© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Multi-test Detection and Protection Algorithm Against Spoofing Attacks on GNSS Receivers

Aleksandar Jovanovic
Electronics and Signal Processing Laboratory (ESPLAB)
Ecolé Polytecnique Fédérale de Lausanne
Lausanne, Switzerland
aleksandar.jovanovic@epfl.ch

Cyril Botteron, Pierre-Andre Fariné
Electronics and Signal Processing Laboratory (ESPLAB)
Ecolé Polytecnique Fédérale de Lausanne
Lausanne, Switzerland
cyril.botteron@eplf.ch, pierre-andre.farine@epfl.ch

***Abstract*— The vulnerability against interference, spoofing, and jamming of GNSS receivers is considered nowadays a major security concern. This security threat is exacerbated with the existing market availability of GPS jamming and spoofing equipment sold at reasonable prices. If jamming is the main issue faced at present, spoofing, which allows hijacking someone from the expected path, may lead to even worse consequences. Even with the latest security measures that are going to be deployed on the Galileo PRS signals, GNSS receivers are prone to attacks that are relatively easy to implement. In this paper, we identify different countermeasures and security schemes that can be used against spoofing attacks. These countermeasures include some modifications on the GNSS receiver's side, rather than requiring modifications of the whole existing GNSS infrastructure. More specifically, we propose a detection and protection scheme consisting of several statistical tests, based on the computations of moving variances of Doppler offset and C/No estimates, together with a consistency test of the PVT computation. We evaluate the performance of the proposed scheme through simulations and using a measurement setup consisting of a Spirent GSS8000 full constellation simulator whose output is combined with the one from a rooftop GPS antenna before being fed to a receiver front-end. Finally, we compute the probability of detection and false alarm in spoofing detection using the proposed scheme.**

Keywords—Vulnerability, spoofing attacks, countermeasures, GPS, Galileo, statistical tests, detection, protection, security.

I. INTRODUCTION

The second generation of GNSS (Global Navigation Satellite Systems) is almost upon us, with GPS L1-C getting ready to be deployed and Galileo just on the horizon. Although they bring more advanced signaling features, such as more power, pilot channels, and advanced multipath mitigation, OS (Open Service) Galileo and GPS signals can also be the target of various types of attacks: jamming, spoofing and meaconing attacks, as initially described in [1].Therefore, it is becoming crucially important to find a way to protect these GNSS signals.

A spoofing attack differs from a jamming one in the sense that the objective of the former is just to make the GNSS receiver stop working while the latter is to fool the receiver into thinking it is in a different (false) position. This position could be a few meters off or it could be hundreds of miles off. Therefore, even more than jamming, spoofing is an incredibly dangerous and threatening form of attack. As an example, a spoofer could be used to broadcast a false location to a GNSS receiver in a truck carrying a load of dangerous weapons. The spoofer would make the receiver report that it was still on track, when in fact the truck could have been stopped and stolen. By the time this is detected, it might be too late [2].

Spoofing signals can be generated by satellite simulators that are available today on the market. Typically, the received power of the spoofing signal should exceed that of the legitimate signal. The receiver then operates with the forged signal as input and computes the location induced by the spoofer. Based on a sophistication of the performed spoofing attack, three different types of attack can be identified:

- *Signal synthesizer type*: A class of unsophisticated spoofer that blindly transmits forged synthesized satellite signals, without targeting specific GNSS receivers. For example, it could produce the navigation solution it wishes to impose, roughly estimating the positions of the satellite constellation, and then transmitting forged signals towards the GNSS receivers [3].
- *Meaconing or replay type:* Alternatively, spoofed signals can be generated based on previously received GNSS signals: the adversary records navigation messages and retransmits them [1].
- *Smart spoofer type:* the spoofer first estimates the GNSS signal parameters in real-time based on the previously received signals, and transmits the newly synthesized signals towards the GNSS receiver target.

The essence of the attacks against commercial GNSS receivers lies in the fact that the PRN codes of the satellites are publicly known. This allows an adversary to construct and transmit GNSS signals identical to those sent by a satellite. The objective of the adversary is then be to forge the navigation messages, transmit them over an area, and this way manipulate the PVT solutions of the GNSS receivers in this area [3]. Nonetheless, the adversary should first force its victim GNSS receivers to lose their lock on legitimate GNSS signals and then re-lock on the adversary's forged. To mount such an attack, the adversary should act essentially in two steps. First, it should jam the GNSS signals, to force GNSS receivers to lose lock with the satellites, and then start transmitting its forged messages. The adversary could mount the second and essential stage of its attack even without forcing receivers to lose their lock to GNSS signals. This would be possible when there are

978-1-4799-3320-4/14/$31.00 © 2014 IEEE

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

gaps in GNSS coverage, that is, areas where GNSS receiver cannot lock onto more than three satellites. This may occur often in urban environments and in general due to obstacles that cause loss of GNSS signals.

Signal synthesizer spoofing attacks have the lowest level of sophistication. Bogus signals are generated and then broadcast towards GNSS receivers inducing confusion about exact position and time. This is performed by simply mounting a GPS antenna to a GNSS signal simulator and broadcasting newly synthesized signals towards GNSS receiver, as shown in [3]. Most GNSS signal simulators are heavy and expensive. If used in this simplest attack mode, by synthesizing the GNSS signal without trying to match the exact satellite constellation and signal's parameters, this unsophisticated type of attack can be easily detected. This is because of the difficulty of synchronizing a simulator's output with the actual GNSS signals in its vicinity. An unsophisticated attack effectively acts like signal jamming, and may cause the victim GNSS receiver to lose lock and perform a partial or complete reacquisition. This can be a clear sign of undergoing a spoofing attack. If the unsophisticated attack somehow avoids causing a loss of lock, it will nonetheless likely cause an abrupt change in the victim receiver's GPS time estimate. Jumps in the GNSS receiver clock is also a clear sign of an underlying spoofing attack, as discussed in [4]. In summary, the ease of mounting such an unsophisticated attack via GPS signal simulator makes this attack mode relatively likely. Moreover, detecting such an attack can be also easily performed, using countermeasures based on GNSS signal's statistics that are explained in section III.

The replay or meaconing attack type is based on receiving the GNSS signal and replying it with some delay. Even if the cryptographic protection of GNSS signals exists, it is still possible for an adversary to manipulate the receiver's PVT solution, as shown in [5]. The adversary can receive legitimate GNSS signals, record them, and transmit them at a later point in time and at a different point in space. This is possible because, essentially, cryptography ensures the authenticity and integrity of messages but cannot ensure signal authenticity: a message can be retransmitted by any radio other than the one of the message originator.

Smart spoofing attack is a group of adversarial attacks that is usually targeted to individual GNSS receivers, and aims to transmit signals with characteristics similar to real satellites. One of the challenges that must be overcome to carry out such attacks successfully is to know the exact position and velocity of the target GNSS receiver antenna. This knowledge is required to precisely position the adversarial signals (code offset, code and carrier Doppler, etc.) relative to the genuine GNSS signals at the target antenna. The smart spoofer needs to use directive transmitter antennas to be able to mimic the real satellites and spoof multiple GNSS receivers. Therefore, this attack requires all of the challenges of mounting a single GNSS receiver-spoofer attack, with the additional expense of multiple receiver-spoofers and the additional complexity that the perturbations to the incoming signals must be phase coordinated. One known defense against such an attack is cryptographic authentication [4]. Overall, a smart spoofing attack via multiple phase-locked portable GNSS receiver-spoofers is somewhat less likely than an attack via a single portable receiver-spoofer, but may be very difficult to detect with user-equipment-based spoofing defenses. However, a target receiver equipped with a stable reference oscillator and a low-drift IMU (Inertial Measurement Unit) could resist an attack via receiver-spoofer for several hours. In this paper, we do not address a smart spoofing adversary, for the explained reasons. We further investigate the spoofing defense using countermeasures that can provide protection against unsophisticated and replay attacks, after presenting the state-of-the-art in the spoofing protection.

II. State-of-The-Art in Spoofing Protection

Prevention of intentional spoofing attacks is a requirement for reliable GNSS signaling. Next-generation GNSS (GPS III and Galileo) will provide various levels of authenticated signaling and message data integrity to civil receivers. Of the four projected European Galileo services, Safety of Life (SOL) will control access to integrity data through encryption, while Public Regulated Services (PRS) and Commercial Services (CS) will control access to the signals themselves through encrypted ranging codes and navigation data messages. On the other hand, Galileo Open Services (OS) as well as existing GPS civil signals do not provide authenticated signaling, and rely on anomaly detection techniques to identify spoofing. These methods have varying levels of success, depending on the sophistication of spoofing and detection capabilities. Data communications are also unauthenticated and do not provide cryptographic integrity protection, allowing spoofing and simulation of data messages. Further on, we list the spoofing protection schemes that have been proposed until now, and discuss their detection success level.

