Università degli Studi di Padova

Corso di Laurea Magistrale in
Ingegneria delle Telecomunicazioni

Identification of spoofed GNSS signal from carrier phase measurements with multiple antennas

Laureando
Davide Reginato

Relatore
Prof. Nicola Laurenti

Anno Accademico 2016/2017

To my family

Contents

Abstract

GNSS-dependent positioning, navigation and timing synchronization procedures have a significant impact on everyday life. Therefore, such a widely used system is becoming an attractive target for terrorists and hackers for various motives. As a consequence, spoofing and antispoofing algorithms have become an important research topic within the GNSS discipline. In this thesis the environment of a fixed single-antenna spoofer and a fixed multi-antenna receiver is analysed and a new algorithm for spoofing detection is proposed which uses differential GNSS measurements.

Chapter 1

Introduction

GNSS-dependent systems are widespread in current positioning and navigation applications. There is an increasing attention to safe and secure GNSS applications such as air, marine and ground transportations, police and rescue services, telecommunication systems and mobile phone. Nowadays, most mobile phones as well as vehicles are equipped with positioning and navigation systems utilizing GNSS systems. In addition, countless time tagging and synchronization systems in the industries rely primarily on GNSS. As a consequence, GNSS systems is becoming an attractive target for illicit disruption by terrorists and hackers.

GNSS signals are vulnerable to in-band interferences because of being extremely weak broadcast signals over wireless channels. Therefore, it is sufficient a low-power interference to jam or spoof GNSS receivers for several kilometres of distance. For example, spoofing attack could effectively deceive an activity monitoring GNSS receiver mounted on a cargo transport. Therefore, the GNSS receiver will be logging a counterfeit trajectory with various consequences.

Spoofing and antispoofing mechanisms are emerging issues in modern GNSS applications that will increasingly attract research in future [1]. Spoofing is a deliberate interference that aims to force GNSS receivers in generating false position solutions [2]. The spoofer attempts to resemble authentic GNSS signals in order to mislead the target receiver. Recently the implementation of sophisticated spoofers has become more feasible and less costly due to rapid advances in software-defined radio (SDR) technology [4].

This thesis investigates this problem on applications where there is a fixed receiver with multiple antennas exploiting Differential GNSS (DGNSS) measurements. This environment corresponds to different applications such as mobile phone network cells.

The thesis is organized as follows: an overview on how a GNSS system

works in chapter 2 followed by the description of the signal model considered for the proposed algorithm in chapter 2. Then there is chapter 3 which describes what spoofing is and the most famous countermeasures with the description of the improved algorithm which is based on the results on [3]. In chapter 4 i will be shown the proposed algorithm performance in spoofing detection and spoofed satellites identification. Concluding considerations are provided in chapter 5.

Chapter 2

GNSS system description

In this chapter it will be described the fundamental concepts to understand how a GNSS system works starting from the geometrical properties of the satellite constellation to fulfil all the GNSS requirements to calculate the user position. Moreover, there is a part where it is described the two process of the receiver which permit to the user to discover which satellites are in view and, subsequently, to track them.

2.1 Constellation

Satellite navigation constellations have very different geometrical constraints from satellite communications systems, first of all the multiplicity of coverage. The navigation solution requires a minimum of four satellites to be in view of a user to provide the minimum of four measurements necessary to determine three-dimensional position and time. Therefore, a constraint on the constellation is that it must provide a minimum of coverage of four satellites at all times. In order to ensure this level of coverage, the nominal constellation was designed to provide more than four satellites in view so that this constraint can be maintained even with a satellite runs out of service. Also, more than four satellites in view is useful for user equipment to be able to determine if a satellite is measuring a signal or timing anomaly. Therefore, the practical constraint for coverage of the constellation is a minimum six satellites in view above 5° minimum elevation angle. The problem of constellation design for satellite navigation has the following major constraints:

1. Coverage needs to be global.

2. At least six satellites need to be in view of any user position at all times.

3. The constellation needs to have good geometric properties, which requires a dispersion of satellites in both azimuth and elevation angle from a user.

4. The constellation needs to be robust against single satellite failures.

5. The constellation must be maintainable given the increased frequency of satellite failures with a large constellation.

6. It is preferable to minimize the frequency and magnitude of manoeuvres required to maintain the satellites within the required range of their orbital parameters.

7. There are trade-offs between the distance of the satellite from the surface of the Earth versus payload weight.

In particular, for the GPS constellation a 6-plane configuration was selected with four satellites per plane. The orbital planes are inclined by 55°, in accordance with Walker's results. The planes are equally spaced by 60° in right ascension of the ascending node around the equator. Satellites are not equally spaced within the planes, and there are phase offsets between planes to achieve improved geometric dilution of precision characteristics of the constellation. Hence, the GPS constellation can be considered a tailored Walker constellation. For a complete description of the Walker constellation read [5].

2.2 Calculating user position

In order to determine user position in three dimensions (x_u, y_u, z_u) and the offset t_u, pseudorange measurements are made to four satellites resulting in the system of equations

$$\rho_j = \| \mathbf{s}_j - \mathbf{u} \| + ct_u \tag{2.1}$$

where j ranges from 1 to 4 and references the satellites. Equation can be expanded into the following set of equations in the unknowns x_u, y_u, z_u, and t_u:

$$\rho_1 = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} + ct_u \tag{2.2}$$

$$\rho_2 = \sqrt{(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2} + ct_u \tag{2.3}$$

$$\rho_3 = \sqrt{(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2} + ct_u \tag{2.4}$$

$$\rho_4 = \sqrt{(x_4 - x_u)^2 + (y_4 - y_u)^2 + (z_4 - z_u)^2} + ct_u \tag{2.5}$$

where x_j, y_j, and z_j denote the jth satellite's position in three dimensions.

2.3 Satellite signal acquisition

Signal acquisition is a search process. This search process, like the tracking process, requires replication of both the code and the carrier of the space vehicle (SV) to acquire the SV signal. The range dimension is associated with the replica code. The Doppler dimension is associated with the replica carrier. The initial search process is always a C/A code search for C/A code receivers and usually begins with a C/A code search for P(Y) code receivers. The initial C/A code search usually involves replicating all 1,023 C/A code phase states in the range dimension. Some criteria must be established to determine when to terminate the search process for a given SV and select another candidate SV. Fortunately, the range dimension for C/A code search is bounded by the ambiguity of C/A code to only 1,023 chips total range uncertainty, but it is essentially unbounded for direct P(Y) code search.

