by the company it seemed like this miniature GPS simulator module could perform just the bare minimum of what was required for our task. That is, the ephemeris data could be changed directly, but the simulator could not simulate as many satellites as needed and the software accompanied with it was very limiting. Though, this was by far the cheapest option. This GPS Simulator is shown in the Figure 4 below:

CLAW (Photo: Jackson Labs Technologies)

Figure 4: CLAW GPS Simulator

The second GPS simulator we researched was the Constellator from Syntony [4]. This device seemed much more advanced than the CLAW GPS simulator as it could perform real time simulations with multi-antenna and multi-receiver capabilities. After reading the data sheet provided by the company, this device never explicitly said that the ephemeras data could be directly accessed and changed. But after watching some videos on the software paired with the GPS simulator, it seemed as though it would be able to perform such a task. However, after contacting the company trying to ask some questions, they never responded, so the price and exact details of this GPS simulator remain unknown. This GPS simulator is shown in Figure 5 below:



Constellator. (Photo: Syntony)

Figure 5: Constellator Syntony GPS Simulator

The third GPS simulator we researched was the Rohde & Schwarz SMBV100A [5]. This GPS simulator was discontinued by its company but could be purchased by external vendors such as Electro Vent or Ebay. Both of which sold this device for around $10,000. After contacting the appropriate vendors and asking some questions as well as reading through the data sheet. This device had the ability to allow direct changes to ephemeris data but included far too many features than we needed for our task, especially for the price that it was offered. The GPS simulator is shown in Figure 6 below:

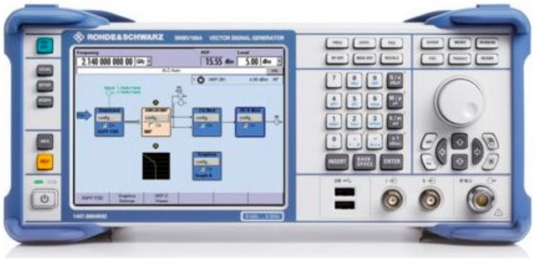


Figure 6: Rohde & Schwarz SMBV100A (discontinued)

The Fourth GPS simulator we researched was the GSG-5 series Orolia GNSS simulator [6]. Which evidently led us to our fifth GPS simulator we researched which was the BroadSim Orolia GNSS simulator [7]. Both GPS simulators are shown in Figure 7 and Figure 8 below:

Figure 7: GSG-5 Series Orolia GNSS/GPS Simulator

Figure 8: BroadSim Orolia GNSS/GPS Simulator

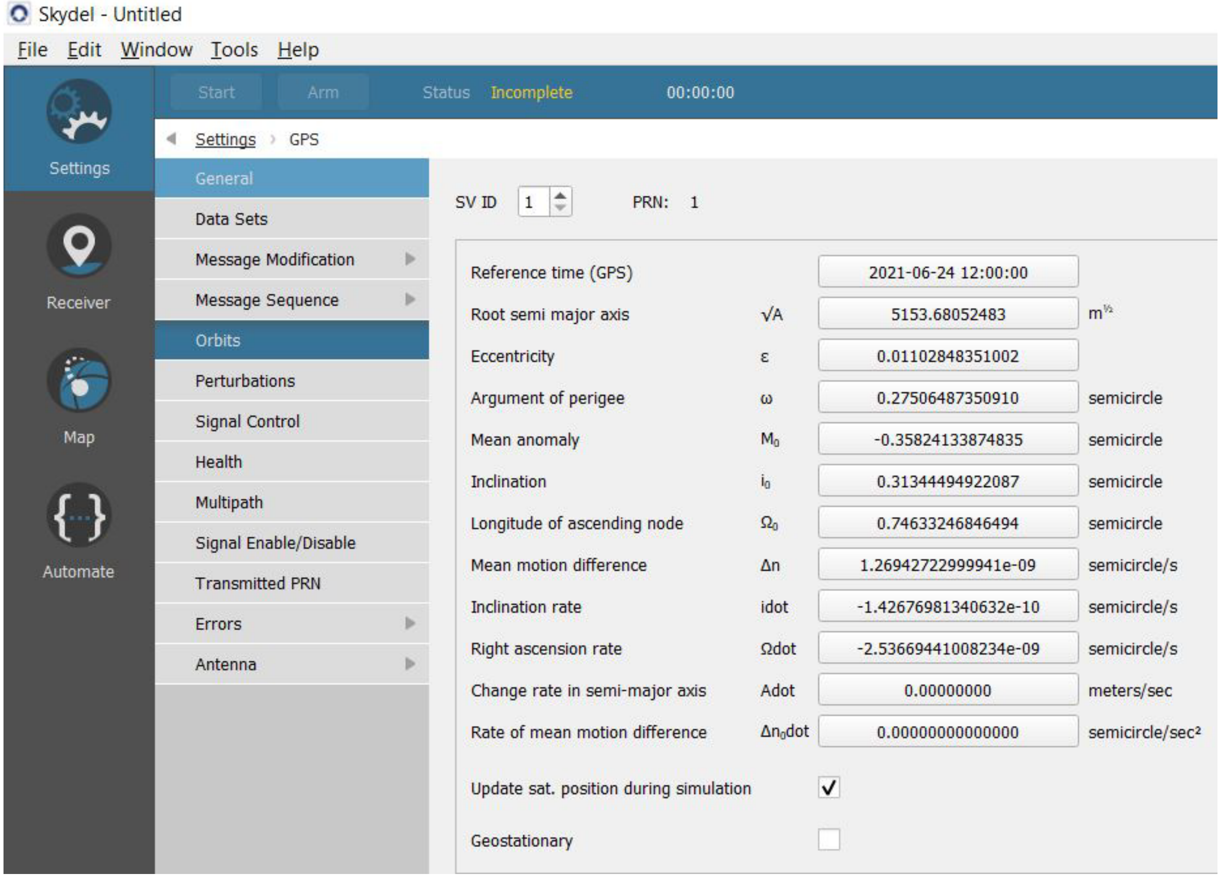
Both of these GPS simulators seemed very capable of our research task for simulating GPS spoofing on the computed time offset by changing the ephemeris data. However, once again, these GPS simulators had far too many “extra” features that weren’t needed for our task and the price seemed even more expensive than the third GPS simulator we researched, the Rohde & Schwarz SMBV100A.