Many protection solutions against spoofing of GNSS receivers have been proposed in the last decade on that front [3] [4] [5] [6] [7] [8] [9] [10] [11]. The purpose of security protection techniques is based on providing the integrity of transmitted data and also the authenticity of the transmitter (satellites). There are clearly two types of signal protection that can be used: cryptographic and non-cryptographic protection. Cryptographic protection of GNSS signaling can be achieved by using data encryption, using either a symmetric or asymmetric cryptography scheme. By digitally signing broadcast satellite messages, the authentication of GNSS signals can be provided, and also serve as protection against spoofing attacks. The GNSS receiver simply discards the navigation messages whose signature cannot be verified using the satellite's well-known public key. Any kind of spoofing attack will be hard to implement unless the private key of the satellite is known. Unfortunately, this kind of protection is not immune against replay attacks [5]. Since the arrival times of GNSS signals are important in pseudorange measurements in order to obtain an accurate PVT solution, replay attack will cause erroneous solution even for cryptographically protected GNSS messages.

A similar solution for GNSS signal protection that is rather complex, but could provide a high protection level for GNSS receivers is described in [5] and [6]. The concept is based on dividing the GNSS navigation message in two parts, one that is DSSS modulated by secret spreading codes (SSC), and the

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

other that describes the first one and carries navigation data. The first part of the message transmits information about the arrival time of GNSS signals, and the second part provides information that describes the first part. Using both, the GNSS receiver is able to calculate its position and clock offset in a way that is immune against attacks. By introducing the first part of the message that provides information about the propagation time to the receiver, and by detaching this coded message from the navigation message, more efficient and secure communication can be provided. The first message represents the coded part of the message, using the PRN code that is not known to GNSS receivers a priori. Therefore, the attacker is not able to demodulate and decode GNSS signal without the second message. This method can be applied without the need to distribute and share any long-term secret keys. There is no information available to any GNSS receiver that would enable it to attack others. The time difference between the two signals should be long enough, so that an adversary cannot generate bogus GNSS signals or replay them before the arrival of the navigation message. In the moment of the navigation message's arrival, both the attacker and the GNSS receiver are able to generate the signal that the satellite broadcast some time earlier and to detect the exact time of arrival of signal. The proposed protection scheme can provide a high security level for GNSS receivers, but the disadvantage is that it requires the modification of the existing GNSS in order to support the different navigation message structure and it requires highly synchronized receiver's clocks. Note that a solution that does not require modifications of the existing system, and is also based on the navigation messages authentication is proposed in [7].

Non-cryptographic protection usually stands for more advanced correlation architectures and advanced tracking algorithms for providing security to GNSS signaling. Another GNSS spoofing protection method that falls into the group of advanced tracking architectures for spoofing protection is based on the estimation of signal tracking parameters [8]. It uses multipath estimation techniques for spoofing detection, based on complex statistical detection tests that are computationally and implementation-wise demanding.

A spoofing protection based on cross-correlation of unknown encrypted signals with the existing GNSS signals is proposed in [9]. The solution that is proposed is based on hypothesis testing theory, and develops a codeless cross-correlation detection method for use in narrow-band civilian GNSS receivers. It was shown that, by using the encrypted military GPS P(Y) signal, successful spoofing detection can be achieved. The high cross-correlation statistics mean that both signals are present in the GNSS receiver, and there is no spoofing. If the statistics is low, a spoofing alert is issued. One drawback of this technique is the spoofing detection threshold dependence on the encrypted and received signal power, and for reaching a low false alarm probability, the correlation accumulation intervals should be long.

A straightforward spoofing detection technique based on signal power measurements was proposed in [10] and it was shown to be effective for verifying the authenticity of the received GNSS signals in urban multipath environments, if the spoofer signal power is abnormally higher than that of the authentic signal when the receiver is in the proximity of the standoff spoofer. A suboptimal detector was proposed and a statistical analysis was performed to assess the performance of the proposed technique. If the average spoofer and authentic signal power is known then the detection of spoofing attack is trivial. However, if is completely unknown then it has a finite optimum, that is, a function of and the type of propagation environment detected by the receiver [11] in which an expression for computing the optimum was deduced and applied to various channels.

The first step to ensure that the GNSS receiver is locked to a legitimate satellite signal is to perform a consistency check (PVT solution, frequency and code phase). An example is the RAIM (Receiver Autonomous Integrity Monitoring) concept that is a well-known defense against faulty pseudorange measurements [12]. Detecting any mismatch in pseudoranges and PVT observable could happen due to an adversary trying to deceive the GNSS receiver, or due to the bad satellite data. Consistency checking provides the statistical tests for detection and exclusion of a single faulty pseudorange measurement. Consequently this only provides a single level of protection based on pseudorange tests. In case an alarm is raised, the GNSS receiver should enter the alert mode, where a number of additional consistency checks should be performed. Monitoring the signal quality can be performed by using multiple correlators to detect anomalies and asymmetries of the autocorrelation peak. Monitoring correlation pairs can track the autocorrelation peak independently, with different correlator spacing and independent tracking loops. Then, the autocorrelation peak symmetry test can be performed in the pseudorange domain, as proposed in [13].

In the next section, we describe our GNSS signal protection scheme that relies on a non-cryptographic protection concept, similarly to the aforementioned principles, but more reliable and less complex.

III. Signal Anomalies Detector

We seek to provide a solution that can protect GNSS receivers against the aforementioned spoofing attacks and ensure that they can identify signals that are transmitted by an adversary. The value of the security scheme we propose lies exactly in preventing fraudulent messages from being used and thus from manipulating the PVT solution. The approach we take relies on monitoring the physical properties of the GNSS signals. In fact, the physical characteristics of the GNSS signals provide a set of distinctive features that typically differ significantly from those pertaining to transmissions from adversarial devices. Therefore, we propose an anti-spoofing protection scheme based on monitoring the GNSS signal's features and performing a detection that relies on statistical tests of GNSS signals. The tests are based on C/N_0 time history of all satellite signals and keeping tracks of the C/N_0 estimation over the time. Based on the C/N_0 statistics, we propose a first detection test formed as a Power Threshold Detector (PTD) test. The second test is based on the statistics of the carrier Doppler offset change in the form of a Doppler Offset Detector (DOD) test. Both tests are integrated in the GNSS receiver and perform the spoofer detection based on a RAIM-like principle, as well as using the post-processing

architecture based on adaptive tracking algorithms. Moreover, position and time update consistency tests are performed as well in the form of SCT (Signal Consistency Test).

The received signal analysis is performed on the tracking stage, and the decision about further processing of a GNSS signal is based on predefined thresholds for the PTD and DOD test's statistics and the outcome of the SCT test. The baseband model of the GNSS signal $S_C(t)$ consisting of n legitimate signals and m spoofed signals can be represented as:

$$S_C(t) = \sum_{i=1}^{n} A_i\, d_i(t-\tau_i)c_i(t-\tau_i)e^{j2\pi t f_{d,i}} + \sum_{i=1}^{m} A_{is}\, d_{s,i}(t-\tau_{si})c_i(t-\tau_{si})e^{j2\pi t f_{ds,i}} + \eta(t) \quad (1)$$

where A_i and A_s represent the i-th channel gain for the legitimate and the spoofed signal, respectively. Similarly, d_i and d_s represent the data bits for the legitimate and spoofed signal, τ_i and $\tau_{s,i}$ are the code delays and $f_{d,i}$ and $f_{ds,i}$ are the Doppler frequencies for the i-th channel, corresponding to the legitimate signal and spoofing signal, respectively. $\eta(t)$ represents the Gaussian white noise.

The tests we propose relate to A_i and A_s, as well as $f_{d,i}$ and $f_{ds,i}$. We further describe the concept of each test before showing the performance evaluation in section IV.

A. Power Threshold Detector (PTD)

In the following, we describe the detector based on monitoring the change of a satellite's signal power, which involves monitoring and recording the statistics of the C/N_0. The idea is to estimate the moving variance of the observed signal C/N_0. For the i-th satellite vehicle, we call it $MV_i(W)$, where W is the window size over which the moving variance is computed. This value is monitored for all satellites in range. If the value exceeds some preset thresholds Th_i defined by the GNSS receiver, it should enter the alert mode. This countermeasure is based on the idea that relatively unsophisticated GNSS spoofing attacks will tend to use satellite simulators. Such simulators will typically provide signal strengths many orders of magnitude larger than any possible satellite signal at the Earth's surface, but at least 3 dB above, as has been reported in [14]. In the presence of this test, a main difficulty for the spoofer will be to calibrate the incident signal power at the GNSS receiver antenna, as it is a function of the distance between the spoofer and GNSS receiver and the environmental effects, as well as the antenna gain patterns of both spoofer and GNSS receiver. If the GNSS receiver monitors the signal power level, the only solution for the spoofer to deceive it is to have more transceivers, which receive and transmit GNSS signals to different users with different frequencies and powers. Again, the power level of the signal transmitted from the ground propagates and changes faster, having different statistics comparing to the signals coming from the satellites, that have low variation amplitudes, and therefore those attacks can be only targeted to individual GNSS receivers.