One Doppler bin is defined as approximately $2/(3T)$, where T = signal integration time per cell or dwell time per cell. Dwell times can vary from less than 1 ms (Doppler bins of about 667 Hz) for good C/N_0 signals up to 10 ms (67-Hz Doppler bins) for bad C/N_0 signals. Unfortunately, the actual C/N_0 is unknown until after the SV signal is acquired. Signal obscuration, RF interference, ionospheric scintillation and antenna gain roll-off can all significantly reduce C/N_0. The search pattern usually follows the range direction from early to late in order to avoid multipath with Doppler held constant until all range bins are searched for each Doppler value. In the Doppler bin direction, the search pattern typically starts from the mean value of the Doppler uncertainty and then continues one Doppler bin at a time on either side of this value until the 3-sigma Doppler uncertainty has been searched. Then the search pattern is repeated, typically with a reduction in the search threshold scale factor. It is important to recognize that the C/A code autocorrelation and crosscorrelation sidelobes can cause false signal detections if these sidelobes are strong enough. The sidelobes tend to increase as the search dwell time is decreased. To counter this problem, a combination of both increased dwell time (to minimize sidelobes) and a high detector threshold setting (to reject sidelobes) can be used for the initial search pass. On subsequent search passes, the dwell time and threshold can be decreased. The penalty for this scheme is increased search time when the C/N_0 is low. During the dwell time, T, in each cell, the I (In-Phase) and Q (Quadrature-Phase) signals are integrated and dumped and the envelope $\sqrt{I^2 + Q^2}$ is computed. Each envelope is compared to a threshold to determine the presence or absence of the SV signal. The detection of the signal is a statistical process because each cell either contains noise with the signal absent or noise with the signal present. Each case has its own probability

density function (pdf). The pdf for noise with no signal present, $p_n(z)$, has a zero mean. The pdf for noise with the signal present, $p_s(z)$, has a nonzero mean. The threshold is usually based on an acceptable probability of false alarm, P_{fa}. For the chosen threshold, V_t, any cell envelope that is at or above the threshold is detected as the presence of the signal. Any cell envelope that is below the threshold is detected as noise. There are four outcomes of the decision processes, two wrong and two right. The two statistics that are of most interest for the signal detection process are the probability of detection, P_d, and the probability of false alarm, P_{fa}. These are determined as follows:

$$P_d = \int_{V_t}^{\inf} p_s dz \tag{2.6}$$

$$P_{fa} = \int_{V_t}^{\inf} p_n dz \tag{2.7}$$

where:

- $p_s(z)$ = pdf of the envelope in the presence of the signal
- $p_n(z)$ = pdf of the envelope with the signal absent

To determine these pdfs, assume that I and Q have a Gaussian distribution. Assuming that the envelope is formed by $\sqrt{I^2 + Q^2}$, then $p_s(z)$ is a Ricean distribution [15] defined by:

$$p_s(z) = \begin{cases} \frac{z}{\sigma_n^2} e^{-(\frac{z^2+A^2}{2\sigma_n^2})} I_0(\frac{zA}{\sigma_n^2}), & z \geq 0 \\ 0, & z < 0 \end{cases} \tag{2.8}$$

where:

- z = value of the random variable
- σ^2 = RMS noise power
- A = RMS signal amplitude
- $I_0(\frac{zA}{\sigma_n^2})$ = modified Bessel function of zero order

Equation (2.8) for $z \geq 0$ can be expressed in terms of the predetection SNR as presented to the envelope detector, C/N, as follows:

$$p_s(z) = \frac{z}{\sigma_n^2} e^{-(\frac{z^2}{2\sigma_n^2} + C/N)} I_0(\frac{z\sqrt{2C/N}}{\sigma_n}) \tag{2.9}$$

where:

- C/N = predetection signal to noise ratio
- $C/N = A^2/2\sigma_n^2 = (C/N)T$
- T = search dwell time

For the case where there is no signal present, then evaluating (2.8) for $A = 0$ yields a Rayleigh distribution for $p_n(z)$, which is defined by:

$$p_n(z) = \frac{z}{\sigma_n^2} e^{-(\frac{z^2}{2\sigma_n^2})} \tag{2.10}$$

The result of integrating (2.7) using the pdf of (2.10) is:

$$p_{fa} = e^{-(\frac{V_t^2}{2\sigma_n^2})} \tag{2.11}$$

Rearranging (2.11) yields the threshold in terms of the desired probability of false alarm and the measured 1-sigma noise power:

$$V_t = \sigma_n \sqrt{-2 \ln P_{fa}} = X\sigma_n \tag{2.12}$$

For example, if it is desired that $P_{fa} = 16\%$, then $V_t = X\sigma_n = 1.9144615\sigma_n$. Using this result, the probability of detection, P_d, is computed for the expected C/N_0 and dwell time, T, using (2.6) and (2.9) with $\sigma_n = 1$ (normalized).

2.4 Satellite signal tracking

There are two different approaches to track a signal satellite. One which utilizes a replica of the carrier of the signal satellite, called Carrier tracking loop, and the other utilizes a replica of the satellite PRN code, called Code tracking loop. In this section these two techniques will be described.

2.4.1 Carrier tracking loop

Figure 2.1 presents a block diagram of a receiver carrier tracking loop. The designs of the carrier predetection integrators, the carrier loop discriminators and the carrier loop filters characterize the receiver carrier tracking loop. These three functions determine the two most important performance characteristics of the receiver carrier loop design: the carrier loop thermal noise error and the maximum LOS dynamic stress threshold. Since the carrier tracking loop is always the weak link in a stand-alone GNSS receiver, its threshold characterizes the unaided GNSS receiver performance.

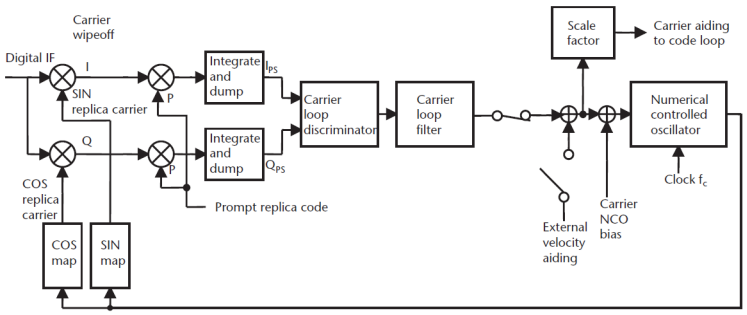


Figure 2.1: Generic GNSS receiver carrier tracking loop block diagram (Fig. from [11]

The carrier loop discriminator defines the type of tracking loop as a PLL, a Costas PLL, which is a PLL-type discriminator that tolerates the presence of data modulation on the baseband signal, or a frequency lock loop (FLL). The PLL and the Costas loop are the most accurate, but they are more sensitive to dynamic stress than the FLL. The PLL and Costas loop discriminators produce phase error estimates at their outputs. The FLL discriminator produces a frequency error estimate. Because of this, there is also a difference in the architecture of the loop filter.

