Jaakko Oksanen

Solutions for spoofing and jamming attacks

Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communications Technology

Bachelor's Thesis

02 November 2021

Abstract

Author:	Jaakko Oksanen
Title:	Solutions for spoofing and jamming attacks
Number of Pages:	31 pages
Date:	02 November 2021
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communications Technology
Professional Major:	Smart Systems
Supervisors:	Markus Hurme, Senior Manager of Software Simo Sainio, Senior Lecturer

In the GNSS (Global Network Satellite System) world, jamming and spoofing attacks are an increasing threat. In the thesis we go through several ways of defending against such attacks. One defence method against these attacks is also implemented in this study. Spoofing attacks are used to distort location and timing information, which are essential in many industries.

The idea of the thesis was to create an AGC (Automatic Gain Controller) and SNR (Signal to Noise Ratio) monitoring software feature and also to test the effectiveness of this software in detecting spoofing. The software was made for 5401 and 5405 devices from Oscilloquartz. The AGC is a control system, which is used to stabilize incoming signals and the SNR value tells the power of the useful signal compared to the noise.

The goal of this work was to create a software feature for spoofing detection that follows and compares the AGC and SNR values. Many in-house measurements were done to see how the values fluctuate under normal circumstances and under a simulated spoofing situation. The measurements were carried out to understand the AGC and SNR values' reactions and differences between normal conditions and while being spoofed. The spoofing situation was created by using a GNSS simulator. The software feature monitors and calculates averages of the values and sets an alarm when set threshold values are exceeded. The feature was written in C programming language.

In the end a working feature was created, which detected spoofing quite well and worked much better than the spoofing and jamming indicators from the receiver. This feature is a good way to detect spoofing, but it does have its flaws and should not be used as a lone defense against spoofing. In the future this feature could be expanded to monitor other values from the receiver as well to improve functionality and it can be tested with better equipment to calibrate the threshold values more accurately.

Keywords: GNSS, Spoofing, Jamming, GPS

Tiivistelmä

Tekijä:	Jaakko Oksanen
Otsikko:	Solutions for spoofing and jamming attacks
Sivumäärä:	31 sivua
Aika:	02.11.2021
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Älykkäät järjestelmät
Ohjaajat:	Vanhempi Ohjelmisto Johtaja Markus Hurme Lehtori Sami Sainio

Häirintä ja huijaushyökkäykset ovat kasvava uhka laitteissa, jotka käyttävät maailmanlaajuista satelliittiverkkoa. Tässä työssä tutustutaan tarkemmin siihen, millaisia hyökkäykset useimmiten ovat ja miten niiltä kannattaa puolustautua. Työssä implementoidaan myös yksi puolustuskeino. Huijaushyökkäyksien idea on vääristää sijainti- tai aikatietoja, jotka ovat elintärkeitä monilla eri aloilla.

Tämän insinöörityön idea oli tehdä AGC- ja SNR-arvoihin perustuva monitorointiominaisuus sekä testata sen toimivuus. Ohjelmisto tehtiin Oscilloquartzin 5401- ja 5405-laitteisiin. AGC on ohjausjärjestelmä, jota käytetään vastaanotettujen signaalien stabilointiin, ja SNR kertoo hyödyllisen signaalin tehon verrattuna turhaan kohinaan.

Tämän työn tavoite oli luoda ohjelmisto-ominaisuus huijaushyökkäyksien tunnistusta varten, joka seuraa ja vertaa AGC- ja SNR-arvoja. Tavoitteena oli myös testata, kuinka hyvin ominaisuus onnistuu tunnistamaan huijaushyökkäyksiä. Monta mittausta tehtiin, jotta saatiin hyvä käsitys, miten arvot vaihtelevat normaaleissa tilanteissa ja simuloiduissa huijaushyökkäyksissä. Huijaushyökkäyksiä simuloitiin GNSS-simulaattorin avulla. Ohjelmisto monitoroi ja laskee keskiarvoja AGC- ja SNR-arvoille sekä asettaa hälytyksen, jos asetetut raja-arvot ylittyvät. Ominaisuus tehtiin C-ohjelmointikielellä.

Työn lopputuloksena on toimiva ominaisuus, joka tunnisti huijaushyökkäyksiä melko hyvin. Monitorointiohjelma toimi huomattavasti paremmin kuin vastaanottimen omat huijaus- ja häirintäindikaattorit. Tämä ohjelma toimii melko hyvin huijausyritysten tunnistuksessa, mutta siinäkin on puutteensa eikä sitä kannata käyttää ainoana puolustuksena huijaushyökkäyksiä vastaan. Parhaan suojan saa, kun yhdistelee monia eri puolustuskeinoja. Työtä pystyy myös jatkamaan tulevaisuudessa lisäämällä muitakin arvoja monitoroitavaksi, mikä voi parantaa luotettavuutta. Testaaminen paremmilla laitteilla saattaa myös auttaa asettamaan raja-arvoja tarkemmin.

Avainsanat: GNSS, Satelliittiverkko, Häirintä, Huijaus, GPS

Table of Contents

List of Abbreviations

1PPS	Pulse Per Second
540X	5401 and 5405 devices by Oscilloquartz
AGC	Automatic Gain Controller
CDMA	Code-Division Multiple Access
CLI	Command Line Interface
dBm	Decibel-milliwatts
GLONASS	Global Navigation Satellite System
GNSS	Global Network Satellite System
GPS	Global Positioning System
IRNSS	Indian Regional Navigation Satellite System
NTP	Network Time Protocol
ns	Nano Seconds
PTP	Precision Time Protocol
QZSS	Quasi-Zenith Satellite System
SBAS	Satellite-based Augmentation System
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol

SNR	Signal to Noise Ratio
SyncE	Synchronous Ethernet
UTC	Coordinated Universal Time

1 Introduction

Spoofing and jamming are an increasing threat to all devices that use GNSS. The need for reliable GNSS service has increased drastically in the last decade and it will continue to rise in the future, but solutions for spoofing and jamming attacks have been quite stagnant [1].

GNSS systems are used in variety of vehicles to know their real time locations. Many cases have been reported where ships at sea have crashed into rocks because of the ships GNSS receiver thinking it is somewhere it's not [2]. This is also a problem in the United States and Mexico's border where drug traffickers are spoofing and jamming police drones, which interferes with law enforcement's oversight over drug routes [3].

The thesis reports about different types of spoofing and jamming attacks and how to defend against them. The thesis also goes into detail on how one software based spoofing detection feature works and is implemented.

The idea of the thesis was to create a AGC and SNR monitoring feature using C programming language and see how well it could be used to detect spoofing. The software feature was created for the 5401 and 5405 devices from Oscilloquartz.

Oscilloquartz has manufactured time synchronization solutions for over 50 years. The company manufactures devices such as PTP (Precision Time Protocol) grandmasters and cesium clocks. Oscilloquartz wanted this project, because safety is one of the core values of the company and they wanted to see if AGC and SNR monitoring could improve protection against spoofing on their devices.

This introduction is the first chapter of the thesis. The second chapter goes through the basics of GNSS, jamming and spoofing. The third chapter has information about Oscilloquartz and the 540X products that are used in the

thesis for the monitoring feature and also a few other major products. Chapter four focuses on the importance of AGC and SNR values and how they can be used in spoofing detection. The fifth chapter goes through testing done before implementing the feature to see how the values change under normal conditions. The chapter then discusses implementation of the feature. The last part of chapter five goes through testing results on how effective the feature is at spoofing detection. Chapter six summarizes the entire project and goes through the goals, results and how this software feature could be expanded in the future.

2 Global Network Satellite System

GNSS is a constellation of satellites in space that transmit positioning and timing information to GNSS receivers. Location from satellites is calculated using trilateration, which will be explained in more detail later. Around seven percent of the global gross domestic product relies on GNSS, which means protecting it is extremely important [4]. GNSS is used in a variety of industries such as energy, finance, defence, mobile networks, aviation and automotive. The usage of GNSS is expected to increase rapidly over the next decade, with things such as smart watches, automated driving, drones and Internet of Things becoming more popular. In a report made by the European GNSS agency in 2019 they predicted that the number of installed GNSS devices would increase from around six billion in 2019 to over ten billion in 2029 (figure 1).