To successfully perform an attack, the adversary has to mask valid GNSS signals and pass the PTD test, which means generating a signal power according to its distance from the GNSS receiver. This confirms that the attack could only individually be directed to specific zones and specific GNSS receivers. If the attacker has the knowledge of the GNSS receiver's position or could track the vehicle in real-time, it could adjust the power such that the signal level at the place of the attacked receiver matches the expected mean power of the signal and deceives it. We identify this attack as the most sophisticated (smart spoofer). In the case of the static attacker and assuming that the power generated by the attacker has to be matched within P_{rx1} and P_{rx2} to defeat the egitimate receiver, the area it can control will be limited by a ring with a radius $R_1 < R < R_2$, where R_1 and R_2 are radii of the circles shown in Figure 1, that can be determined using the free-space propagation model using the minimal and maximal value for P_{rx1} and P_{rx2} (Note that P_{rx2} needs to exceed the true GNSS signals as received at the receiver antenna and $P_{rx1} > P_{rx2}$).

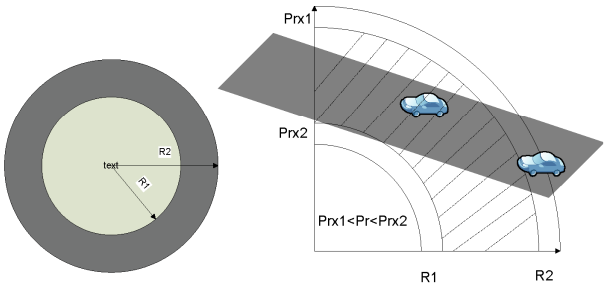

Figure 1 - Limitation of a zone controllable by an adversary based on a power of a signal

In order to define a qualitative expression for the success of the attack under the PTD scenario, we consider the ratio of the surface around the spoofer where the power generated by the spoofer and received by the receiver is within P_{rx1} and P_{rx2}, to the total surface where the spoofer power is at the minimum P_{rx2}. Therefore, if only a PTD test is used without considering the other protection tests, the success of an attack can be estimated as:

$$r = \frac{S_2 - S_1}{S_2} = \frac{R_2^2 - R_1^2}{R_2^2} \quad (2)$$

This ratio can be considered as an upper bound for the attacker's success ratio, if we defined it as the ability of the attacker to control a certain zone and make the GNSS receivers lock onto a spoofed signal. Practically, this ratio depends on the movement pattern of the GNSS receiver. We could therefore conclude that the improvement over the case without a PTD test when the attacker controls the whole zone with the radius R_2 comparing to the case when the controlled zone is limited to the ring marked by radii R_1 and R_2, can be computed as:

$$i = 1 - r = \frac{R_1^2}{R_2^2} \quad (3)$$

As we can observe from Figure 2, where an example of the success ratio r of a spoofer is analyzed, the better the C/N_0 estimation, the more surface area can be limited by the PTD test. R_2 is fixed by the maximal detectable radiated power, whereas R_1 varies, and at the beginning, the attacker success ratio is very high, which corresponds to an attacker able to control the whole area, but as soon as the PTD test is applied,

the surface an attacker can control decreases, and the success rate decreases as well. R_1 is initially set to 4000 m at the distance from the spoofer, but as it increases, the distance between R_1 and R_2 decreases (R_1 becomes $R_1 + x$), and the success ratio decreases as well. This is an illustration of how, by using the PTD test only, it is possible to detect the spoofing attack and decrease the attacker's success rate, but it is clear that it also depends on the exact geometry and the equipment an attacker possess.

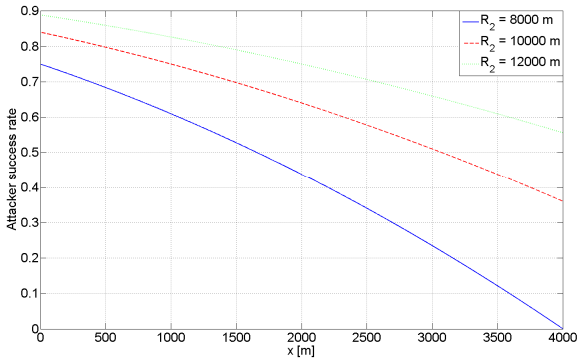

Figure 2 - Attacker success ratio dependence on the surface area bounded by R_1 and R_2

For a mobile GNSS receiver, the attacker success ratio will be even smaller, since there will be some time needed for the GNSS receiver to unlock from the satellite due to jamming, and then lock to the spoofer's broadcasts. Therefore, this analysis may be regarded as providing us with an upper bound for the success of the attack if only PTD is performed.

In order to establish the PTD and define the thresholds to reliably detect the presence of a spoofing signal, the first step is an analysis of the C/N_0 statistics when no adversarial signals are present. Figure 3 shows the C/N_0 computed for tracking seven Galileo E1 signals, and computed during the periods of 400 ms. It can be observed that the variation of the C/N_0 is relatively stable for the majority of the satellites, not exceeding the variation of more than ± 3 dB. This can be better observed by computing the moving variance of the estimated C/N_0 under a window of certain size.

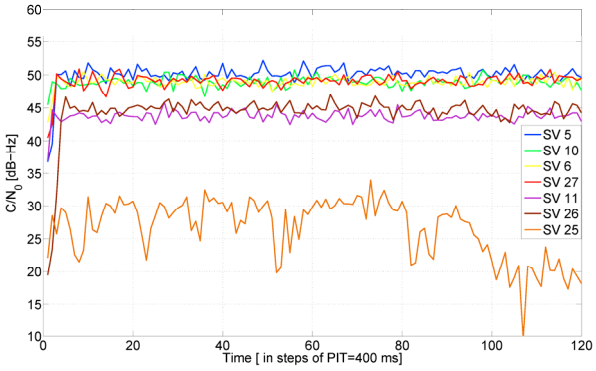

Figure 3 - Estimation graph for C/No for seven satellite vehicles at certain moment of time using computation period of 400 ms

The moving variance is obtained by computing the variance of sets of data and shifting it forward, creating a new subset of numbers, computing consequently a new variance. This process is repeated over the entire data series. New data set consisting of computed variances represents the moving variance. The formula for representing analytically the moving variance is the following [16]:

$$\sigma^2_{MV} = \frac{1}{W}\sum_{k=n-W+1}^{n}\left[x(k) - \overline{x(n)}\right]^2 - \overline{x(n)} = \overline{x^2(n)} - \overline{x(n)} \quad (4)$$

$\overline{x(n)}$ corresponds to the average of the subset values, $\overline{x^2(n)}$ is the sum of the squares over the number of samples in the subset W, and n is the subset number. We used a window of size $W = 100$ (C/N_0 −samples), that corresponds to a time-frame of 400 ms. Any change in the C/N_0 variation is easily detectable using the moving variance principle. This can be observed from Figure 4, where the moving variance for five satellite signals is plotted, as well as for a ground spoofer's signal, generated using the Spirent GSSS8000 simulator. In order to simulate this spoofed signal, we positioned one satellite simulating spoofer very close to the Earth, such that the power variation due to the movement can be clearly detected.

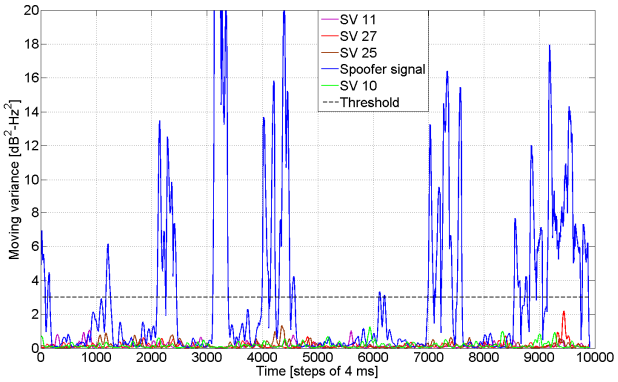

Figure 4 - Moving variance of C/No for five satellite vehicles and a spoofer using variance computation window of 400 ms

Previous papers that were considering estimation of the signal power in order to form the spoofing test were based on the absolute power estimation and its statistics, such as the works presented in [10] and [11]. We took different approach, consisting in the computation of the moving variance of the power estimation that is a metrics much more sensitive on the change between the transition between the legitimate and a spoofing signal. Therefore, its statistics and probability distribution is different as well, as it will be shown later in section VI.

The advantage of the legitimate GNSS satellite signals is that their C/N_0 variation is low, due to the great GNSS receiver-satellite distance. On the contrary, the spoofer is located on the ground close to the GNSS receiver's antenna, and if mobile, variation of the C/N_0 will have different distribution and its moving variance will have high peaks, several orders of magnitude higher than the legitimate satellites. We can observe in this example that, by setting the

threshold for moving variance $MV_{th} = 3\ dB^2 - Hz^2$, spoofing signals could be easily detected and mitigated.

A main problem with the PTD test that may arise is the varying multipath environments, in which case the signal power can vary depending on the multipath pattern superimposed to the GNSS signal. Consequently, the analysis considered here does not assume a severe multipath environment, and considers static and dynamic scenarios with clear LOS between the satellites and GNSS receiver, as well as between the spoofer and the GNSS receiver.