To tolerate dynamic stress, the predetection integration time should be short, the discriminator should be an FLL, and the carrier loop filter bandwidth should be wide. However, for the carrier measurements to be accurate, the predetection integration time should be long, the discriminator should be a PLL, and the carrier loop filter noise bandwidth should be narrow. As a consequence some compromises must be made to resolve this opposite requirements. A well-designed GNSS receiver should close its carrier tracking loops with short predetection integration times, using an FLL and a wideband carrier loop filter. Assuming there is data modulation on the carrier, it should then automatically change into a Costas PLL, gradually adjusting the predetection integration time equal to the period of the data transitions while also gradually adjusting the carrier tracking loop bandwidth as narrow as the dynamics permits.

2.4.2 Code tracking loop

Figure 2.2 shows a block diagram of a GNSS receiver code tracking loop. The designs of the predetection integrators, the code loop discriminator and the code loop filter characterize the receiver code tracking loop. These three functions determine the most important two performance characteristics of

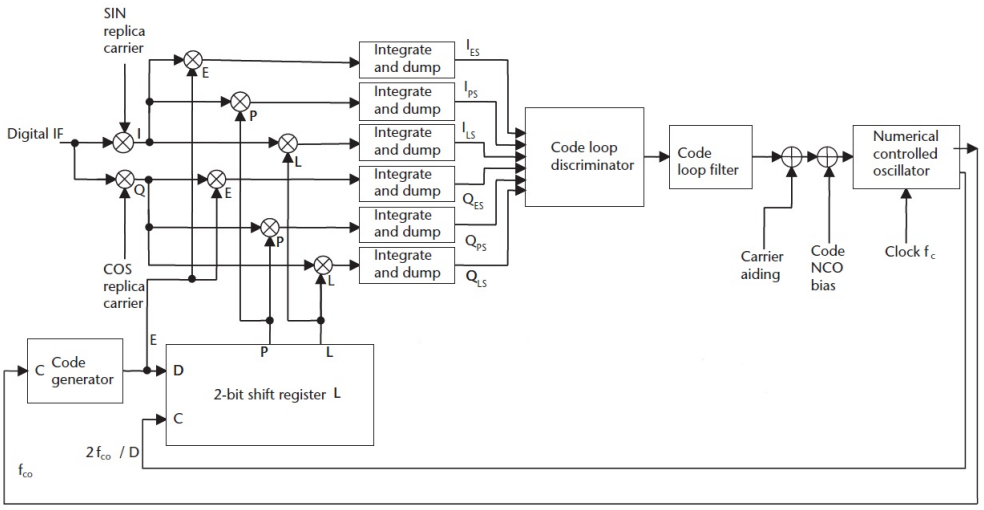


Figure 2.2: Generic GNSS receiver code tracking loop block diagram (Fig. from [11]

the receiver code loop design: the code loop thermal noise error and the maximum LOS dynamic stress threshold. Even though the carrier tracking loop is the weaker in terms of the receiver's dynamic stress threshold, it would be disastrous to attempt to aid the carrier loop with the code loop output. This is because the code loop thermal noise is orders of magnitude larger than the carrier loop thermal noise. In general coherent DLL provides superior performance when the carrier loop is in PLL. Under this condition, there is signal plus noise in the I components and mostly noise in the Q components. However, this high-precision DLL mode fails if there are frequent loss of phase lock because the signal power is shared in both the I and Q components, which consequently causes power loss in the coherent DLL. All of the DLL discriminators can be normalized. Normalization removes the amplitude sensitivity, which improves performance under rapidly changing SNR conditions. Therefore, normalization helps the DLL tracking and threshold performance to be independent of AGC performance. However, normalization does not prevent reduction of the gain when SNR decreases.

Chapter 3

Signal model

In this chapter it will be described the signal model used to test the algorithm for spoofing detection, in particular there is an explanation of what differential GNSS measurements are and which approximations have been done to verify the performance of the spoofing detection technique.

3.1 Differential GNSS measurements

A single-frequency SPS (Standard Positioning Service) GNSS user can often attain better than 10 m, 95% positioning and 20 ns, 95% timing accuracy worldwide. There are many applications, however, that require levels of accuracy, integrity, availability, and continuity beyond even what a GNSS PPS (Precise Positioning Service) receiver can provide. For such applications, augmentation is required. There are two general classes of augmentation: differential GNSS (DGNSS) and external sensors/systems.

DGNSS is a method to improve the positioning or timing performance of GNSS using one or more reference stations at known locations, each equipped with at least one GNSS receiver. The reference station provides information to the end user via a data link that may include:

- corrections to the raw end user's pseudorange measurements, corrections to GNSS satellite-provided clock and ephemeris data, or data to replace the broadcast clock and ephemeris information;
- raw reference station measurements (e.g., pseudorange and carrier phase);
- integrity data (e.g., reliability indications for each visible satellite);
- auxiliary data including the location, health and meteorological data of the reference station.

DGNSS techniques may be categorized in different ways:

- absolute or relative differential positioning;
- local area, regional area or wide area;
- code based or carrier based.

In this work I used carrier-based GNNS technique to perform spoofing detection at end user side, in particular I used single difference carrier phase (SDCP) between two antennas of a GNSS receiver. This method is easily adaptable to multi-antenna GNSS receiver.