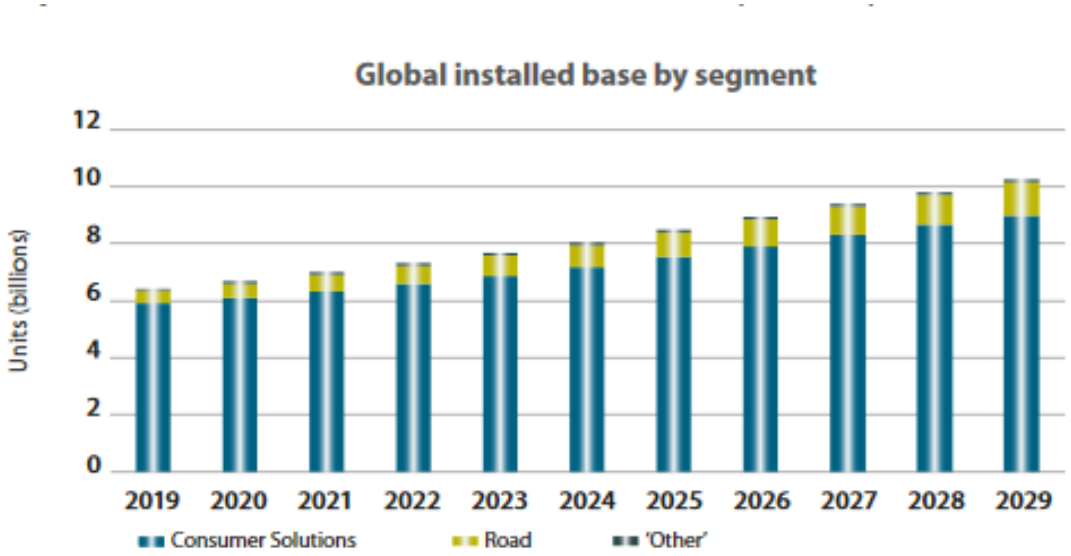

Figure 1. Number of installed GNSS devices by segment [5].

Each satellite is equipped with atomic clocks, which are extremely stable [6]. These clocks are calibrated frequently to a ground clock in a control station to ensure that the time they distribute is accurate. These control stations have an important task of tracking, controlling and sending information to satellites. The receiver's job is to decode messages from satellites and distribute needed

information forward, this is usually either time or position. Getting positioning from satellites is obtained by using trilateration (figure 2), which involves measuring distances between satellites and the receiver.

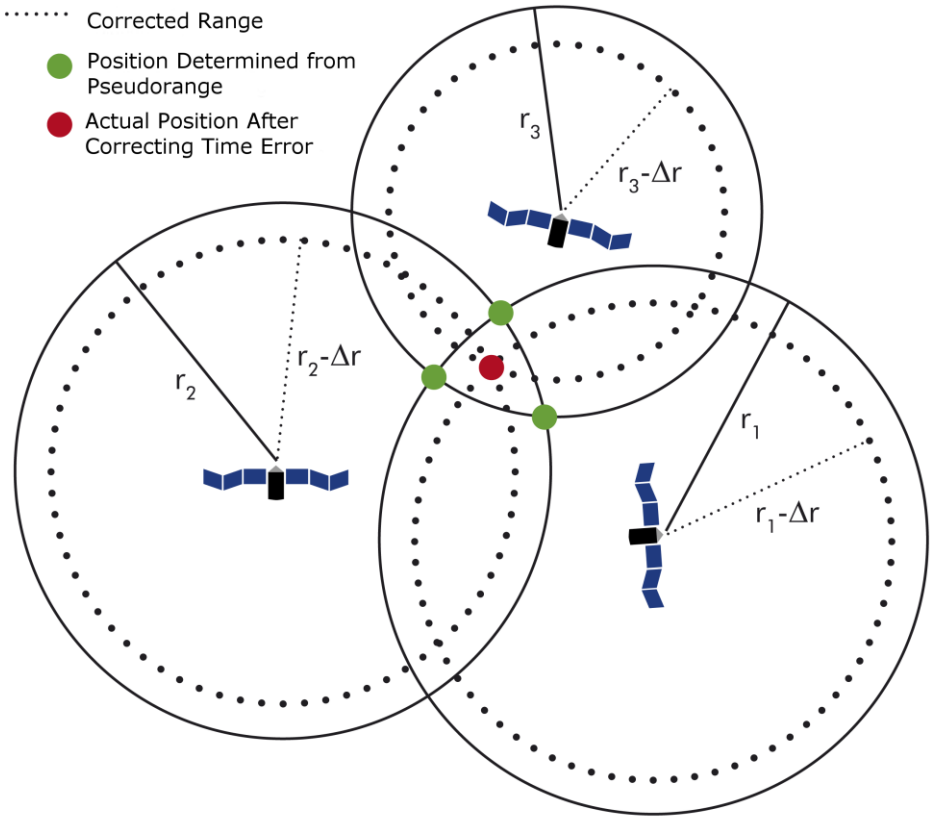

Figure 2. How trilateration works [7].

In the past most receivers outside of government and professional use have been single-frequency and single-constellation, because of expensive prices. Nowadays multi-frequency and multi-constellation receivers are more common, which increases accuracy, reliability and redundancy (figure 3). A common misconception with GNSS receivers is that they send information back to satellites, which is not true. Most receivers in most cases that are in use are passive, which means they only receive data. The only exception to this is Galileo's Support to Search and Rescue Service, where in emergencies some receivers can send location data to Galileo satellites and the satellites can then forward this information to local rescue centres [8].

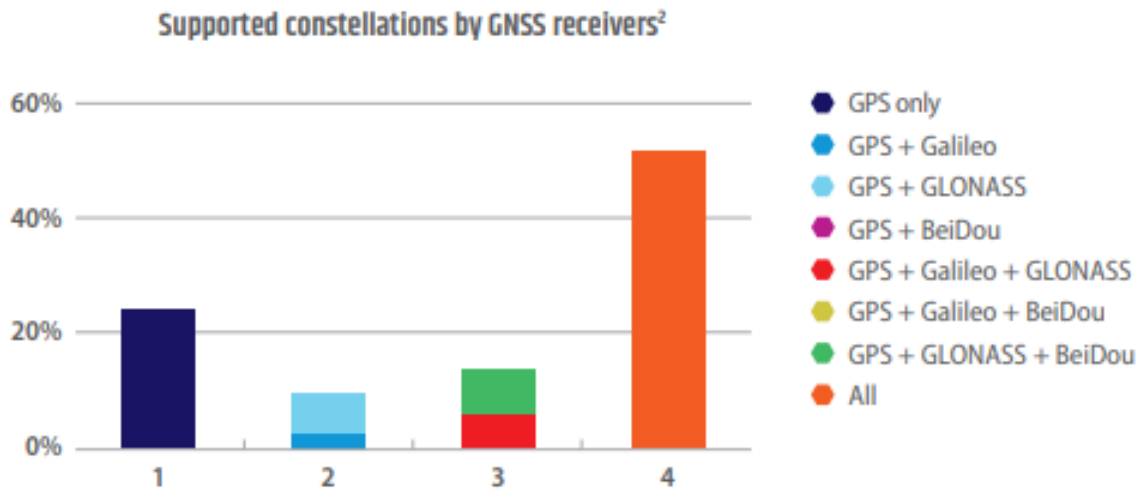

Figure 3. How many percent of receivers support different types of constellations at the end of first quarter of 2020. Study of around 500 different receivers [9].

Currently there are four globally operational GNSS systems. The United States' GPS (Global Positioning System) is the oldest working system and it has been available since 1994 globally. GPS was first made to be only for military use, but after realizing it's potential in other sectors, the United States made GPS available for civilian use as well. GPS is the most used system in the world. It currently has 31 usable satellites in orbit and 27 of those are in use and four are in reserves. Since the 1970's the United States has spent over 35 billion dollars on GPS and it is said to have a yearly operational cost of around 750 million dollars [10].