B. Doppler Offset Detector (DOD)

The second spoofing detection test we propose is based on previously received GNSS signal's Doppler offset, that relates to the change in carrier frequency with respect to the nominal transmitter frequency (f_c = 1575.42 MHz). The Doppler shift is produced due to the relative motion of the satellites with respect to the GNSS receiver. The satellite velocity can be computed using ephemeris information and an orbital model available at the receiver [14]. The received frequency, f_r increases as the satellite approaches and decreases as it recedes from the receiver, and it can be approximated by the classical Doppler equation:

$$f_r = f_c\left(1 - \frac{av_r}{c}\right) \tag{5}$$

where f_c is the nominal (transmitted) frequency, f_r the received frequency, v_r the satellite-to-user relative velocity vector, and c the speed of light. The product av_r represents the radial component of the relative velocity vector along the line-of-sight to the satellite. As the GNSS carrier frequency is high and the satellites velocities are large, large Doppler offsets are produced within the range of ± 5 kHz, and vary rapidly. If the oscillator of the GNSS receiver has a frequency shift of ± 5 kHz, the resultant frequency shift may go up to ± 10 kHz. The rate of Doppler offsets' receiving frequency caused by the relative movement between satellite and vehicles is approximately 40 Hz per minute at the maximum for a static GNSS receiver and can be assumed linear [15]. If the receiver is mobile, the Doppler shift variation can be estimated knowing the velocity of the receiver and the direction (altitude).

Interestingly, keeping track of Doppler offsets can indicate the beginning of a spoofing attack, when an adversary is trying to make the GNSS receiver lock onto the false signal. If a DOD test is performed during the tracking, the adversary signals can be eliminated before the navigation message is decoded. For the static GNSS receiver, the Doppler offset can be assumed changing according to a linear model if the receiver's clock is stable. If the Doppler offset for each satellite vehicle SV_i differs more than the statistically-computed thresholds defined a priori in the range $(\Delta f_{min}, \Delta f_{max})$, the GNSS receiver can deem the received signal as the result of an attack. Moreover, the GNSS receiver can still predict the Doppler offset while the GNSS signals are unavailable using the linear prediction model. Once the lock to the GNSS signals is re-established, estimated Doppler offsets

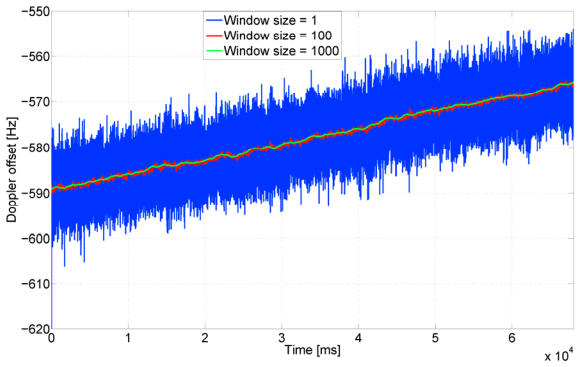

Figure 5 - Moving average of Doppler offset observable for window sizes of 1, 100 and 1000

can be compared to the received ones. If the latter exceeds a threshold, the GNSS signal is deemed adversarial and rejected.

What make this approach attractive are the smooth changes of Doppler offset and the ability to predict it with low, essentially constant errors over long periods of time.

Figure 5 shows the Doppler offset variation when tracking SV 5 using RF samples collected from a Spirent GSS8000 simulator [17] connected to a Fraunhofer front-end [18] and processed in software: the maximum change in rate of Doppler offset is within ± 20 Hz around a linear curve fitted to the data. This shows that with sufficient samples, the Doppler offset rate can be estimated. The example stands for a static GNSS receiver. Using the window of a Doppler offset observable, and computing the moving average over the time window, a lower Doppler offset's variation is achieved along with a smoother transition to the next state, and therefore higher sensitivity can be achieved in Doppler offset change.

The variance across the Doppler offsets in a window of a certain size, so-called moving variance, can provide a detection of any changes in the Doppler offset statistics. Figure 6 shows the moving variance of Doppler offsets for window sizes of 100, 500, and 1000 samples. We can observe that the moving variance does not exceed 30 Hz for a window size greater than 100. Statistical analysis showed that even with smaller window sizes (10 samples), and considering all satellites in view, it does not exceed 40 Hz 90 % of the time. Therefore, setting the threshold for the moving variance to this value as it is done for the PTD test can provide a reliable detection indicator for the onset of a spoofing attack. Moreover, once the alert for the spoofing attack based on the moving variance threshold detector is issued, prediction of Doppler offset based on a linear prediction model can provide the GNSS receiver with approximate Doppler offset to continue tracking.

If a static GNSS receiver scenario is considered, the future Doppler offset samples ($\overline{D(t)}$) can be predicted using the previous n samples of $D(t)$ using the linear prediction model as:

$$\overline{D(t)} = \sum_{i=1}^{n} a_i\, D_{n-1}(t) \tag{6}$$

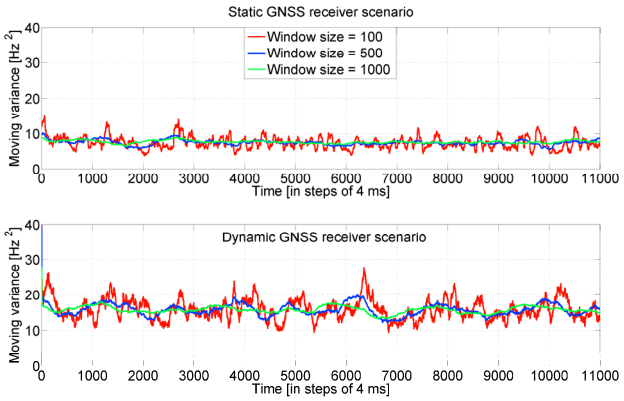

Figure 6 - Moving variance of Doppler offset for different window sizes (100, 500 and 1000) and static and dynamic scenario

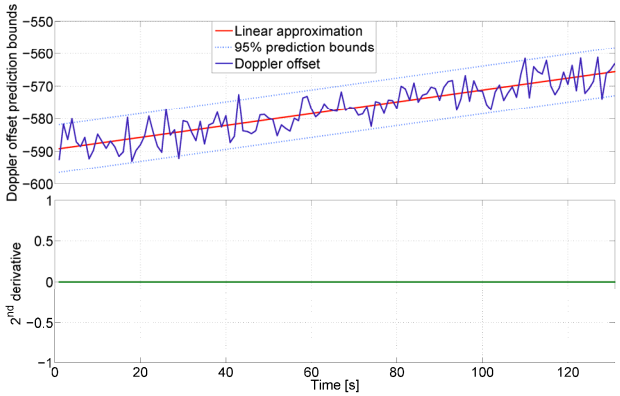

Figure 7 - Doppler offsets prediction based on the linear regression model for the dynamic scenario

The future Doppler offset samples are predicted based on the previous sample history, and are computed as a weighted linear combination of past n samples using the weight a_i. Weights a_i are selected to minimize the mean square error (MSE) between $D(t)$ and $\overline{D(t)}$. The error to minimize e_m is given as:

$$e_m = E\left[\left(D(t) - \overline{D(t)}\right)^2\right] = E[(D(t) - \sum_{i=1}^{n} a_i D_{n-1}(t))]^2 \qquad (7)$$

Solution of this set of equations provides values for coefficients a_i. The obtained equations are Yule - Walker equations, and though there are many efficient algorithms that solve this set of equations, one of them is the algorithm developed by Levinson and Durbin [19]. Note that each satellite has different velocity dynamics and therefore the linear prediction coefficient should be separately computed. Nonetheless, this does not affect the ability of the receiver to distinguish between real and false satellite signals with help of DOD test.

Also, the accuracy of the linear prediction model does not need to be very high, since the Doppler offset mostly depends on satellite velocity (that is in the range of ± [1-5] km/s), and the contribution of the ground receivers is minor. A spoofer would need to match the Doppler offset of every satellite signal, for which he would need multiple antennas, and multiple transmitters (one per channel), if not in possession of complex, expensive, and relatively bulky full constellation simulators that can generate multiple channels at the same time on the same antenna.

The principle of using a linear model for the Doppler offset prediction is shown in Figure 7. Based on the history of Doppler offsets for each satellite, the linear prediction model computes the future estimates of the future Doppler offset. The DOD prediction test therefore consists in performing a comparison of the estimated and upcoming samples of Doppler offset and checking if they are inside the limits estimated with 95 % confidence. If this is fulfilled, the normal operation of the GNSS receiver is performed.

C. GNSS Signal Consistency Tests (SCT)

The need to provide continuous navigation between the update periods for GNSS receivers (which essentially are discrete-time position/time sensors with sampling interval of approx. one second or 10 Hz), has already led to the use of inertial sensors, altimeters, speedometers, odometers to calculate GNSS receiver location [3]. However, the accuracy of such sensors degrades with time, and the cost is high for commercial instantiations of GNSS receivers. Therefore, as an enhancement in spoofing detection already discussed, we propose to use GNSS signal consistency check test, which we group in a single test as SCT. It is based on the consistency in location and time update, ephemeris data and pseudorange rate change, as well as clock offset change.