3.2 Model description

In this section I will describe the signal model used for the spoofing detection algorithm which is the topic of this thesis. Consider a two-antenna assembly positioned d metres apart from each other with an arbitrary orientation. The carrier phase Φ_m^i at the ith antenna ($i = 1, 2$) for the mth received PRN signal can be written as [7]:

$$\Phi_m^i = \frac{1}{\lambda}[\rho_m^i(t) + c(dt_m(t) - dT^i(t)) - \frac{I^i(t)}{f^2} + \zeta_m^i(t) + w_{\Phi_m^i}(t)] + N_m^i \quad (3.1)$$

where:

- $\rho_m^i(t)$ = true range between SV (at transmit time) and receiver (at receive time) [m]
- $\frac{I^i(t)}{f^2}$ = ionospheric delay parameter [Hz^2m)
- f = carrier signal frequency (1575.42 MHz for L1)
- $\zeta_m^i(t)$ = measurement delay due to troposphere [m]
- c = speed of light [m/s]
- $dT^i(t)$ = receiver clock error [s]
- $dt_m(t)$ = satellite clock error [s]
- $w_{\Phi_m^i(t)}$ = AWGN measurement noise due to receiver an multipath [m]
- λ = wavelength of L1 carrier

- N_m^i = integer carrier-phase cycle ambiguity [cycles]

The ionospheric error $\frac{I^i(t)}{f^2}$ has a negative sign, reflecting the fact that the ionosphere yields a delay of an advance of the phase measurement [8]. The term N_m^i is the carrier-phase integer ambiguity. This is necessary because the carrier-phase observable is not the total range measurement, but it is a measurement of the accumulated Doppler since a particular time epoch, at which time there was an unspecified (N) number of carrier cycles between the mth satellite and the ith receiver. The term N_m^i can be thought of as a constant, initially unknown bias added in each of the carrier-phase measurements which happens to be an integer number of cycles. The values for N_m^i are different and independent for measurements between different receivers or different satellites. However, the values for N are constant for the whole observation time.

Based on 3.1, between-receivers single difference carrier phase $\Delta\Phi_m^{1,2}$ observations can be written as:

$$\begin{aligned}\Delta\Phi_m^{1,2} &= \Phi_m^1 - \Phi_m^2 \\ &= \frac{1}{\lambda}[\Delta\rho_m^{1,2}(t) - c\Delta dT^{1,2}(t) - \frac{\Delta I^{1,2}(t)}{f^2} + \Delta\zeta_m^{1,2}(t) + w_{\Delta\Phi_m^{1,2}}(t)] + \Delta N_m^{1,2}\end{aligned} \tag{3.2}$$

We observed that the term relative to the satellite clock error in Equation 3.1 disappears in Equation 3.2 because is the same term of the mth satellite. In addition, receiver noise $w_{\Delta\Phi_m^{1,2}}(t)$ remains AWGN due to the fact that I performed only linear operations.

3.3 Considered approximations

Observing Equation 3.2 and considering the receiver antenna position, we can simplify SDCP model as:

$$\Delta\Phi_m^{1,2} = \frac{1}{\lambda}[\Delta\rho_m^{1,2}(t) + w_{\Delta\Phi_m^{1,2}}(t)] + \Delta N_m^{1,2} \tag{3.3}$$

This approximations are due to the fact that:

- ionospheric and tropospheric delays are the same on the two antennas because their short distance;
- the two antennas are synchronised with the same receiver, so the term $c\Delta dT^{1,2}(t)$ disappears.

Chapter 4

Spoofing

In this chapter there will be an overview on spoofing, in particular on the possible attacks and countermeasures to disturb GNSS user navigation. Moreover, there is a description of the particular environment where spoofing detection is performed and of the improvements which gives this new algorithm in spite of the one which is described in [3].

4.1 Spoofing techniques

A GNSS spoofing attack tries to deceive a GNSS receiver by broadcasting wrong GPS signals: structured to resemble a set of normal GNSS signals or by rebroadcasting genuine signals received at a different time. These spoofed signals may be modified to cause the receiver to estimate its position to be somewhere other than where it actually is or to be located where it is but at a different time, as determined by the attacker. One common form of a GNSS spoofing attack begins by broadcasting signals synchronized with the authentic signals observed by the target receiver. The power of the counterfeit signal is then gradually increased and the receiver follows the new spoofed signal instead of the authentic one.

Spoofing techniques can be divided into three main categories [2], [4], [9].

4.1.1 GNSS signal simulator

In this category a GNSS signal simulator with a RF front-end is used to resemble authentic GNSS signals. The signals generated by the spoofer are not essentially synchronized to the real GNSS signals. Therefore, the spoofing signal looks like noise for a receiver operating in the tracking mode. However, this type of spoofers can effectively deceive commercial GNSS receivers if

the spoofing signal power is higher than the authentic signals. A GNSS signal simulator is the simplest GNSS spoofer and it can be detected by different antispoofing techniques such as amplitude monitoring, consistency checks among different measurements, and consistency check with inertial measurement units (IMUs).

4.1.2 Receiver-Based Spoofers

A more advanced type of spoofer consists of a GNSS receiver with a spoofer. This system first synchronizes to the current GNSS signals and extracts the position, time, and satellite ephemeris, and then it generates the spoofing signal knowing the distance between its transmit antenna and the target receiver antenna. This kind of spoofer is difficult to discriminate from the authentic signals and is more complicated than the first category. The main challenge for the realization of this spoofer is transmitting the spoofing signals to the intended victim receiver with the correct signal delay and strength. Note that the spoofing power should be slightly higher than the authentic signal power to successfully mislead the target receiver but it should not be much more than the typical power of GNSS signals. Aligning the carrier frequency and phase to the authentic GNSS signals, minimizing the self-jamming effect and cancelling relative data bit latencies are other limitations that a receiver-based spoofer should deal with. Carrier phase alignment to the authentic signals needs centimetre level knowledge of the distance between the spoofer transmit antenna phase centre and the target receiver antenna phase centre. Therefore, it would be a great advantage for this spoofers if the spoofer antenna were very close to the target receiver antenna. This spoofers are relatively hard to detect since they are synchronized to the real GNSS satellites and can spoof receivers in tracking mode. Figure 4.1 shows a repeater-spoofer structure proposed by [4].

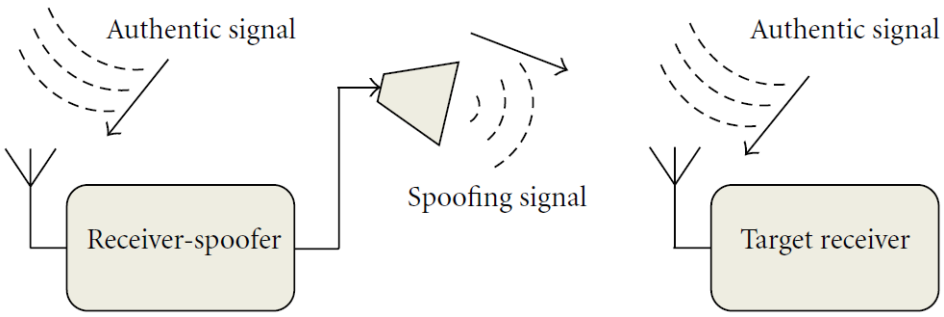


Figure 4.1: Repeater spoofer block diagram (Fig. from [4])

4.1.3 Sophisticated Receiver-Based Spoofers

This category is the most complex and effective type of the spoofing categories. This type is assumed to know the centimetre level position of the target receiver antenna phase centre to perfectly synchronize the spoofing signal code and carrier phase to those of authentic signals at the receiver [9]. This type of spoofer can take advantage of several transmit antennas in order to defeat direction of arrival antispoofing techniques. In this case the spoofer needs to synthesize an array manifold that is consistent with the array manifold of the authentic signal to defeat an angle of arrival (AOA) discriminating GNSS receiver. The complexity of constructing such a spoofer is much higher than the two previous categories discussed above. Compared to the previous spoofing categories, the effectiveness region of this type of spoofer is much more limited. The reason is that carrier phase alignment and array manifold synchronization might be achieved only for a very small region where target receiver antennas are located. In addition, there are some physical limitations regarding the spoofer antenna placement relative to the target receiver antennas. As such, the realization of this type of spoofers is very difficult and in many cases impossible due to the geometry and movement of the target receiver antennas.