Europe's Galileo is the newest system. It became operational in 2016 and it consists of 30 satellites in total of which six are in reserves and 24 are in use. Unlike all the other major GNSS systems Galileo is entirely maintained by civilians and it has an accuracy of up to around one meter, which is currently the best accuracy that the general public can get from any system. Each Galileo satellite contains two passive hydrogen maser and two rubidium atomic clocks that work independently of each other. The passive hydrogen masers are used as master clocks, because their accuracy is about four times better than rubidium clocks. Hydrogen masers can keep time within 0.45 ns (nano seconds)

for about 12 hours and rubidium clocks to about 1.8 ns for 12 hours [11]. Galileo is free of charge for everyone and its development costs are estimated to be around ten billion euros [12].

China’s BeiDou, achieved global coverage in 2020. BeiDou has three stages. BeiDou-1 which consisted of only three satellites and it was decommissioned in 2012 right after BeiDou-2 became operational. BeiDou-2 replaced Beidou-1 and provided coverage for the Asia-Pacific region (figure 4), it consisted of 30 satellites. BeiDou-3 was completed on 23 of June 2020 and provides global coverage. China’s whole BDS system contains a total of 48 satellites in the constellation of which 42 are operational [13].

Figure 4. BeiDou-2 coverage in 2012 [14].

Russia’s GLONASS (Global Navigation Satellite System), achieved global coverage in 1995. The satellite system’s capacity was severely reduced in the late 1990’s due to a lack of maintenance and GLONASS did not achieve full global coverage again until late 2011. GLONASS has a total of 27 satellites in the constellation of which 23 are operational. Unlike in other constellations older

GLONASS satellites use FDMA (frequency division multiple access) for signal modulation. This differs from the more common CDMA (code-division multiple access) method by assigning each satellite with its own specific carrier frequency. The main reasons for the change to CDMA is that the receiver and antenna design is not as complex and expensive. It is also simpler to create multi-constellation GNSS receivers if every constellation uses CDMA. GLONASS has an accuracy of up to just under three meters (figure 5).

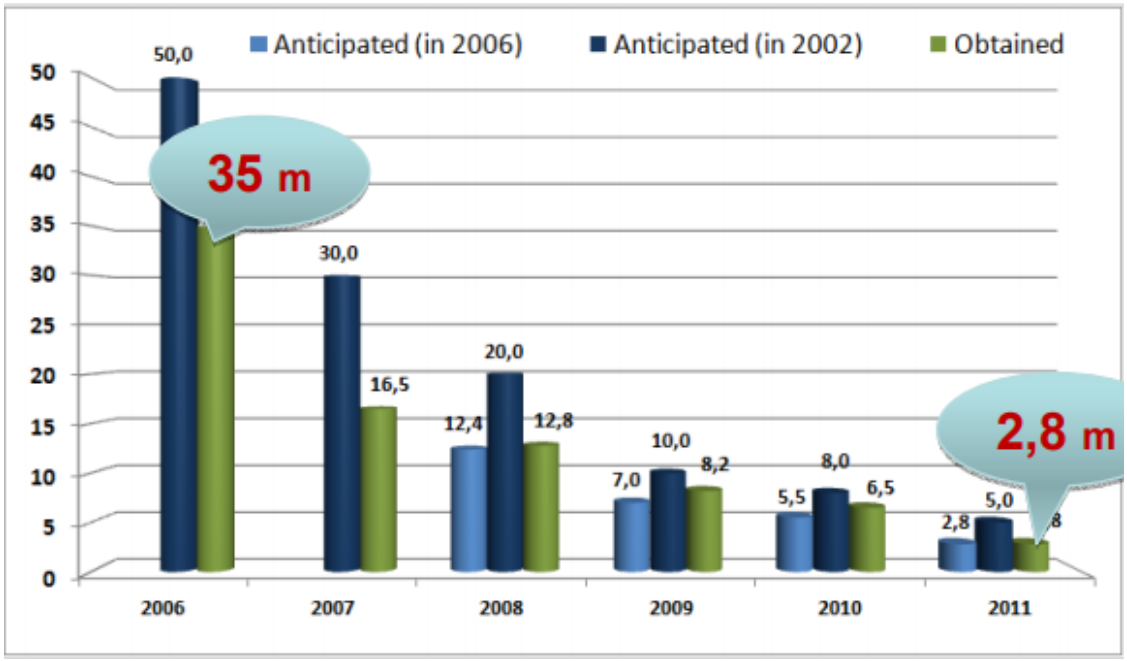

Figure 5. Accuracy of GLONASS from 2006 to 2011 [15].

In addition to the major global satellite systems, there are two systems that give regional coverage. Japan's QZSS (Quasi-Zenith Satellite System) is a four-satellite constellation and the current plan is to turn it into a seven-satellite constellation by 2023. QZSS provides coverage to the Asia-Oceania region and it also works as a SBAS (Satellite-based Augmentation System) service [9]. The other regional system is India's IRNSS (Indian Regional Navigation Satellite System) and it consists of seven operational satellites with plans to increase the number to eleven. IRNSS covers India and the region 1 500 kilometres around it.

Several countries and regions have implemented a SBAS (figure 6). The idea of SBAS is to improve accuracy, availability and reliability of GNSS. In many sectors the use of SBAS is necessary, because GNSS systems alone do not fulfil the stringent operational requirements. For example, airplanes can not rely on GPS alone in critical stages of flights like the landing and takeoff. An SBAS is needed to fulfil the operational requirements established by the International Civil Aviation Organization.

These systems work by calculating positional error in the GNSS by comparing data from satellites to fixed locations on ground. Any difference between the real location and the data from the satellites can be determined to be an error. This error data is then sent to a central computer, where a correction is calculated and the correction is then sent to satellites. After satellites receive the correction they broadcast it over the area [16]. With SBAS and high-end receivers sometimes accuracy can be in the tens of centimeters range, but usually the accuracy is in the range of a few meters.

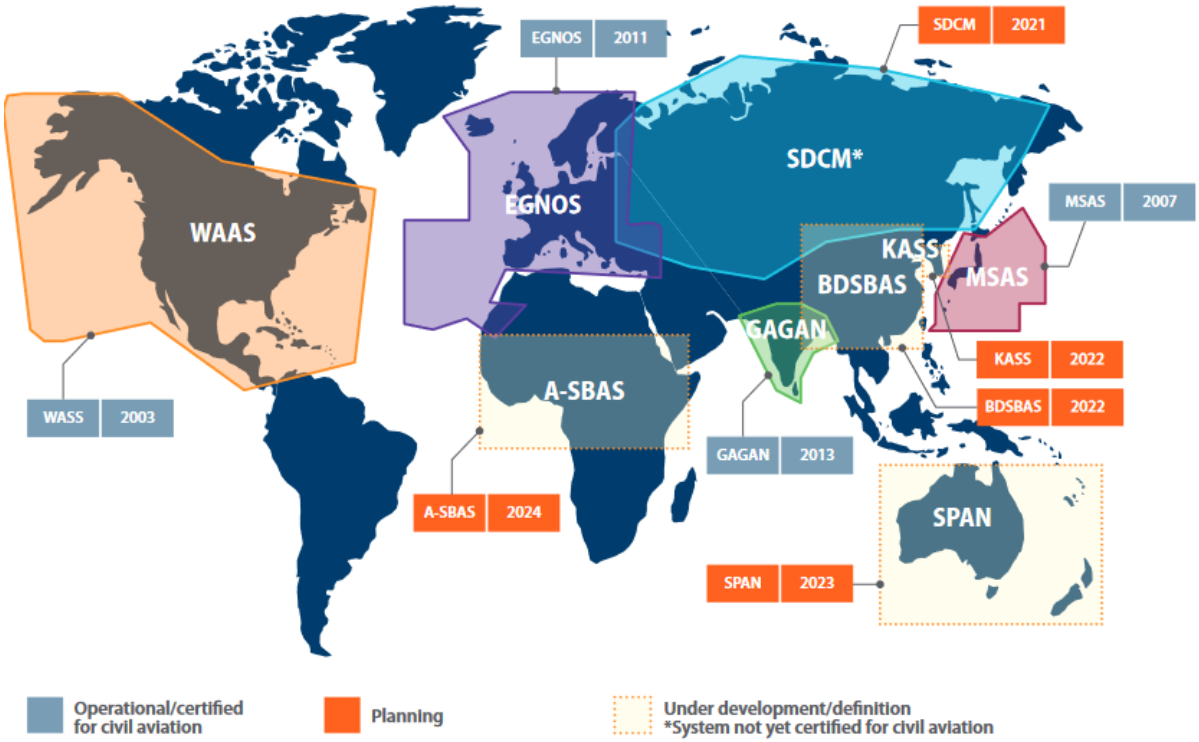

Figure 6. Current operating and planned SBAS [9].