The cross-checking tests of the GNSS signal observables on which the SCT is relying upon are the following:

- If the reception of GNSS signals is disrupted, the local oscillator switches from normal to holdover mode, with timing accuracy depending on the stability of the local oscillator. The quartz crystals of different clocks might be running at slightly different frequencies, causing the clock values to gradually diverge from each other (skew error). To enable such a scheme, the behavior of quartz clocks is important, and in particular the period during which the receiver can maintain coarse synchronization. A simulation based study [20] of quartz clocks claims that coarse time synchronization can be maintained at microsecond accuracy without GPS reception for 350 s in 95 % of cases. This means that a quartz oscillator can maintain millisecond synchronization for a few hours, including random errors and temperature change induced inaccuracies. If we define limits for the computed minimal and maximal time offsets after establishing the lock again, $\tau_{min} < \tau < \tau_{max}$, it is possible to reject spoofed signals after losing lock with the satellite and again locking by comparing if the time shift τ satisfies the established bounds.

- The received ephemeris data that is used for satellite position computation is compared with previous ephemeris history records, as well as almanac data to ensure that the computed satellite positions are not too far away from the expected position provided by the almanac. The almanac contains approximate positions of the satellites in the specific moment in time. From the almanac, information about the set of available satellites that are expected to be at the sky is given by $\{SV_i\}, i = 1, \dots, n$ (n is the satellite vehicle number). This information is important, since, if the set of satellites that is being searched $\{SV_j\}, j = 1, k$, does not match the former expected set, or the number of observed satellites is less or larger than the number of expected ones ($k < n$ *or* $k > n$), this could be the sign of an attack, and the signals from the spoofer can be detected and eliminated.

- The GNSS receiver should be able to keep track of its location and time information and detect abrupt changes during the navigation, and also any inconsistency detected (such as large offsets in position and time between two update periods). If any of these is detected, the GNSS receiver navigation switches to an alert mode.

- The pseudorange rate, defined as the rate the pseudorange changes in between two update period is constantly checked and monitored. Any abrupt change in the pseudorange rate function can be a sign of the spoofing attack as well.

D. Spoofing Detection and Protection Scheme

As discussed above, the countermeasures we consider here rely on information the GNSS receiver obtained before the onset of an attack, or more precisely, before the suspected onset of an attack, and include:

- SCT test, calculated from GNSS navigation messages,
- PTD test, detecting the variation of GNSS signal power (C/N_0)
- DOD test, based on received GNSS signal Doppler offset measurements.

We propose the integration of a separate and independent module in the GNSS receiver chain, whose role is to perform the proposed statistical tests. This spoofing detection and protection module (SDP) is an integral part of the GNSS receiver after signal the down-conversion of GNSS signal to IF, that have direct access to IF data input stream. The detection and protection scheme relies on the receiver-autonomous monitoring of GNSS signal parameters. The protection scheme based on SDP assumes several protection levels, and is illustrated in Figure 8. It is a complex processing unit, capable of performing the detection tests on the incoming GNSS signals, containing enough memory to keep the history of the GNSS signal's statistics, and able to provide a high probability of detection and protection against spoofing.

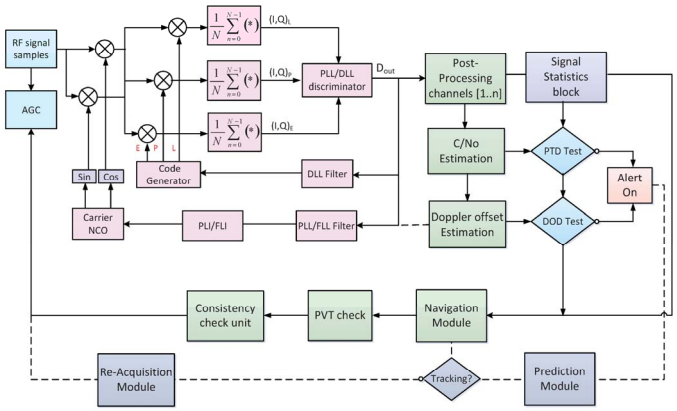

Figure 8 - Spoofing detection and protection (SDP) scheme

The SDP module is integrated in the channel tracking stage, as a part of the adaptive tracking algorithm, as well as navigation and positioning stage. After down-conversion, RF samples are fed into the tracking module, that successfully tracks the existing satellite channels, and provides tracking results to the post-processing block, that keeps tracks of the GNSS signal statistic's history, in order to compare it to the upcoming data, and prompt the decision about further processing. C/N_0 estimation and Doppler offset estimation is performed during the tracking, in order to detect the signals coming from untrusted sources. PTD and DOD tests are then performed, and based on the outcome, if any of the tests causes the alert to turn 'ON', processing immediately switches to protection mode. Protection mode uses statistical data of Doppler offset and GNSS signal power, and performs a further check if the tracking can be continued. This is performed using a prediction module. If tracking cannot be established, processing transits to re-acquisition, where the GNSS receiver prompts to acquire the same GNSS satellites it was tracking before, and establishes the lock again. If both tests are correct, navigation can be normally performed. The consistency check unit shown in Figure 8 is active all the time, performing the abovementioned SCT test.

We further test the proposed detection and protection scheme using a realistic setup described further on, and show its robustness against three types of spoofing attacks.

IV. ATTACK IMPLEMENTATION AND PROTECTION

Different architectures to implement jamming and spoofing attacks are possible. These architectures can be split into two main categories as shown in Figure 9 and described below:

- Adversarial signals are mixed with legitimate signals at GNSS antenna before they are processed (Option I).

- Adversarial signals are mixed with legitimate signals at baseband (Option II).

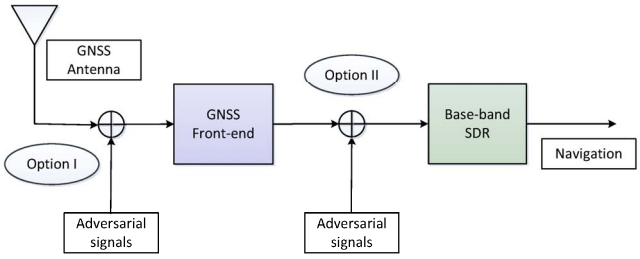

Figure 9 - Two different architectures for attack implementation

The first solution (Option I) is closer to a real world scenario, where both legitimate and adversarial signals pass through each stage of the GNSS receiver. The second solution (Option II) is easier to implement and simulate because it involves only software operations, and the signals are mixed in baseband. The advantage of mixing the signals after the front-end stage is that it allows for starting the simulations with different parameters that are easily configured andthe evaluation of the proposed countermeasures can be performed promptly. The disadvantage is the assumption that the adversarial signals have already passed the front-end stage, including the automatic gain control (AGC). We implemented both solutions for our analysis. However, in the scope of this paper, the results are only shown using Option I that is more realistic.

V. SPOOFING DETECTION AND PROTECTION RESULTS

Several experiments were carried out to show the resistance and reliability of the proposed spoofing protection scheme. The unsophisticated spoofing attacks, such as the ones that do not take into account the exact position and parameters of a GNSS receiver are straightforward to detect and reject. The smart spoofer, as we define it, is a spoofer that has the access to the real-time position of a GNSS receiver under the attack, and is in the vicinity of a GNSS receiver able to transmit GNSS satellite signals that are harder to detect and reject. For the experiments performed here, we assume the implementation of three different types of a smart spoofer that is exclusively based on the replay attack concept:

- Static spoofer, randomly generating and transmitting satellite signals over the air in the area of a GNSS receiver (type I).
- Static spoofer, able to receive and re-transmit in real-time GNSS signals from multiple transmitters, each corresponding to one satellite signal (type II).
- Static smart spoofer, able to receive and transmit in real-time signals from multiple transmitters towards a mobile GNSS receiver in a car moving in an urban area, each corresponding to one satellite signal (type III).

The simulation set-up we use consists of a Spirent GSS8000 simulator [17] that emulates the real satellite constellation, combined with signals coming from our GPS rooftop antenna, emulating the spoofer, in a way that is shown in Figure 10. Tests we perform for spoofing detection are separately shown in a SDP module, that continuously monitors the signal parameters, and based on the outcome of the PTD, DOD and SCT tests, issues an alert and switches to protection mode in case of spoofing detection.

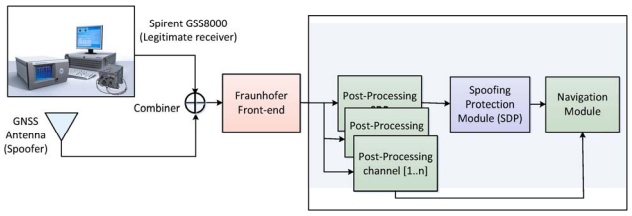

Figure 10 - Spoofing measurement setup including detection and protection unit

The outcomes from the proposed PTD and DOD tests for the Spoofer type I are shown in Figure 11 for satellite SV 14. It is obvious that by performing the two proposed tests, the spoofer of this type can be detected and an alert issued in further processing. DOD test is straightforward, since there is a clear shift in the received Doppler for more than 100 Hz, whereas the PTD test has a lower detection probability, since the power of both signals is similar, as the spoofer tries to match the estimated signal power. In another example, shown in Figure 12, the spoofer tries to match the Doppler of a GNSS receiver, but has higher amplitude variations, which is easily detectable by a PTD test. Based on the thresholds for PTD and DOD tests set to 2 $dB^2 - Hz^2$ and 400 Hz^2 respectively, the attack can be successfully detected and mitigated (in both examples, a window of 10 samples is used for the computation of the moving variance). According to Figure 8, the receiver switches to prediction mode, where the tracking loops are re-initialized to the code delay and carrier offset before the spoofing started. Further protection consists in a comparison of the received and predicted Doppler offset and C/N_0 , based on the GNSS signal tracking history, and deciding about further processing.