4.2 Antispoofing techniques

Several antispoofing techniques have been proposed in the open literature and can generally be classified into two main categories, namely spoofing detection and spoofing mitigation. Spoofing detection algorithms concentrate on discriminating the spoofing signals but they do not necessarily perform countermeasures against the spoofing attack, while spoofing mitigation techniques mainly concentrate on neutralizing the detected spoofing signals and help the victim receiver to retrieve its positioning and navigation abilities. In the following subsections a brief introduction is provided on different techniques proposed for spoofing detection category, which the topic of interest of this thesis.

4.2.1 Spoofing detection

Based on the Signal Power Monitoring

1. C/N_0 *monitoring.* Most GNSS receivers employ C/N_0 measurements as a parameter that characterizes the received signal quality. In open sky conditions, only satellite movements and ionosphere variations can

cause gradual changes in the received signal power. However, when a higher power spoofer deceives a GNSS receiver, the received C/N_0 may experience a sudden change that can indicate the presence of the spoofing signal. The antispoofing receiver can continuously monitor the C/N_0 and look for any unusual variation that can be a sign of spoofing attack. It is easy for a GNSS receiver to store a time history of the signal received from each satellite.

2. *Absolute power monitoring.* Since the path loss between the spoofer and target receiver is highly variable, it is difficult for a spoofer to estimate the transmit power required to resemble authentic signal strength of the authentic GNSS signal at the target receiver [10]. The maximum received power of the GPS signal at earth devices is around -153 dBW at the L1 frequency [11]. Therefore, reception of a spoofing signal whose absolute power is considerably higher than the expected authentic GNSS signal power is a simple technique of detecting a spoofing attack.

3. *Received power variations vs Receiver movement.* Based on the free space square law of propagation, the received power of a free space propagating signal is proportional to the inverse of the squared propagation distance. GNSS satellites are around 20000 kilometres away from the earth surface. Therefore, if the receiver moves on the earth surface in low multipath environments, no considerable change in the received power from authentic satellites should be observed. However, the spoofing signal is usually transmitted from a single directional antenna located much closer to the receiver compared to the GNSS satellites. Therefore, the movement of the receiver relative to the spoofer antenna can considerably change the received C/N_0 from spoofing signals.

4. *L1/L2 power level comparisons.* There is a predefined power level difference between GNSS signals in different frequency bands [10] and many GNSS receivers are able to monitor both L1 and L2 signals. Therefore, a large difference between L1 and L2 power levels can reveal the presence of a spoofing signal. This method can successfully detect the single-band spoofers.

Based on spatial processing

1. *Multiantenna spoofing discrimination.* In [2] a spoofing detection technique is proposed which observes the phase difference between two fixed

antennas. Knowing the orientation of the antenna array and the satellites movement trajectory, the theoretical phase differences can be calculated and compared to the phase difference observed by the antenna array to discriminate the spoofing threat. The main drawback of the algorithm is that it takes a long time to discriminate the spoofing signals. In addition, this technique requires a calibrated antenna array with known array orientation in order to operate properly. The proposed algorithm belongs to this antispoofing technique.

2. *Synthetic array spoofing discrimination.* In [12] a spoofing detection technique that employs a synthetic antenna array has been proposed. In this scenario a single-antenna handheld GNSS receiver is moved along a random trajectory and forms a synthetic antenna array structure. The received signals amplitude and phase corresponding to different PRN signals are continually compared to each other using a correlation coefficient metric (ϱ_{ij}).

Based on TOA discrimination

1. *PRN code and data bit latency.* In case that the receiver-based spoofer does not have any prior information regarding the navigation data bits, it should first decode the received GNSS signals and then generate a processed replica as the spoofing signal. Hence, an unavoidable delay exists between the spoofing data bit boundaries with respect to the authentic ones [4],[13],[14]. Therefore, analysing at which time instants the data bit transition happens, a spoofing attack might be detected. This technique encounters some limitations because the GNSS data frame structure is already known and it consists of different parts with different update frequencies. The update frequency of most parts of the GNSS frame is very low. Therefore, the majority of the GNSS data bits can be predicted by the spoofer if it has already acquired the GNSS information.

2. *L1/L2 signals relative delay.* GPS satellites transmit encrypted P(Y) codes on both L1 and L2 frequencies. The signals received on these two frequencies have a relative delay/attenuation that is caused by the different frequency response of the ionosphere. Therefore, if a dual frequency GNSS receiver correlates the L1 and L2 signals, it should observe only one correlation peak [10]. The propagation delay in L2 is larger than the L1 frequency, therefore the relative delay of correlation peaks is already known to the GNSS receiver. The spoofer should be

able to generate signals on both frequencies in order to defeat this countermeasure.

Based on Signal Quality Monitoring (SQM)

SQM techniques have been employed to monitor the GNSS correlation peak quality in multipath fading environments [15]. Spoofing attacks on a tracking receiver can affect the correlator output in a way similar to multipath effect [16]. Therefore, authors of [9], [17], [18] have extended the SQM techniques to detect the spoofing attack on tracking receivers that are working in line-of-sight (LOS) condition. They have employed the ratio and delta SQM tests in order to detect any strange asymmetry and/or flatness of GPS correlation peaks that is generated by the spoofing attack. It is assumed that the receiver has initially locked onto the authentic correlation peaks and a spoofing attack tries to deceive the receiver to track its fake correlation peaks. The SQM antispoofing techniques are powerful methods to detect the spoofing attack especially in the LOS propagation environments. However, in the presence of multipath, the SQM method might not be able to discriminate between spoofing signals and multipath reflections.