2.1 Jamming

Jamming is intentional blocking or interference to the GNSS signal with a frequency transmitting device. A complete loss of GNSS signal is quite easy to detect but if the jamming is more subtle, detecting it can be a lot more difficult. When the GNSS signals reach earth they are fairly weak, so jamming them does not require much power. A typical signal received from a GPS satellite is around −127.5 dBm (decibel-milliwatts), which is equal to $178*10^{-18}$ watts. Jamming is often used in spoofing attacks to improve chances of success.

Most common case of jamming is preventing vehicles from being tracked with GNSS. Many criminal organizations also use this technique to steal cars and high value items with trackers. Mexico reported that in around 85 percent of car thefts jammers were being used [17]. Some jammers can affect GNSS devices from over two kilometres away, so identifying where the jamming is coming from can be difficult. This means people using jammers who have no ill intent, can unintentionally cause major harm. This exact situation happened in New Jersey, where a truck driver hid from his employer by using a jammer and parked his car near an airport. The Newark airport systems navigation was disrupted and the man got a fine of almost 32 000 dollars [18]. A jammer that plugs into a car’s cigarette lighter can be bought for as low as 20 euros (figure 7).

Figure 7. A small car cigarette lighter powered jammer [19].

Easiest way to defend against jamming is to purchase a good oscillator for the time server. Usually these jamming events do not last a very long time, so having a good oscillator that keeps time relatively stable is a good solution. Another good solution is buying an anti-jamming antenna that blocks ground signals or adding redundant antennas in other places. It is also important to remember that not all interference is intentional, sometimes faulty equipment or a nearby antenna transmitting can cause accidental interference that can easily be mistaken for jamming.

2.2 Spoofing

Usually spoofing attacks fall under one of three categories. The first and easiest kind to implement is a replay spoofing attack. In this kind of spoofing attack the point is to delay the signal to the receiver, thereby spoofing it. The GNSS signal is first intercepted and then broadcasted on the same received frequency with much higher power. This kind of attack is relatively simple to implement, but it is not very effective on its own. This type of spoofing attack is also called

meaconing. Replay spoofing attacks are often combined with jamming to increase chances of success.

The second category is a forgery spoofing attack, which is much more complicated to implement than a replay spoofing attack. In this kind of an attack the spoofer can either forge a satellite signal directly or analyse a real satellite signal and then add received satellite parameters to the forged signal to improve chances of success. The forged signal is broadcasted at a much higher amplitude than the real signal to cover up the real signal and to make sure that the receiver locks into the forged signal.

The final category and the hardest to implement is an estimation spoofing attack. In this kind of an attack the spoofer estimates unknown satellite information and then uses the estimates to generate a signal. These kinds of attacks are used when the satellite messages include unknown security codes. The effectiveness of the estimation spoofing attack is completely dependent on the successfulness of the code estimation. If the spoofer is unable to estimate the unknown information the attack will most likely fail, however if the estimation is successful the spoofing has a good chance of working.

Spoofing attacks are much less common than jamming attacks, but spoofing attacks are much harder to detect. It is difficult to know exactly how much spoofing is going on, because spoofing done with sophisticated equipment can be extremely difficult to detect. Even if a spoofing attack is detected by the victim they might not want to report it for security or bad publicity reasons. Spoofing is also getting more and more popular and anybody with around 300 euros (figure 8) can do it with some help from numerous videos and guides online about the subject. Spoofing used to be very expensive, but with the introduction of cheap software-defined radios has lowered the cost of spoofing from many thousands to a few hundreds of euros.

One good example of the dangers of spoofing happened in 2011. A highly classified United States military drone was captured by the Iranian military’s cyberwarfare unit by spoofing the drone to think it was landing at a friendly base

in Afghanistan, when in reality it was landing in Iran [20]. Iran has since claimed to have reverse engineered the drone and created their own version of it. Another good example of spoofing is when Regulus Cyber successfully spoofed a Tesla Model 3 to change lanes into incoming traffic, exit highways at incorrect locations and do unnecessary braking and accelerating [21]. Tesla's autopilot features rely very heavily on GNSS and by spoofing it, it is possible to make the car's autopilot do almost anything. Even though this spoofing test was done only on a Tesla Model 3 this problem is most likely company wide, since all of their vehicles use the same chipset.

Figure 8. Software controlled radio module that can be used for spoofing. Costs about 300 euros [22].

Defending against spoofing attacks is much more difficult, because the point is to make the receiver think it's getting valid data. Good ways to defend against spoofing are purchasing an anti-jamming antenna which blocks ground-based signals and using a multi-constellation and multi-frequency receiver. Another good solution is having two different receivers, one set to a stationary mode in a fixed position and another one set in navigation mode and comparing the

position of the two. Having an alternative source of time is also a good idea so the distributed time stays relatively stable, even though that alone does not help if the device does not notice the spoofing.

All of the formerly mentioned defences against spoofing are good, but they might require purchasing additional hardware. Spoofing detection can also be on the software level. For example, consistency checking, analysing signal parameter statistics, analysing signal arrival times or finding deviation in the doppler shift. It is also possible to calculate an estimation for the trajectory of a satellite and check if the position changes over an allowed range or comparing the location distance between two receivers. Usually software based spoofing protection compares multiple different values from the signal to see if there are any inconsistencies. Table 1 shows some of the upsides and downsides of each spoofing detection method.

Table 1. Upsides and downsides of spoofing detection methods.

Detection Method	Upsides	Downsides
Consistency checking	Easy to implement	Can be forged with a spoofer
Analysing signal parameter statistics	Effectiveness and implementation difficulty depends on the amount of parameters analysed	Effectiveness and implementation difficulty depends on the amount of parameters analysed
Analysing signal arrival times	Good effectiveness and easy to implement	Requires stationary receiver
Satellite trajectory calculation	Good effectiveness	Difficult to implement and requires a lot of processing power
Doppler shift deviation checking	Easy to implement	Can be forged with a spoofer
Location between two receivers	Good effectiveness	Requires multiple receivers in fixed locations

European satellite system Galileo is also experimenting in adding anti-spoofing services in the form of authentication available to the public, which would be a great way to combat spoofing. Previously GNSS authentication has only been available for governments and a few select others. This would be a great protection against replay and forgery spoofing, which are the most common types of attacks. This would force the spoofer to invest in more expensive equipment and make it much more difficult to successfully conduct spoofing.

3 Oscilloquartz

Oscilloquartz is an industry leader in time synchronization devices. From small portable PTP Grandmaster clocks that plug into SFP (Small Form-factor Pluggable) ports to large atomic cesium clocks, they create a vast selection of devices for all network timing needs. Oscilloquartz was first a department in Ebauches in 1949 and in 1971 Oscilloquartz was registered as a corporation officially. Oscilloquartz was then acquired by ADVA in 2014. Oscilloquartz makes a variety of products such as cesium clocks, PTP grandmaster clocks, PTP slave clocks and NTP (Network Time Protocol) servers. These products are used in over 90 countries.

3.1 540X

The 540X encompasses five models. Four different variants of 5405 and 5401. All of these products come with full management support with SNMP (Simple Network Management Protocol) versions two and three and remote CLI (Command Line Interface) access with Telnet and Secure Shell. Devices also have support for syncE (Synchronous Ethernet) and the Syncjack monitoring tool, which can be used to monitor time error between a source and a reference signal. Syncjack’s programmable source and reference signals include GNSS, PTP, syncE and 1PPS (Pulse Per Second) . All 540X models run on the 32-bit Nios 2 soft-core processor. 540X devices have spoofing and jamming protection on the device level and artificial intelligence-based spoofing and jamming protection on the Ensemble Controller Software.