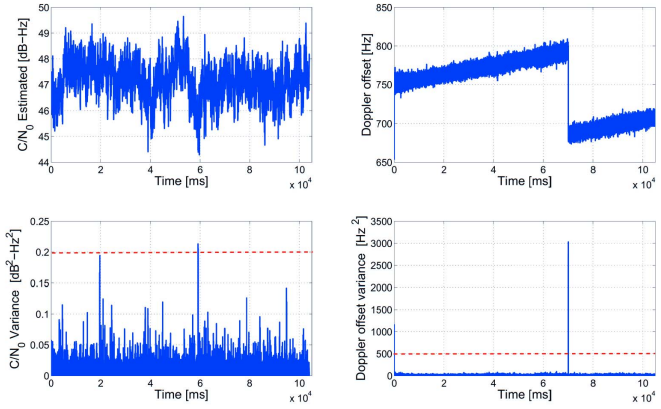

Figure 11 - Detection of spoofing: PTD and DOD tests for Spoofer Type I using window size of W = 10

One of the tests in the SDP scheme shown in Figure 8 in the navigation stage is the SCT test, which consists in keeping

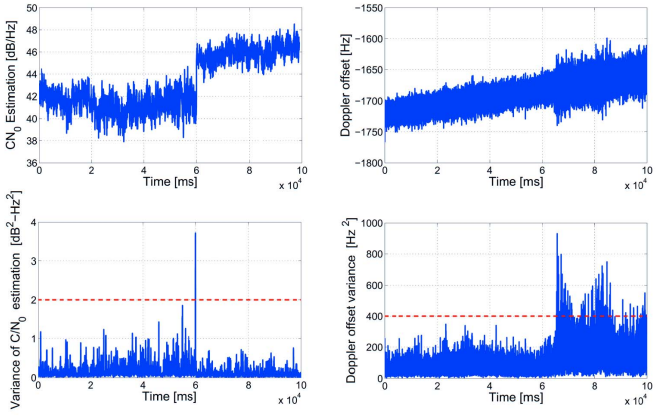

Figure 12 - Detection of spoofing: PTD and DOD tests for Spoofer Type I using window size of W = 10

tracks of the continuous and smooth update of the position, time and pseudorange rate. Any abrupt changes of these that the GNSS receiver detect in real-time can be due to the signals coming from untrustful sources and should be rejected.

Position offset caused by the Spoofer Type I for the previous example is shown in Figure 13. There is an abrupt change in the position update a couple of hundred meters away from the legitimate position, easily detectible by the SCT test.

Figure 13 - Position change of the Spoofer Type I

Depending on the outcome of the DOD, PTD and SCT tests, the GNSS receiver is able to bring the decision about the navigation based on the decision logic shown in Figure 8. It could happen that one of the proposed tests fails, but because of the complexity of the protection scheme the probability of a false alarm for all tests and all satellites used for navigation is very small, as we further show in section VI. Outcomes of the DOD and PTD tests for a spoofer Type II are shown in Figures Figure 14 and Figure 15 for five satellites in view. In this case, it is assumed that the spoofer possesses high-gain antennas, and multiple transmitters (one for each satellite). It is important to notice that the spoofing starts at the same moment for all satellites, and that the spoofing detection is positive for all satellite channels, although there is a difference in detection success of individual channels.

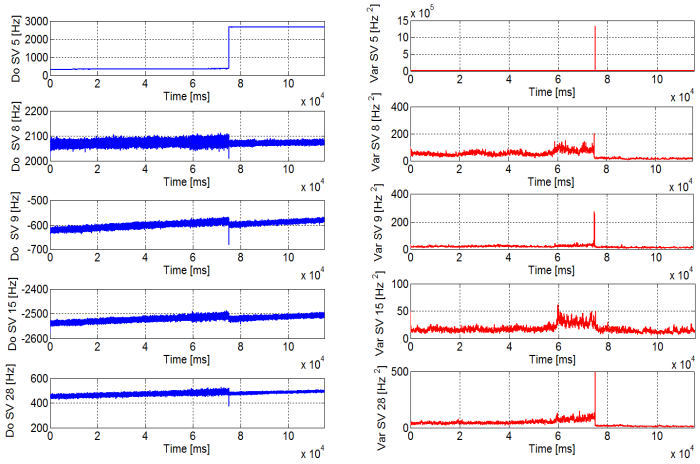

Figure 14 - Detection of spoofing: DOD test and its variance for Spoofer Type II

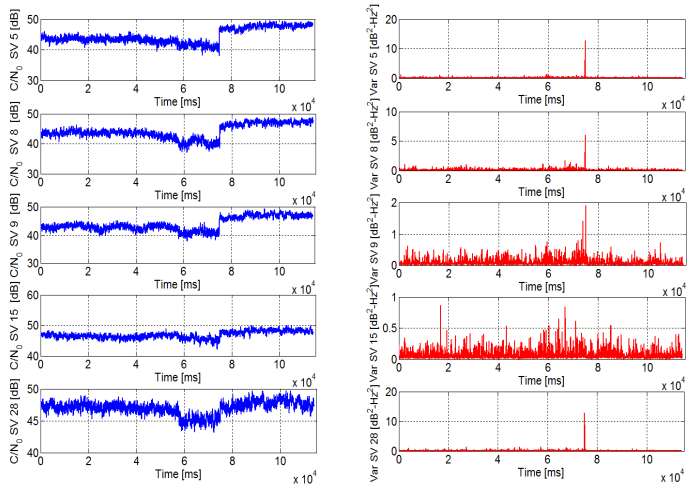

Figure 15 - Detection of spoofing: PTD test and its variance for Spoofer Type II

Finally, the third test with a mobile GNSS spoofer is considered (Type III), where the Doppler offset changes fast, due to the fast-changing velocity and direction change of the GNSS receiver. In this case, a lower window size should be used when computing the moving variance, to that the detection scheme will be more sensitive to change of a signal statistics.

Experimental evaluation showed that a considerable window size in order to achieve good detection is W=10 samples for the mobile scenario, and W=100 samples for the static GNSS receiver. These are the values for the window size that we used here.

The detection ability of the proposed scheme is tested for spoofing a mobile GNSS receiver with a static smart spoofer, located in the area and receiving the signal from the same set of satellites, re-distributing them over the spoofing area where the mobile GNSS receiver is located. In this case, Doppler offset depends on the exact trajectory of a mobile GNSS receiver, and its velocity change.

DOD test outcome for the GNSS mobile receiver moving to a simple rectangular pattern is shown in Figure 16. Although the Doppler offset changes continuously, DOD test was able to detect the spoofing signal, whose moving variance exceeds the threshold as can be seen in the second set in the same figure (staring at time 60 s).

Similar results were obtained using a PSD test, noting that when the attack begins, the usually estimated power drops, and then increases to more than it was before the onset of the attack, as can be observed from Figure 17. Also, if we have a closer look on the trajectory of a mobile receiver, we could notice that it contains high jumps in the estimated position, as can be seen from Figure 18. The red line is a trajectory of the GNSS receiver, and the green trajectory is a trajectory of the GNSS receiver under spoofing. Therefore, it is clear that by using PTD and DOD together with the SCT test, it is possible to detect the spoofer with a high probability, and switch to alert processing mode, based on which outcome further processing is performed.