4.3 Algorithm design

4.3.1 Environment description

The algorithm is based on single difference carrier phase (SDCP) $\Delta\Phi_m^{1,2}$ between the two antennas of the receiver where one is considered as the reference of East, North, Up (ENU) local coordinate system. As shown in Fig.4.2, a represents the vector between reference antenna and the second antenna, and c_m is the vector between the mth satellite and reference antenna. $\theta_m(t)$ and $\Psi_m(t)$ are, respectively, the elevation and azimuth angles of the mth satellite, while θ_a and Ψ_a are the elevation and azimuth angles of the second antenna with respect to the reference antenna. As you can see from Fig.4.2, the magnitude of $\Delta\rho_m^{1,2}(t)$ is a function of the distance between the two antennas, d, and the azimuth and elevation angles of incident signals with respect to the antenna baseline.

To compute the vector c_m is necessary to know the satellite ephemeris which can be downloaded from the broadcast signal of the satellite if you have the certainty that you are not already being spoofed. Once calculated the satellite position in the Earth-Fixed Earth-Centered (ECEF) coordinate system using the algorithm described in Tab. 4.1 and converted it in ENU local coordinate system, you have all the parameters to perform the algorithm

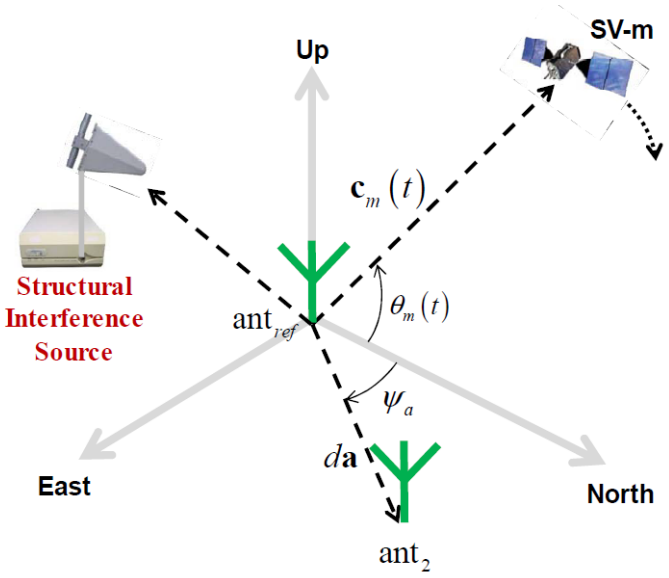


Figure 4.2: Proposed double antenna structure (Fig. from [3])

described in the following section. The ephemeris definition are shown in Tab. 4.2.

Moreover, we suppose that the spoofer has a fix position during the entire attack duration, as the receiver, and can choose a position which around the receiver so the parameter θ_m for the spoofed satellite is set to zero.

4.3.2 Spoofing detection algorithm

Defining $\mathcal{S} = \{\text{satellites in view}\}$ and $\mathcal{F} = \{\text{spoofed satellites}\}$, the algorithm is the following:

1. Compute the matrix $\Delta\Phi^{\mathcal{F}}(p_{\mathcal{F}})$ which has as rows the SDCP of the satellites in view, $\Delta\Phi_m^{1,2}$, observed during a selectable period of time t_o, without noise in ideal conditions.

2. Compute the matrix $\Delta\Phi_e^{\mathcal{F}}(p_{\mathcal{F}}) = \Delta\Phi - \Delta\Phi^{\mathcal{F}}(p_{\mathcal{F}})$ for $\forall\mathcal{F} \subset \mathcal{S}$ where $p_{\mathcal{F}}$ are the parameters of the attack and $\Delta\Phi$ are the matrix composed by the variables $\Delta\Phi_m^{1,2}$ measured by the receiver antennas, so with noise $w_{\Delta\Phi_m^{1,2}}(t)$ which is assumed having constant statistics during the time period t_o.

3. Compute $(\mathcal{F}^*, p^*_{\mathcal{F}}) = \arg\min_{\mathcal{F}\in 2^{\mathcal{S}}\setminus\{0\}, p_{\mathcal{F}}} \|\Delta\Phi_e^{\mathcal{F}}(p_{\mathcal{F}})\|_{\text{F}}^2$ and the corresponding $\|\Delta\Phi_e^{\mathcal{F}^*}(p^*_{\mathcal{F}})\|_{\text{F}}^2$ where $\|\cdot\|_{\text{F}}^2$ represents the squared Frobenius

(1)	$a = (\sqrt{a})^2$	Semimajor axis
(2)	$n = \sqrt{\frac{\mu}{a^3}} + \Delta n$	Corrected mean motion
(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
(6)	$\sin \nu_k = \frac{\sqrt{1-e^2} \sin E_k}{1-e \cos E_k}$ $\cos \nu_k = \frac{\cos E_k - e}{1-e \cos E_k}$	True anomaly
(7)	$\phi_k = \nu_k + \omega$	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)	$r_k = a(1 - e \cos E_k) + \delta r$	Corrected radius
(13)	$i_k = i_0 + (di/dt)t_k + \delta i_k$	Corrected inclination
(14)	$\Omega_k = \Omega_0 + (\dot{\Omega} - \dot{\Omega}_e)(t_k) - \dot{\Omega}_e t_{0e}$	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

Table 4.1: Computation of a satellite's ECEF position vector (Tab. from [11])

t_{0e}	Reference time of ephemeris
$\sqrt{a}$	Squared 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
$\dot{\Omega}$	Rate of change of longitude of the ascending node
Δn	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

Table 4.2: GPS ephemeris data definition (Tab. from [11])

norm (sum of squared entries) of a matrix to find out the most probable spoofed satellites.

4. Compute $\Gamma = \frac{\|\Delta\Phi_e^{\emptyset}\|_{\mathrm{F}}^2 - \|\Delta\Phi_e^{\mathcal{F}^*}(p_{\mathcal{F}}^*)\|_{\mathrm{F}}^2}{\sigma_w}$

5. If $\Gamma > \gamma$, then a spoofing attack is detected and the spoofed satellites belong to $\mathcal{F}^*$. In the opposite case there is no spoofing attack.

The threshold γ is selected to have a good trade-off between false alarm and misdetection probability as it can see on the **Results** chapter.

In step (1) $\Delta\Phi^{\mathcal{F}}(p_{\mathcal{F}})$ is computed as the difference between the two pseudoranges of the two receiver antennas with each satellite. Due to the fact that it is necessary to test all possible configurations of spoofed satellites that are in view, it has to try all possible $2^{\mathcal{S}}$ matrices.

In step (2) $\Delta\Phi_e^{\mathcal{F}}(p_{\mathcal{F}})$ allows to compute the squared error between the ideal results and the received one in a joint operation without any assumption of independence between variables. As a consequence, there is no loss of information.