The 5401 is a very small, versatile and compact SFP pluggable grandmaster, boundary and slave clock with a GNSS receiver that has GPS, Galileo, GLONASS, BeiDou and SBAS support (figure 9). It supports sending PTP over layer 2 and over IPv4/IPv6 simultaneously. It has a timing accuracy of +/-100 ns from UTC (Coordinated Universal Time). It can have up to 64 unicast slaves at 128 PPS (Packets Per Second). The 5401 has a power consumption of under 1,5 watts.

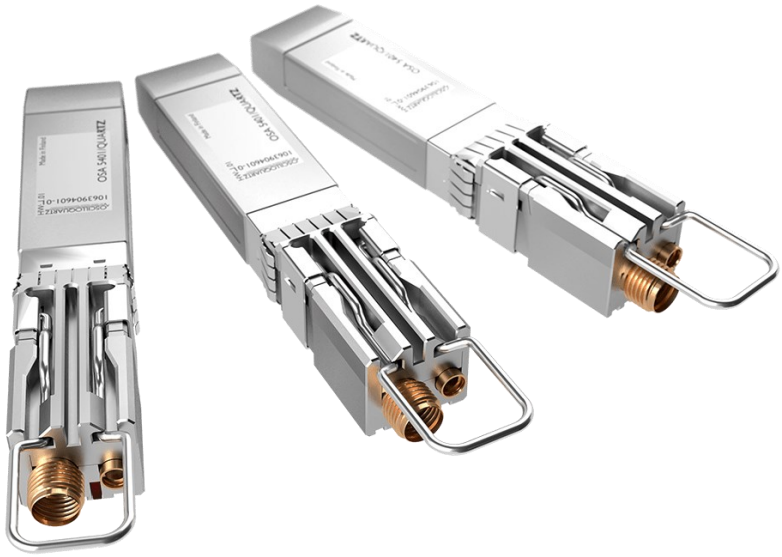

Figure 9. Three 5401 products [23].

The 5405 comes in four different versions. Two of them work outdoors, which are the 5405-O and 5405-MB. The 5405-O is a compact environmentally hardy grandmaster and NTP-server made for outdoor deployment (figure 10). The 5405-O has unique spoofing detection method, where it can compare the location and 1PPS data from the two different receivers it has. The 5405-MB is very similar except it has a multiband GNSS receiver for higher precision. 5405-MB will also have a similar spoofing detection feature in the future, even though it only has one receiver. The 5405-MB's receiver can calculate its current position while in fixed mode, which can then be compared to the fixed location. The outdoor variants are IP66-compliant, which means they can handle even the harshest weather and they have an operating temperature between -40 and +70 degrees Celsius. They also come with a pole, cabinet and wall mount. 5405 models have maximum power consumption of 3,0 watts without SFP.

One of the indoor models is the 5405-I, which has a dual integrated GNSS receiver and support for external GNSS antenna option. The 5405-P is the second indoor model, which is meant to be an energy substation grandmaster features alarm relay, 1PPS, time of day and IRIG (Inter-Range Instrumentation Group) interfaces and uses an external GNSS antenna.

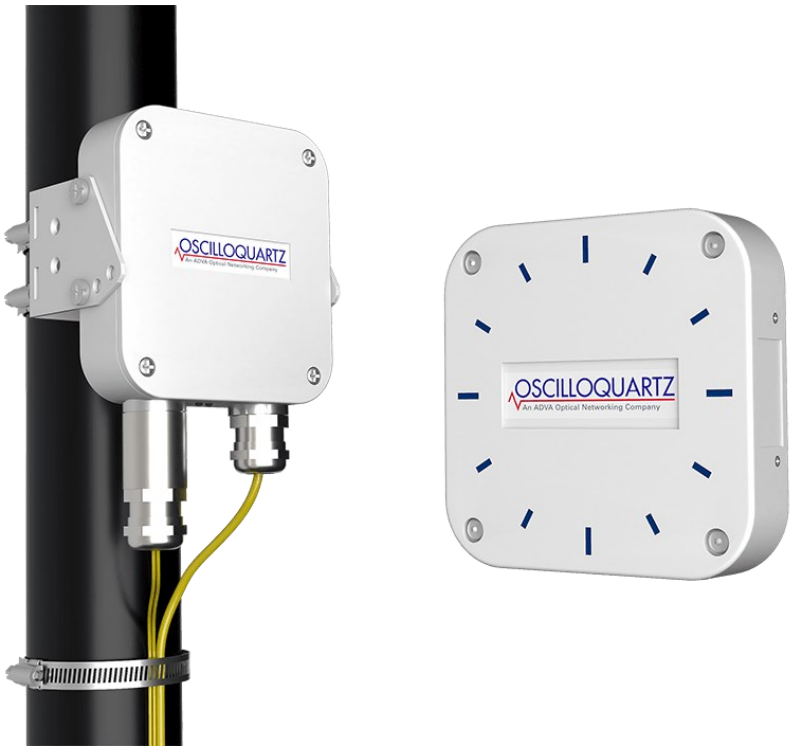

Figure 10. 5405-O Model [24].

All 5405 devices come with GPS, GLONASS, BeiDou and Galileo support. PTP and SyncE fallback options and PTP over layer 2 and IPv4/IPv6. Their receivers also provide an accuracy of +/- 100 ns from UTC on all other than 5405-MB's receiver, which provides an accuracy of +/- 40 ns. The 5405 devices are powered with power over ethernet.

3.2 Other Products

Some of the heavier products Oscilloquartz makes are the 5440, which they call a core PTP grandmaster and it can have over 2 000 unicast slaves (figure 11). The 5440 features an expansion card system, where it is possible purchase up to ten extra expansion cards for extra features to the device. The base unit has eight SyncE/NTP/PTP ports and 40 more can be added with additional line cards and it is also able to have up to four hot-swappable power supplies for redundancy. The 5440 also comes with a web graphical user interface, CLI and SNMP support for remote management.

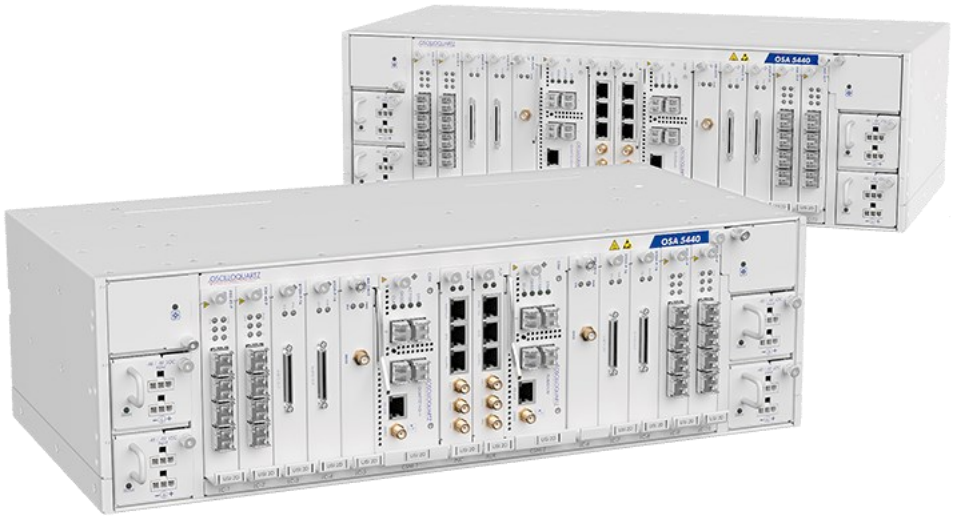

Figure 11. Two 5440 devices [25].

Oscilloquartz also makes cesium clocks like the 3230B, which is an extremely accurate and stable primary reference clock. This device is promised to have an accuracy of around one picosecond for frequency and the device has a ten- or eight-year lifetime depending on the chosen model. The device comes with two direct frequency outputs, one analog output and three digital output interfaces. There is also a possibility to get an additional signal expansion packet with four more digital outputs and one analog output.