After reviewing these GPS simulators, we then began contacting the companies who designed the GPS simulators that we found. Not all of the companies contacted got back to us, and the ones that did pointed towards Orolia products. We then scheduled some calls with application engineers at Orolia. Through these conversations with applications engineers, we were given the Orolia Skydel Software.

2.3 Orolia Skydel Software Procurement

The Skydel software from Orolia is a robust and effective tool for GPS/GNSS simulations [8]. We chose this software for many reasons presented to us through great tech support. Those reasons are as follows: Users are able to run the software on their own computers, along with the options to integrate their own SDR and receiver with the application. Through Orolia’s Academic Partnership program, WWU received software licenses for the simulator at no cost. Within this software, we are able to design simulations and both view and modify the ephemeris, as shown in Figure 9.

We plan to begin training with this software as well as running simulations to test ephemeris modification and spoofing. For a receiver, we will likely use an SDR connected to a PC that can receive the GPS data, allowing us to observe the spoofing results and verify if our spoofing technique is working as expected.



SV ID 1 PRN: 1

Reference time (GPS)		2021-06-24 12:00:00	
Root semi major axis	√A	5153.68052483	$m^{1/2}$
Eccentricity	ε	0.01102848351002	
Argument of perigee	ω	0.27506487350910	semicircle
Mean anomaly	M_0	-0.35824133874835	semicircle
Inclination	i_0	0.31344494922087	semicircle
Longitude of ascending node	Ω_0	0.74633246846494	semicircle
Mean motion difference	Δn	1.26942722999941e-09	semicircle/s
Inclination rate	idot	-1.42676981340632e-10	semicircle/s
Right ascension rate	Ωdot	-2.53669441008234e-09	semicircle/s
Change rate in semi-major axis	Adot	0.00000000	meters/sec
Rate of mean motion difference	Δn_0dot	0.00000000000000	$semicircle/sec^2$

Update sat. position during simulation ☑

Geostationary □

Figure 9: Ephemeris Data Entry for Skydel GPS Simulations

3. Conclusion and Future Works

After researching GPS simulators throughout the Spring quarter of 2022 with Professor Xichen. We have decided to follow through with using the Skydel software offered by Orolia to simulate our GPS spoofing mitigation for phasor measurement receivers.

As of this written report, we plan to continue our research into this area of GPS spoofing starting Fall quarter 2022 using the Orolia Skydel Software. We also plan to learn more about the details and functionality of the Skydel software by attending a live tutorial offered by the Orolia team sometime in the near future. Other faculty members from Western Washington University may be joining this live tutorial as it is possible that this Skydel Software may be implemented into future curriculum for the Engineering department at Western Washington University.

References

[1] Christopher J. Hegarty and Elliot D. Kaplan, “Understanding GPS - Principles and Applications,” 2006.

[2] Xichen Jiang, “Spoofing GPS Receiver Clock Offset of Phasor Measurement Units,” M.S. thesis, University of Illinois at Urbana-Champaign, Champaign, IL, 2012.

[3] Jackson-labs.com, *CLAW GPS Simulator*, 2022. [Online]. Available: https://www.jackson-labs.com/index.php/products/claw_gps_simulator [Accessed: 16-September 2022]

[4] Syntony-gnss.com, *Constellator GPS Simulator*, 2022. [Online]. Available: https://solutions.syntony-gnss.com/gps-testing/simulator [Accessed: 16-September 2022]

[5] Rohde-schwarz.com, *R&S SMBV100A Vector Signal Generator*, 2022. [Online]. Available: https://www.rohde-schwarz.com/us/products/test-and-measurement/vector-signal-generators/rs-smbv100a-vector-signal-generator_63493-10220.html [Accessed: 16-September 2022]

[6] Orolia.com, *GSG-5 Series GPS/GNSS Simulator*, 2022. [Online]. Available: https://store.orolia.com/products/gsg-5-series-gps-gnss-simulator [Accessed: 16-September 2022]

[7] Oroliads.com, *Broadsim GPS Simulator*, 2022. [Online]. Available: https://www.oroliads.com/broadsim [Accessed: 16-September 2022]

[8] Orolia.com, *Skydel GNSS Simulation Software*, 2022. [Online]. Available: https://www.orolia.com/product/skydel-simulation-engine/ [Accessed: 16-September 2022]