In step (3) the $\arg\min$ operation computes the most probable set of spoofed satellites in case there is a detection of a spoofing attack with the following operation.

In step (4) there is the Likelihood Test which compares the squared errors of the assumption of no attack and of the most probable set of spoofed satellites normalized with noise variance $\sigma^2_{w_{\Delta\Phi_m^{1,2}}}$. The normalization has been proved by simulation that improves the Likelihood Test performance.

In step (5) the performance of the threshold was tested on all values for different SNRs and then it was chosen the best one considering false alarm and detection probability.

Finally, to test all attack parameters, $p_{\mathcal{F}}$, it will be described later a method to reduce the algorithm execution time.

4.4 Improvements from algorithm in [3]

The algorithm proposed in [3] utilizes as variable the Double Difference Carrier Phase (DDCP), $\nabla\Delta\Phi_{x,y} = \Delta\Phi_x^{1,2} - \Delta\Phi_y^{1,2}$, and exploits the correlation of this measurements to build a graph with satellites as node and the edges are selected if a Generalized Likelihood Ratio Test (GLRT) is greater than a certain threshold.

This approach is not optimal because DDCP measurements are considered independent when they are correlated, so we lose information computing

DDCP from SDCP, and GLRT is used as a hard decision information to build the unweighted graph.

However, this procedure does not need the satellite ephemeris, but in this environment it is more probable the fixed receiver knows its position and can retrieve from other sources the necessary information to derive satellite ephemeris.

Finally, this algorithm is computationally heavier than the proposed one.

Chapter 5

Results

In this chapter it will describe the chosen parameters for the simulations and it will de shown the performance of the proposed algorithm.

5.1 Simulation parameters

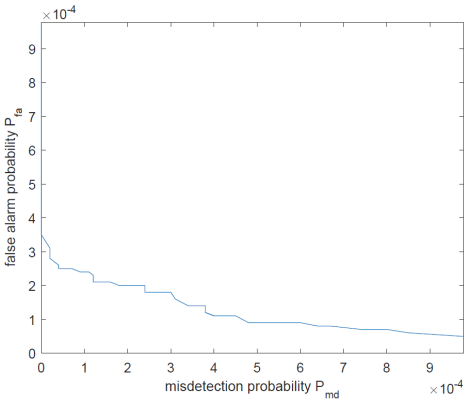
I set the observation time, t_o, to 12 minutes to have a sufficient number of sample to analyse and because in GPS system all data frames are broadcast in 12,5 minutes so the receiver can perform the algorithm in the remaining time with a maximum number of satellites in view of 13.

Moreover, I suppose that the receiver estimates the correct value of the carrier phase cycle ambiguity, N.

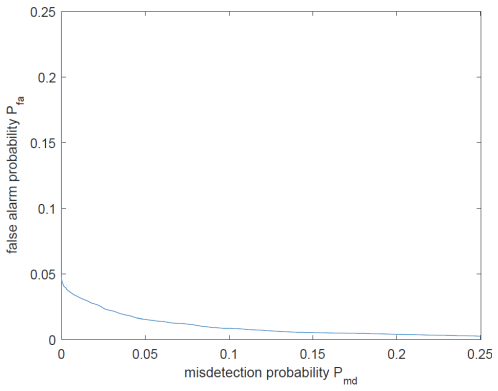
Finally, to test all possible parameters is built a grid of 5x5 with a large resolution to cover all possible spoofer parameter values of Ψ_s and d_s. Then, at each iteration, the grid resolution is shrunk with the following rules:

- It is always halved for Ψ_s variable because the initial values span all 360° with a resolution of 45°;
- It is not halved when the smaller error, $argmin_{(\mathcal{F},p_{\mathcal{F}})} \sum_{i,j} (\Delta\Phi^{\mathcal{F}}_{e\ i,j})^2$, corresponds to one of the two extremes of the grid for the d parameter. If this is the case, then the central value becomes that with the smaller error.

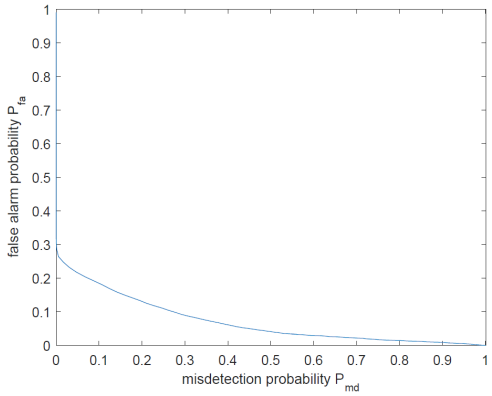
Iterations are stopped when the resolution goes under the variance of the receiver noise, $\sigma^2_{w_{\Delta\Phi^{1,2}_m}}$.



(a) $SNR = -5dB$



(b) $SNR = -10dB$



(c) $SNR = -15dB$

Figure 5.1: False alarm and misdetection probability at different SNR

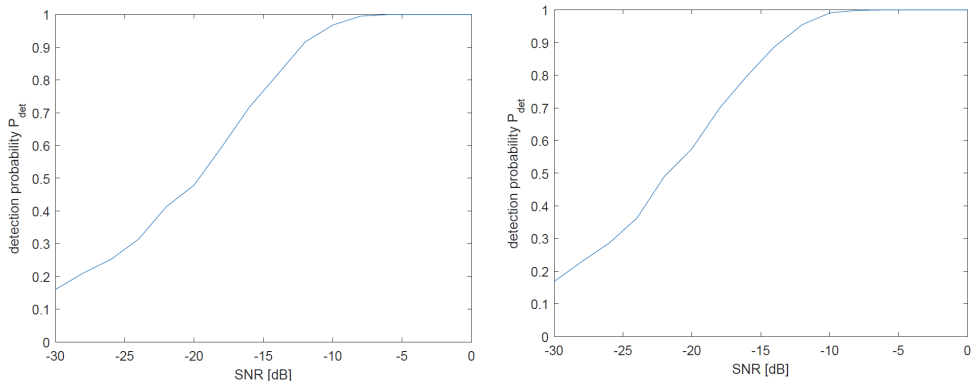
5.2 False alarm vs Misdetection probability

From Fig.5.1 we can see that the algorithm has good performance because at low SNR, with an acceptance of small false alarm probability ($3.5 \cdot 10^{-4}$ for $SNR = -5dB$, $4.3 \cdot 10^{-2}$ for $SNR = -10dB$, 0.28 for $SNR = -15dB$), there is the certainty of the spoofing attack detection. I have also tested higher SNR but the algorithm does not yield any false alarm probability or misdetection event. However, this does not mean that a spoofing attack is always detected with no false alarm probability but we can affirm that the false alarm probability is surely under 10^{-4} due to the fact that I do not run enough iterations to observe lower false alarm probability.