4 SNR and AGC

The SNR value indicates the ratio of the power of the useful signal to the noise signal. This is an important value used in electronics, telecommunications and radio technology among others. This is also a very useful value for GNSS receivers to know how good each satellite's signal is. As can be seen from formulas one and two, SNR can be calculated by dividing the signal with the noise levels and because SNR is a power ratio it can also be expressed in decibels.

$$SNR = \frac{Psignal}{Pnoise} \quad (1)$$

$$SNR = 10log_{10}\left(\frac{Psignal}{Pnoise}\right) dB \quad (2)$$

AGC is a closed-loop control system, which is used to stabilize received signals to stay at appropriate levels. AGC circuits can be found in a variety of systems where the amplitude of the input signal changes a lot, like radio receivers, radars, audio equipment and video equipment. The AGC value changes based on the received signal levels. Basically meaning that the stronger the signal is, less compensating has to be done by the AGC meaning a lower value. AGC resides in the analog front end part of the receiver (figure 12).

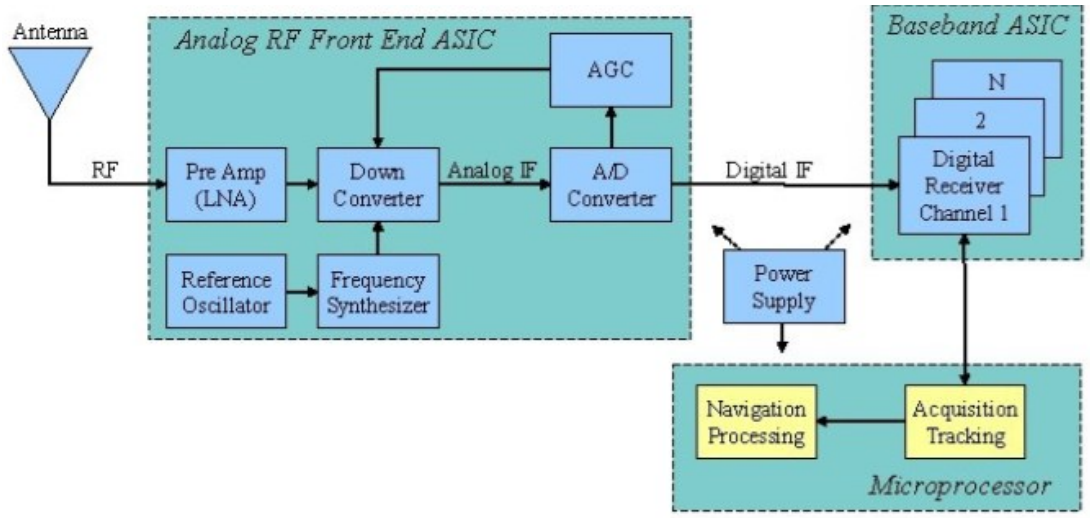

Figure 12. Typical GNSS receiver block diagram [26].

Combining both the AGC and SNR values can be used for spoofing detection by monitoring for sudden unexpected changes in these values. As spoofing attacks rely on overpowering the real GNSS signal, this should affect the AGC value by lowering it since it has to do less compensating. The SNR value should increase, because of each satellites signal is being transmitted with higher power.

5 Implementation

5.1 Preliminary testing

Before starting to implement the monitoring feature, some preliminary testing was required to know how the SNR and AGC values change over longer periods of time and also to get an understanding of how these values react to spoofing events. This is needed to figure out what kind of threshold values and timeframes should be used. A 5405-P with an external rooftop antenna was used for most of the experiments, but some experiments were also made with a 5401 and a 5405-MB.

First step was to measure both values over a long period of time. The 540X devices have a feature that allows data to be sent to a syslog server. It was used to capture the values every 20 seconds for a period of around 15 hours. The results showed that under normal conditions the AGC values seemed to be extremely stable. In the experiments with a 5405-P and 5401 the AGC value did not change at all. During other tests however with a 5405-MB the value did drop about 350 points every once in a while, which is approximately a 4,2 percent drop. It must also be taken into consideration that the AGC value can differ with different receiver models and constellations that are used, because it has no standardization.

The SNR values fluctuated a bit under ten points during the tests and the average value stayed within a few points from the current value (figure 13). The average used in these experiments was the last 15 points, which is equal to five minutes.

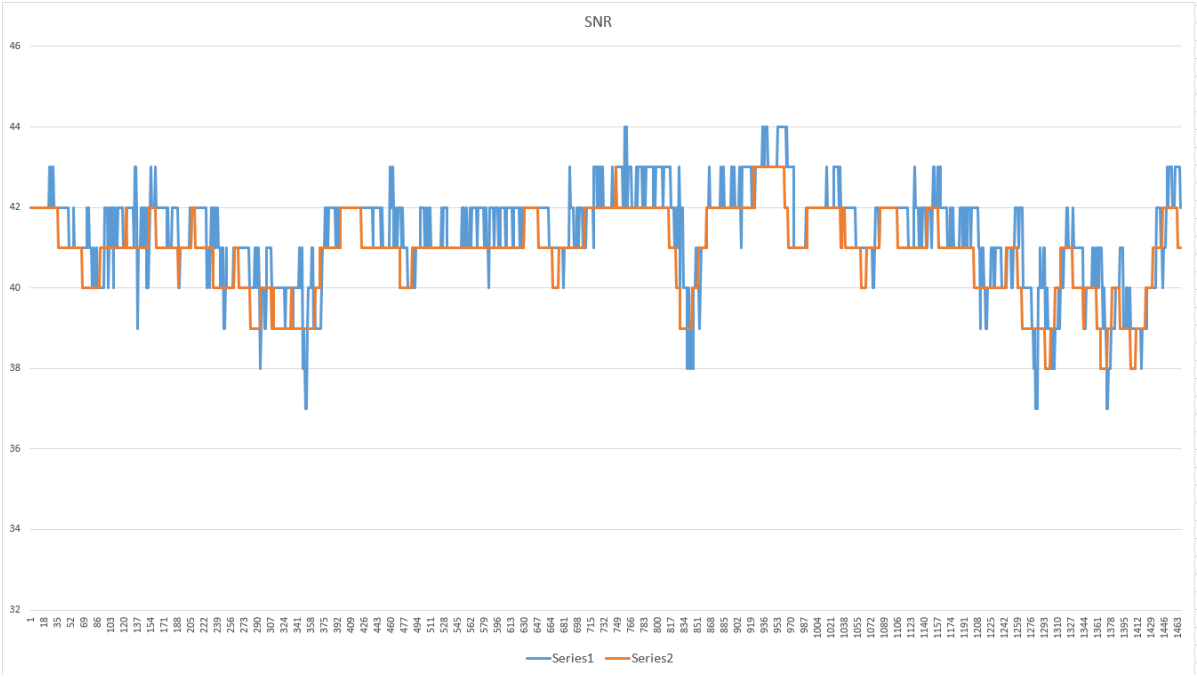

Figure 13. Results of SNR measurement on a 5405-P. Blue line represents the current SNR value and the orange one represents the average.

After some testing on how the values change in normal conditions, a GNSS simulator signal was used to see how the values react in a spoofing situation. The GNSS simulator in use is not as sophisticated as some other spoofing devices, which should be taken into consideration when going through the results. A GSG-5 Series Multi-Function GNSS simulator by Spectracom was used for the testing. It also should be taken into consideration that the antenna's signal is amplified by the GNSS splitter, while the simulator's signal is not (figure 14).

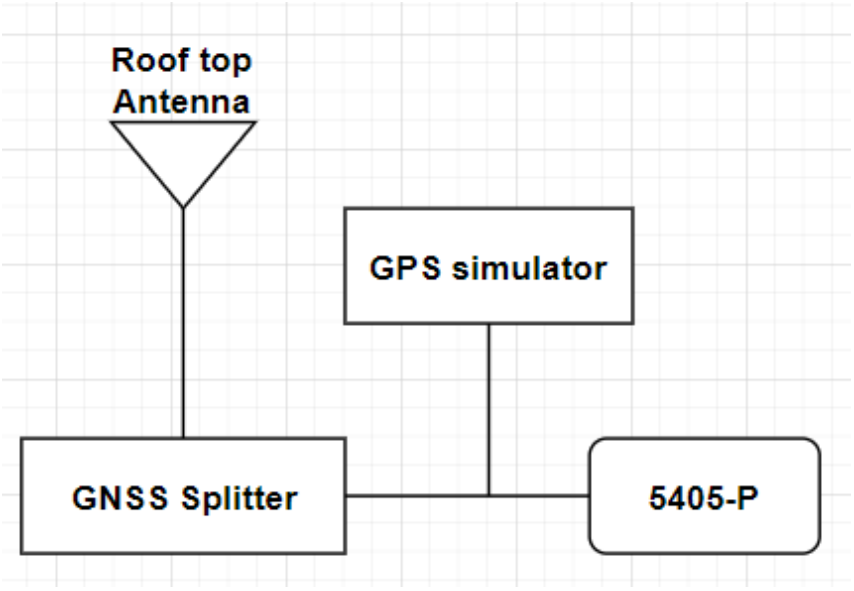

Figure 14. The topology used in testing.