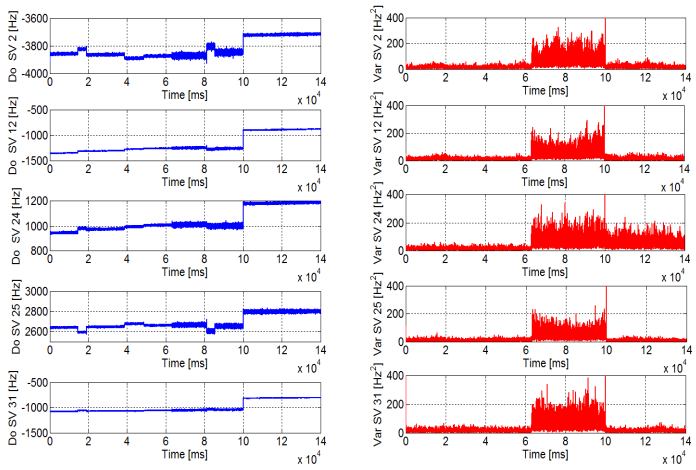

Figure 16 - Detection of spoofing: DOD test and its variance Spoofer Type III

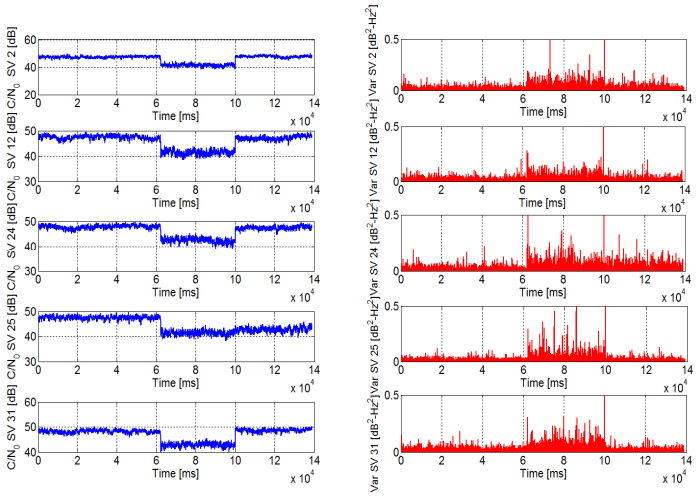

Figure 17 - Detection of spoofing: PTD test and its variance for Spoofer Type III

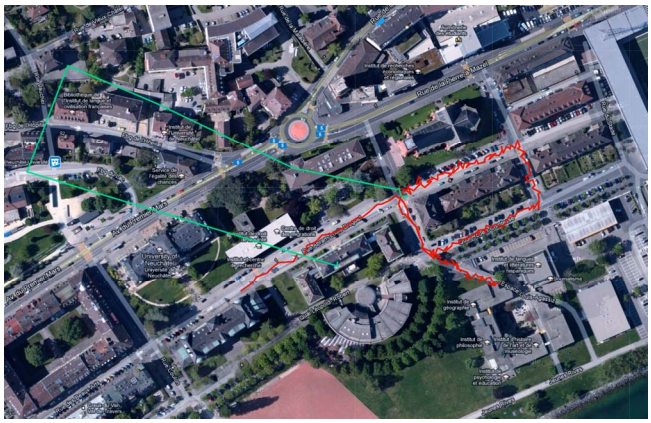

Figure 18 - Position change of the Spoofer Type III

Using this procedure, the spoofer's signals can be successfully detected, and, in a high percentage of cases, mitigated, as it is shown further.

After presenting these results for the proposed tests, and showing that they can be used reliably for the spoofing detection and protection, we further perform a theoretical analysis of the spoofing detection using a probabilistic approach.

VI. Spoofer Protection Reliability

Spoofing detection and protection described and evaluated in the previous sections are based on performing several statistical tests and depending on their outcome, either accepting the received signals for further processing and navigation, or rejecting them, further switching to the recovery procedure. Therefore, the spoofing detection algorithm is based on a comparison of the received Doppler and power with the set of pre-defined thresholds and can be seen as a binary detection problem, deciding between the two hypotheses, the authentic signal hypothesis (H_0), and the spoofing signal hypothesis (H_1), as shown in Figure 19. Note that the thresholds are set based on the authentic signal and the noise statistics as it has been described in [21]. Therefore, the statistics of a spoofer signal are not needed.

As already explained in section III.D, the GNSS receiver is recording the GNSS signal's statistics, especially of the Doppler offset and C/N_0 estimation, and performing the proposed tests on whose basis the detection is performed. The GNSS receiver records N signal samples (n=1,...N) and bounds them to one of the two hypotheses:

$$H_0: x_n = \int_{(n-1)T}^{nT} \left(\sum_{i=1}^{n} A_i \, d_i(t-\tau_i) c_i(t-\tau_i) e^{j2\pi t f_{d,i}} + \eta(t) \right) dt \cong \sum_{i=1}^{n} s_i^a + \xi_a \quad (8)$$

$$H_1: x_n = \int_{(n-1)T}^{nT} \left(\sum_{i=1}^{n} A_{is} \, d_{s,i}(t-\tau_{s,i}) c_i(t-\tau_{s,i}) e^{j2\pi t f_{ds,i}} + \eta(t) \right) dt + \int_{(n-1)T}^{nT} \left(\sum_{i=1}^{n} A_i \, d_i(t-\tau_i) c_i(t-\tau_i) e^{j2\pi t f_{d,i}} + \eta(t) \right) dt \cong \sum_{i=1}^{m} s_i^s + \sum_{i=1}^{n} s_i^a + \xi_s \quad (9)$$

where s_i^a and s_i^s represent authentic and spoofed signals, respectively, and ξ_a, ξ_s are the noise components.

A detection variable $v = C_{th}(y)$, where y represents the moving variance of variable x_n, can be formulated to decide between the two hypotheses, H_0 or H_1, comparing y with the set of pre-defined thresholds $(T_{DOD}, T_{PTD}, T_{SCT})$, related to the DOD, PTD and SCT tests, respectively. A decision based on y can be found from the probability density function (*pdf*) of the moving variance of the proposed tests. Since the hypothesis outcome depends on several tests that have a different probability density function, we assume then can be considered as independent.

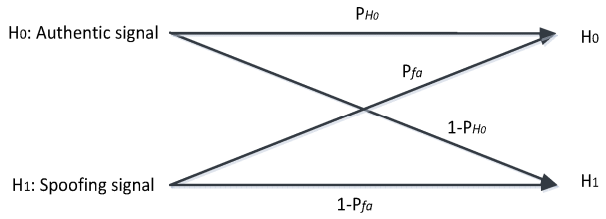

Figure 19 - Binary hypotheses for the authentic and spoofing signal with the corresponding probabilities

Condition C_{th} is the condition that performs the check if the y is smaller than pre-defined threshold for each test:

$$C_{th} = \left((y_{DOD} < T_{DOD}) AND (y_{PTD} < T_{PTD}) AND (y_{SCT} < T_{SCT})\right) \quad (10)$$

The detection variable v is bound to the binary test of H_0 versus H_1 in the following form:

$$v = \begin{cases} 1(H_0), & C_{th}\ is\ true \\ 0(H_1), & C_{th}\ is\ false \end{cases} \quad (11)$$

Therefore, the condition to detect hypothesis H_0 that marks the authentic signal state is to have the detection variable y less than the set of pre-defined thresholds. If any of the conditions from equation (10) is not fulfilled, hypothesis H_0 is declared as false, and the algorithms switches to hypothesis H_1, declaring a spoofing state. Probability of detection P_{H_0} is defined as the probability that detection variable declares the authentic signal state. Probability of misdetection $P_{H_{10}} = 1 - P_{H_0}$ can be computed as the probability that H_0 is declared and the GNSS receiver is in a spoofing state. They can be expressed as:

$$P_{H_0} = P(v = 1|H_0) \quad (12)$$

$$P_{H_{10}} = 1 - P(v = 1|H_0) \quad (13)$$

Probability of error or probability of false alarm can be computed as the probability that the receiver is in a spoofing state, but C_{th} is true and H_0 is accepted:

$$P_{fa} = P(v = 1|H_1) = 1 - F_{v|H_0} = \int_y^{\infty} f_{v|H_0}(y)dy \quad (14)$$

$f_{v|H_0}$ is the *pdf* of each individual test, and $F_{v|H_0}$ the cumulative distribution function. Since the *pdf* of each test might not be the same, in order to compute the probability of error, we have to define the *pdf* of each test, and then compute the final false alarm error probability using equation (14). Assuming that the spoofing detection tests are independent, the final false alarm error probability can be computed as:

$$P_{fa} = P_{fa}^{DOD} \cdot P_{fa}^{PTD} \cdot P_{fa}^{SCT} \quad (15)$$

P_{fa}^{DOD}, P_{fa}^{PTD} and P_{fa}^{SCT} represent the false alarm probabilities for DOD test, PTD test and SCT test, respectively.

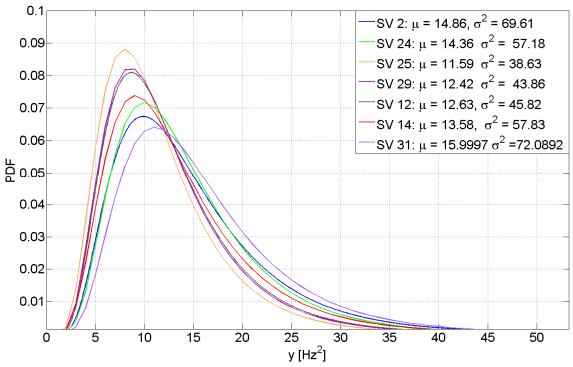

Figure 20 - PDF of Doppler offsets moving variances for Type III example using window size of W=10