Comparing this results with the algorithm in [3], it can be seen that you can set the false alarm probability as small as the user wants, but the misdetection probability is not null and the obtained results are on collected

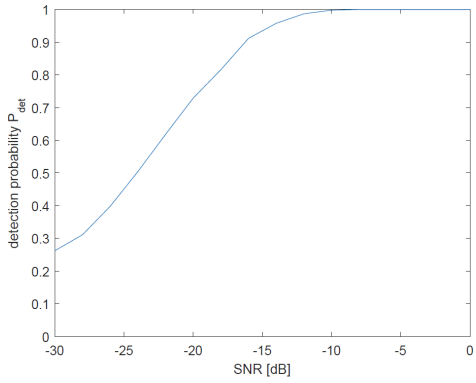
measures in a real environment with good conditions so they does not refer in an environment with low SNR.

5.3 Spoofed satellite identification

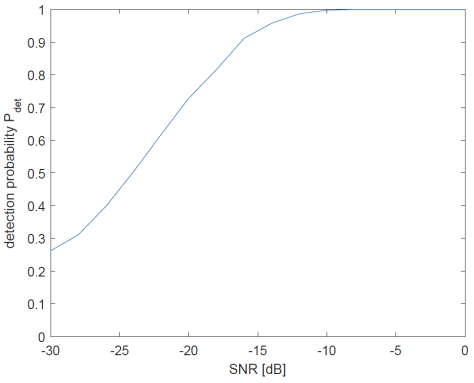


(a) 1 spoofed

(b) 2 spoofed



(c) 3 spoofed



(d) 4 (all) spoofed

Figure 5.2: Mean value of detection probability for different spoofed satellites

From Fig.5.2, after the detection of a spoofing attack, we can see that the correct set identification of the spoofed satellites can be considered correct until the $SNR = -8dB$. At lower SNR the probability of identifying correct spoofed satellites goes down.

However, considering the GPS system design, with a commercial GPS receiver the SNR is between 22 and 29 dB [11] and at this SNR values the proposed algorithm has very good performance.

Comparing this results with the algorithm in [3], it can be seen that the set identification of spoofed satellites has a non-negligible misdetection

probability in a real environment with good condition and it is not tested with low SNR, so in the same condition the proposed algorithm outperforms the one in [3].

Chapter 6

Conclusions

Spoofing attack on GNSS receivers has been considered as a serious threat to mobile phone network synchronisation problem since it uses the GNSS system to synchronize the network. As a consequence, a correct GNSS solution is necessary to have the certainty that the mobile phone network works properly. In this thesis a scenario of a fixed spoofer with a single antenna and a fixed receiver with multiple antennas is considered and an improved version of the algorithm proposed in [3] is tested.

The proposed algorithm performance are very good because, with an acceptance of low false alarm probability, there is the certainty of detecting a spoofing attack and for $SNR > -8dB$ spoofed satellites are surely identified.

However, the proposed algorithm needs to know the receiver position and to initially be certain to not be under attack to correctly receive the satellite ephemeris or to be connected to internet to recover them, which is not a rare situation as in the case of mobile phone network.

Bibliography

[1] X. J. Cheng, K. J. Cao, J. N. Xu, and B. Li, "Analysis on forgery patterns for GPS civil spoofing signals,? in Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09), pp. 353-356, Seoul, Korea, November 2009.

[2] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer", in Proceedings of the Institute of Navigation-International Technical Meeting (ITM '09), pp. 124-130, Anaheim, Calif, USA, January 2009.

[3] Ali Jafarnia Jahromi, Ali Broumandan, Gérard Lachapelle, "GNSS Signal Authenticity Verification Using Carrier Phase Measurements with Multiple Receivers", Position, Location and Navigation (PLAN) Group Geomatics Engineering Department, University of Calgary Calgary, Canada, 2016 IEEE.

[4] T. E.Humphreys, B.M. Ledvina,M. L. Psiaki, B.W. O?Hanlon, and P.M. Kintner, "Assessing the spoofing threat: development of a portable gps civilian spoofer", in Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '08), pp. 2314-2325, Savannah, Ga, USA, September 2008.

[5] Walker, J. G., "Satellite Constellations", *Journal of the British Interplanetary Society*, Vol. 37, 1984, pp. 559-572

[6] Ward, P.,"GPS Receiver Search Techniques", *Proc. of IEEE PLANS '96*, Atlanta, GA, April 1996

[7] P. Misra, and P. Enge "Global Positioning System: Signals, Measurments, and Performance", Ganga-Jamuna Press, 2nd Edition, 2006.

[8] Klobuchar, J. A. (1996). Global Positioning System: Theory and Applications, Volume I, Chapter 12: Ionospheric Effects in GPS, pages 485-515. American Institute of Aeronautics and Astronautics, Inc.

[9] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers", in Proceedings of the Institute of Navigation-International Technical Meeting (ITM '10), pp. 698-712, San Diego, Calif, USA, January 2010.

[10] H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing", in Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS '05), pp. 1285-1290, Long Beach, Calif, USA, September 2005.

[11] E. D. Kaplan and C. J. Hegarty, "Understanding GPS Principles and Applications", Artech House, Boston, Mass, USA, 2nd edition 2006.

[12] J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing detection and mitigation with a moving handheld receiver", GPS World, vol. 21, no. 9, pp. 27-33, 2010.

[13] S. C. Lo and P. K. Enge, "Authenticating aviation augmentation system broadcasts", in Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS '10), pp. 708-717, IndianWells, Calif, USA, May 2010.

[14] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal Authentication, a secure civil GNSS for today", GNSS magazine, pp. 30-39, 2009.

[15] R. E. Phelts, "Multicorrelator techniques for robust mitigation of threats to GPS signal quality" [Ph.D. thesis], Standford University, Palo Alto, Calif, USA, 2001.

[16] D. Shepard and T. Humphreys, "Characterization of receiver response to a spoofing attack", in Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS '11), p. 2608, Portland, Ore, USA, September 2011.

[17] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level", in Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European

Workshop on GNSS Signals and Signal Processing (NAVITEC '10), pp. 1-6, December 2010.

[18] A. Cavaleri, M. Pini, L. Lo Presti, and M. Fantino, "Signal quality monitoring applied to spoofing detection", in Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS '11), Portland, Ore, USA, September 2011.