The GNSS simulator's signal power had to be turned to almost maximum until the 5405-P started to get affected. Under normal circumstances the required signal power from the spoofer would most likely be less, because it would also be affected by any post antenna amplification. The 540X devices receivers documentation states that the AGC value uses a range between 0 and 8191. The receivers documentation does not state any particular reason on why this range was chosen. Value of 8191 means that the AGC is doing the maximum amount of compensation possible.

In the first spoofing test the 5405-P was first locked into a real GPS signal and then the simulator signal was added. Then the simulator signals power was increased rapidly until at the maximum of -65 dBm. The AGC value started decreasing very fast and dropped by a bit under 1000 units from 2808 to 1950. The SNR first decreased drastically from an average of around 40 to 26 and then after a while rose rapidly to around 50 (figure 15). This is most likely because of the receiver first losing the lock from the authentic signals because of a rival much stronger signal presence, which explains the rapid decline. Then the receiver locked into the fake signals created by the simulator, which explains the sudden rise after.

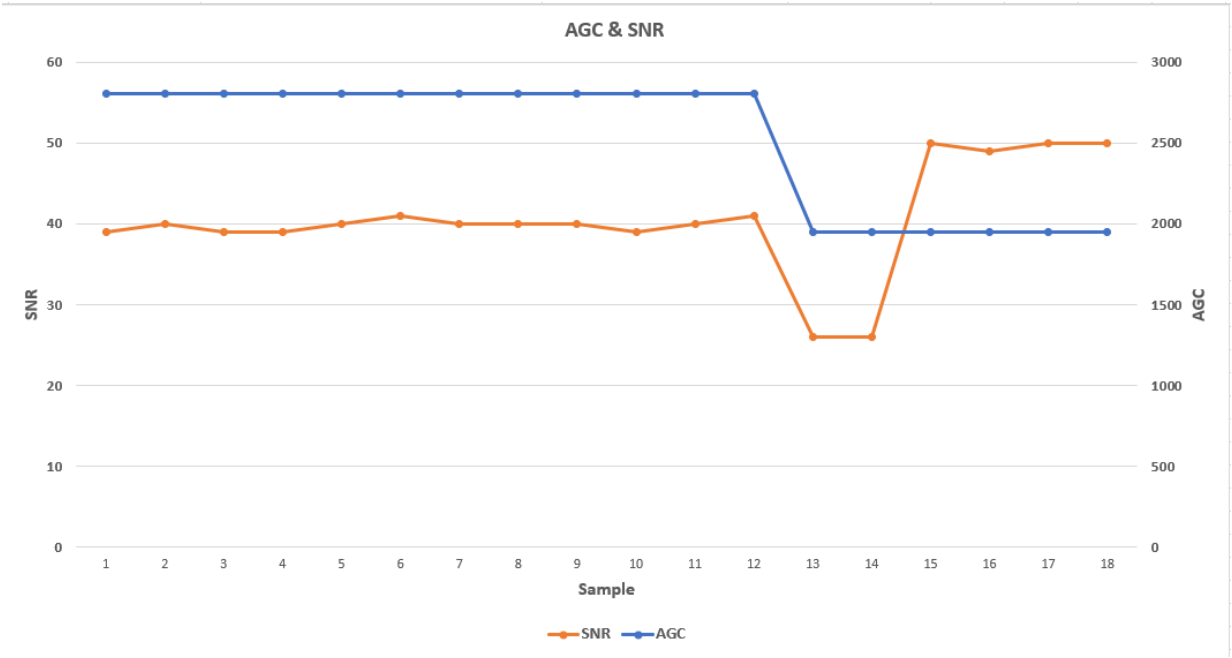

Figure 15. Results from a spoofing test. Simulator signal was added at sample number 12.

In another similar test where the setup was changed so the real signal would not be affected by the splitter amplification. In this test results were mostly the same except for the AGC value, which was around 4000 in the beginning and dropped to around 1650 when the simulator's signal was added. By this we can determine that the GNSS splitters effect to the AGC was around 1200. The same tests were also conducted on a 5401 and the results were very similar.

5.2 Implementation

First steps of the implementation was to figure out the appropriate amount of time the average SNR and AGC should be calculated over and the appropriate amount of samples that should be collected. This feature was written in C programming language. The implementation of the software will be described next.

First thing that needs to be done is to check if the constellation in use has changed, the satellite list is empty, GNSS status has changed or the antenna

has been disconnected. All of these impact the AGC and SNR values. If any of these is true then the monitoring is reset. This is to make sure there are no accidental spoofing alarms going off. The next step was to calculate the current average SNR value from all the currently available satellites and get the current AGC value. After that we compare the new values to previous averages if enough samples have been collected.

If the new values exceed the set thresholds from the averages and enough samples have been collected, the spoofing alarm will be turned on and the new values will not be added to the sample list. The monitoring keeps the alarm on until the current values return to be within the set thresholds from the average. After the AGC and SNR are back within the thresholds, monitoring can continue normally.

If the thresholds are not exceeded or not enough samples have yet been collected, the new values will be added to the sample list. Then finally a new average value will be calculated from the available sample list.

Overall the implementation was fairly simple, but it did take a long time to figure out good threshold values for both the AGC and the SNR and to figure out an appropriate sample rate and size. These values seem to be set at good points at the moment, but that might change in the future when testing is done at a larger scale.

5.3 Testing after implementation

The feature was tested again on the 5405-P and on a 5401 in a similar setup as before. In the first series of tests with the 5405-P, the monitoring feature was able to identify spoofing attacks in six out of nine tests. After setting the threshold values to be a bit more sensitive, ten more test were conducted. Both of the devices were able to identify the spoofing attacks every time on the rest of the tests (figure 15).

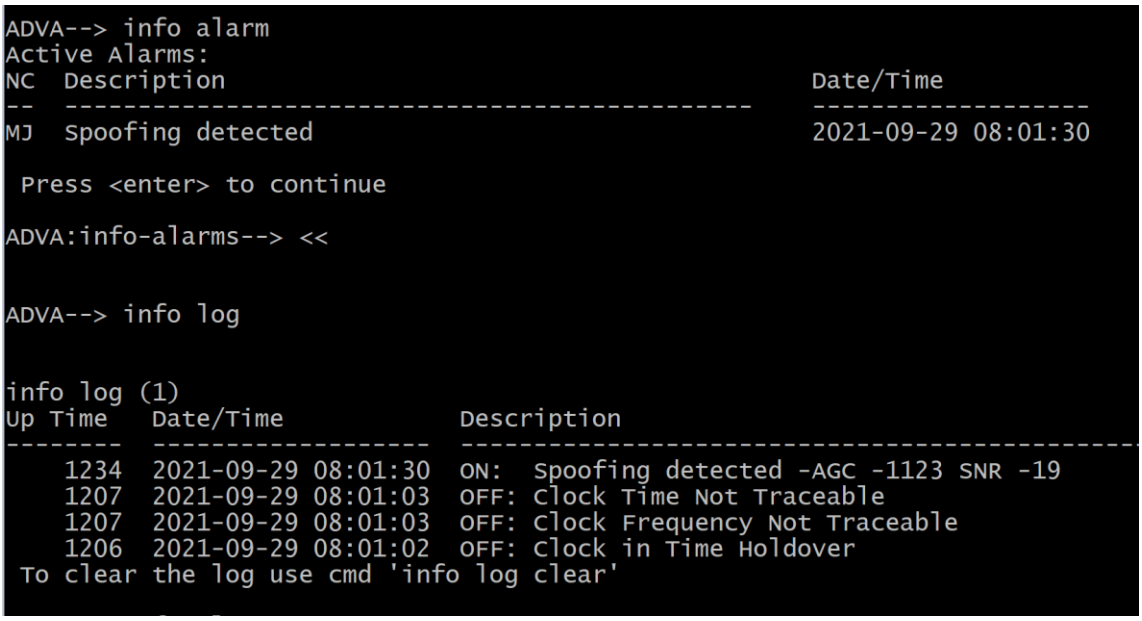

Figure 16. Info log and info alarm outputs on CLI from a 5405-P in a spoofing event.

As can be seen from figure 15 the spoofing event triggers an alarm, which can be seen in the device with “info log” or “info alarm” commands. In the log screen the current deviation of the AGC and SNR values are shown. In this case AGC being -1123 and SNR being -19 from the average. In this scenario the GNSS simulator had just been connected and the power was slowly being increased.

The basic idea behind every test was the same. First the device was locked into a real GNSS signal for at least five minutes. The GNSS simulator signal was then mixed with the real signal at different power levels. The simulated signals power was then increased at different speeds until the device locked into the fake signal.

On some of the tests on the 5401 the GNSS receivers own jamming indicator also worked, but only on a few occasions. The receivers jamming indicator seemed to work if the simulators power was increased very quickly to maximum, but if the power was raised slower or if it was not raised all the way to maximum the indicator did not work. The receivers spoofing indicator never turned on. From these tests it should not be assumed that the receivers spoofing indicator does not work at all, but rather that it is ineffective against

these particular simulator tests. If tested with other equipment it may very well be that the indicator works really well. The receivers documentation states that the spoofing indicator is most easily turned on in the transition phase from a real signal to a spoofed signal.

6 Conclusion

The goal for the thesis was to create a AGC and SNR monitoring software and see how well it can be used for spoofing detection. Overall the monitoring software worked relatively well and is definitely an improvement from the receivers own detection system. This kind of feature can be used for spoofing detection, but it should not be the only defence. A well protected system needs many different types of defences. AGC and SNR monitoring can be used as one of them. Spoofing is a very complex subject and there is no one and all solution for defence.

Even though tests conducted within this thesis show that AGC and SNR monitoring works quite well, it should be assumed that if spoofing is done with more sophisticated equipment the results can be different. It is also difficult to decide where the threshold values should be set, which means they might still be changed in the future. There are many different factors that can alter the AGC and SNR values and all of the tests were done in a stable lab environment with a good antenna placed in a high position on the roof, which might make the values seem more stable than they actually are.

The feature is currently being used in 540X devices as one of many layers of protection against spoofing. The next step for this feature would be to test it with other spoofing devices and in other environments. In the future more values from the receiver could be added to the monitoring as well to improve the effectiveness. It could also be possible to make the threshold values adaptive or create a light machine learning type solution. The solution has to be light in any case, because of the limited free memory and processing power available.

References

1 Vijay. GPS spoofing and dangers of GPS data hacking. www.techworm.net ;2016. <https://www.techworm.net/2016/11/gps-spoofing-dangers-gps-data-hacking.html> [accessed 22, October, 2021].

2 GNSS INTERFERENCE MAP. https://www.regulus.com; <https://www.regulus.com/gnss-interference-map> [accessed 22, October, 2021].

3 Patrick Tucker. DHS: Drug Traffickers Are Spoofing Border Drones. www.defenseone.com; 2015. <https://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/> [accessed 8, July, 2021].

4 Greg Sadlier; Rasmus Flytkjær; Farooq Sabri; Daniel Herr. The economic impact on the UK of a disruption to GNSS. https://assets.publishing.service.gov.uk/; 2017. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf> [accessed 8, July, 2021].

5 The European GNSS Agency. GSA GNSS Market Report. www.euspa.europa.eu; 2019. <https://www.euspa.europa.eu/system/files/reports/market_report_issue_6_v2.pdf> [accessed 20, September, 2021].

6 Timing. www.gps.gov; <https://www.gps.gov/applications/timing/> [accessed 22. October, 2021].

7 Eric Olson. How Does GPS Work. insights.globalspec.com; 2018. <https://insights.globalspec.com/article/10315/how-does-gps-work> [accessed 12, September, 2021].

8 Galileo services. https://www.esa.int/; <https://www.esa.int/Applications/Navigation/Galileo/Galileo_services> [accessed 15, July, 2021].

9 The European GNSS Agency. GNSS User Technology Report. www.euspa.europa.eu; 2020. <https://www.euspa.europa.eu/simplecount_pdf/tracker?file=uploads/technology_report_2020.pdf> [accessed 3, September, 2021].

10 750 Million. https://time.com/; 2012. <https://nation.time.com/2012/05/21/how-much-does-gps-cost/> [accessed 12, July, 2021].

11 Galileo's clocks. https://www.esa.int/; <https://www.esa.int/Applications/Navigation/Galileo/Galileo_s_clocks> [accessed 28, July, 2021].

12 Galileo (satellite navigation). https://en.wikipedia.org/; <https://en.wikipedia.org/wiki/Galileo_(satellite_navigation)> [accessed 22, July, 2021].

13 BEIDOU. https://www.glonass-iac.ru; <https://www.glonass-iac.ru/en/BEIDOU/> [accessed 5, August, 2021].

14 BeiDou. https://en.wikipedia.org/; <https://en.wikipedia.org/wiki/BeiDou> [accessed 12, September, 2021].

15 Sergey Revnivykh. GLONASS status and Modernization. https://www.unoosa.org; 2012. <https://www.unoosa.org/pdf/icg/2012/icg-7/3-1.pdf> [accessed 12, September, 2021].

16 Jackson Murphy. What is SBAS and how does it work?| Free SBAS coverage map. https://blog.junipersys.com/; 2018. <https://blog.junipersys.com/how-does-sbas-improve-gps-free-sbas-coverage-map/> [accessed 11, August, 2021].

17 GPS Jammers Used in 85% of Cargo Truck Thefts – Mexico Has Taken Action. https://rntfnd.org/; 2020. <https://rntfnd.org/2020/10/30/gps-jammers-used-in-85-of-cargo-truck-thefts-mexico-has-taken-action/> [accessed 15, July, 2021].

18 Steve Strunsky. N.J. man fined $32K for illegal GPS device that disrupted Newark airport system. https://www.nj.com; 2019. <https://www.nj.com/news/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html> [accessed 6, August, 2021].

19 Douglas Arnold. GNSS Jamming and how to mitigate it. blog.meinbergglobal.com/; 2020. <https://blog.meinbergglobal.com/2020/04/12/gnss-jamming-and-how-to-mitigate-it/> [accessed 12, September, 2021].

20 Roi Mitt. Top 10 GPS Spoofing Events in History. https://threat.technology/; <https://threat.technology/top-10-gps-spoofing-events-in-history/> [accessed 5, August, 2021].

21 AUTOMOTIVE NAVIGATION CYBERSECURITY. https://www.regulus.com; <https://www.regulus.com/automotive-solution> [accessed 29, July, 2021].

22 Douglas Arnold. GNSS Spoofing and how to mitigate it. https://blog.meinbergglobal.com; 2020. <https://blog.meinbergglobal.com/2020/04/14/gnss-spoofing-and-how-to-mitigate-it/> [accessed 12, September, 2021].

23 OSA 5401 Series. https://www.oscilloquartz.com; <https://www.oscilloquartz.com/en/products-and-services/ptp-grandmaster-clocks/sfp-pluggable-ptp-grandmasters/osa-5401-series> [accessed 12, July, 2021].

24 OSA 5405 Series. https://www.oscilloquartz.com; <https://www.oscilloquartz.com/en/products-and-services/ptp-grandmaster-clocks/integrated-gnss-ptp-grandmasters/osa-5405-series> [accessed 12, July, 2021].

25 Core PTP grandmasters. https://www.oscilloquartz.com; <https://www.oscilloquartz.com/en/products-and-services/ptp-grandmaster-clocks/core-ptp-grandmasters> [accessed 12, July, 2021].

26 Software Receiver Technology. https://slidetodoc.com; <https://slidetodoc.com/the-galileo-gps-software-receiver-company-software-receiver/> [Accessed 2, September, 2021].