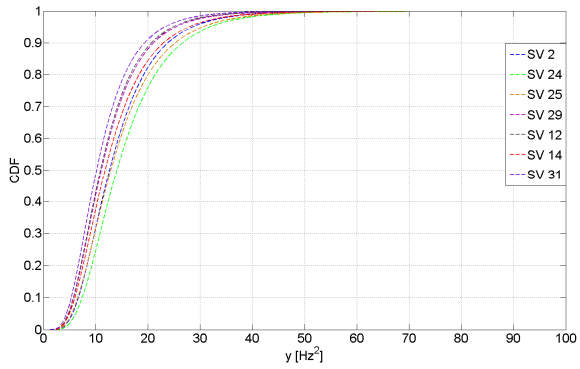

Figure 21 - CDF of Doppler offsets moving variances for Type III example using window size of W=10

pdf and *cdf* (cumulative distribution function) of Doppler offset moving variance for the group of satellites used in the example of Type III, shown in Figure 16 and Figure 17 is shown in Figure 20 and Figure 21, respectively. Distribution of Doppler offset moving variance for a window size of *W*=10 is log-normal, $\mathcal{N}(\mu, \sigma^2)$, therefore expressions for *pdf* and *cdf* can be written as in [19]:

$$pdf(x) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-(\log(x)-\mu)^2/2\sigma^2}$$

$$cdf(x) = \frac{1}{2} + \frac{1}{2} erf\left[\frac{\ln(x)-\mu}{\sqrt{2\sigma^2}}\right] \quad (16)$$

When deciding about the threshold for the moving variance of Doppler offsets, the maximal value of the mean (μ) of the distribution in normal conditions is considered, and the mean during spoofing, as well as the value for the threshold is decided based on criterion that the detection success is higher than 99 %. Considering the satellite set from Type III example, and based on the described computation scheme, the threshold for the Doppler offset moving variance using window size of 10 is T_{DOD}=80 and is taken from Figure 21. For this threshold value, mean false alarm probability is $P_{fa1} = 1 - F_{v|H_0} = 1.6825 \cdot 10^{-4}$.

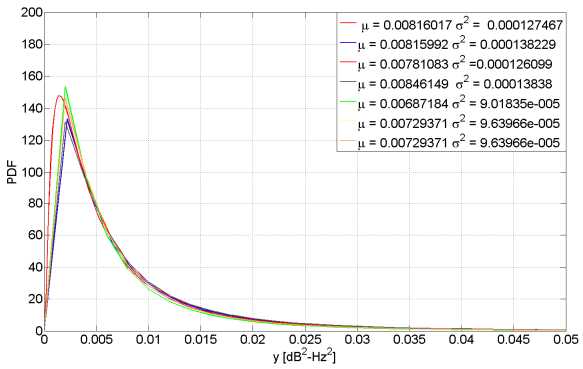

Figure 22 - PDF of C/No moving variances for Type III example using window size of W=100

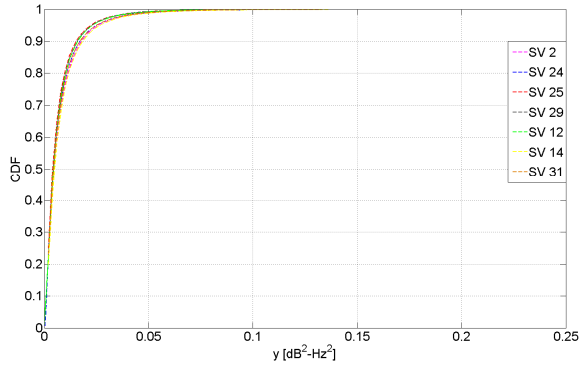

Figure 23 - CDF of C/No moving variances for Type III example using window size of W=100

Variation of C/N_0 when no interference, multipath, or other sources of disturbance are present is also considered in order to decide about the *pdf* and *cdf*, shown in Figure 22 and Figure 23. The distribution of moving variance of C/N_0 estimates is also log-normal, with the corresponding means and variances for this specific case also shown in Figure 22 and Figure 23. *pdf* curves of C/N_0 estimates match the log-normal probability distribution very well, and in a similar way as for the DOD test analysis, we determined the threshold for the PTD test, T_{PTD}= 0.2. The false alarm probability for this threshold is $P_{fa2} = 1 - F_{v|H_0} = 1.3499 \cdot 10^{-4}$.

We can observe that by taking into consideration only DOD and PTD test, the overall mean false alarm probability using equation (15) can be computed. The SCT test probability analysis is not taken into consideration since it is not so easy to estimate its distribution since there are no statistical tests used in this case, and we could not perform a similar analysis as we did for PTD and DOD tests. Taking computed false alarm probabilities for PTD and DOD tests, the overall false alarm probability using only DOD and PTD tests is computed as $P_{fa} = P_{fa1} \cdot P_{fa2} = 2.2713 \cdot 10^{-8}$. As we can observe, this probability is very small, which means that the spoofing detection probability is very high using only PTD and DOD tests.

VII. CONCLUSIONS

In this paper we discussed the vulnerability of the existing GPS and upcoming Galileo navigation system against typical spoofing attacks. It was shown that the replay attack is the most dangerous attack type. We identified and listed many solutions proposed for secure GNSS signaling, the majority of them being based on modification of the existing navigation system, or requiring complex implementations. After that, we proposed a simple solution that relies upon the statistical properties of the received satellite signals, together with an adaptive tracking algorithm concept. More specifically, we proposed a scheme where the statistics of the Doppler frequency offset and C/N_0 are monitored, as well as the consistency in the PVT, ephemeris and pseudorange rate, to detect the presence of a spoofer's signal. The tests we proposed are based on monitoring a moving variance of Doppler offset and estimated C/N_0, which essentially change in the presence of a spoofer, causing abrupt jumps in its statistics for both tests. The protection we proposed integrates the proposed tests in the adaptive tracking scheme in the form of detection and protection module, and is an integral part in the GNSS receiver tracking architecture. We show that by using the Doppler offset and C/N_0 tests, and extremely low probability of a false alarm of spoofing detection can be acheved. Once a spoofing signal is detected, the GNSS receiver switches to protection mode, where the tracking history is further used to predict the future tracking state and re-establish the tracking, or perform the re-acquisition. The proposed scheme was tested for three different spoofer types by simulations, and it was shown that the presence of a spoofer can be successfully detected.

REFERENCES

[1] John A. Volpe, "Vulnerability Assessment of the Transport Infrastructure Relying on the Global Positioning System," National Transportation Systems Center, 2001.

[2] Papadimitratos Panagiotis and Jovanovic Aleksandar, "Protection and Fundamental Vulnerability of Global Navigation Satellite Systems (GNSS)", International Workshop on Satellite and Space Communications (IWSSC), 2008.

[3] Papadimitratos Panos and Jovanovic Aleksandar, "GNSS-based Positioning: Attacks and Countermeasures," IEEE Military Communications Conference (MILCOM), 2008.

[4] Ledvina, M. Brent and Bencze, J. William and Galusha, Brian and Miller, Issac, "An In-Line Spoofing Module for Legacy GPS Receivers," in Proceedings of the US Institute of Navigation International Technical Meeting, 2010, pp. 698-712.

[5] Kuhn, Markus, "An Asymmetric Security Mechanism for Navigation Signals," Proceedings of Sixth Information Hiding Workshop, 2004, pp. 239-252.

[6] Scott, Logan, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation ION GPS/GNSS 2003, p. 1543-1552.

[7] Pozzobon, Oscar, "Keeping the spoofs out: Signal authentication services for future GNSS", Inside GNSS, VOL.6, No. 3, p.48-55, 2011.

[8] Dovis, Fabio and Ali, Khurram and Pini, Marco and Cavaleri, Antonio and Ali, Khurram, "Detection of Spoofing Threats by Means of Signal Parameters Estimation", Proceedings of the ION GNSS, Portland, 2011.

[9] Psiaki, Mark, O'Hanlon, Brady, Bhatti, Jahshan A and Shepard, Daniel P and Humphreys, Todd, "Civilian GPS spoofing detection based on dual-

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

receiver correlation of military signals", Proceedings of the Institute of Navigation GNSS conference, 2011.

[10] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS Spoofing Detection Based on Signal Power Measurements: Statistical Analysis," International Journal of Navigation and Observation, vol. 2012, Article ID 313527, 8 pages, 2012. doi:10.1155/2012/313527.

[11] J. Nielsen, V. Dehghanian, and G. Lachapelle, "Effectiveness of GNSS Spoofing Countermeasure Based on Receiver CNR Measurements," International Journal of Navigation and Observation, vol. 2012, Article ID 501679, 9 pages, 2012. doi:10.1155/2012/501679.

[12] Lee, Young, "Two New RAIM Methods Based on the Optimally Weighted Average Solution (OWAS) Concept", Navigation Journal, ION, vo.54, No:4, p.333-345, 2007.

[13] Phelts, Robert Eric, "Multicorrelator techniques for robust mitigation of threats to GPS signal quality", PhD thesis, The Department of Mechanical Engineering, Stanford University, 2001.

[14] E. D. Kaplan, and C.J. Hegarty, "Understanding GPS Principles and Applications", *Artech House Publishers*, 2006.

[15] Tsui, J. B.-Y. (2001) "Fundamentals of Global Positioning System Receivers: A Software Approach", John Wiley & Sons, Inc., New York, USA. doi: 10.1002/0471200549.

[16] Lyons, Richard, "Understanding digital signal processing", Pearson Education, 2010.

[17] Spirent GSS8000 multi-GNSS Constellation (Galileo and GPS) Simulator, www.spirent.com/Solutions-Directory/GSS8000.aspx.

[18] Fraunhofer broadband triple-frequency L1,L2,L5 Front-end, http://www.iis.fraunhofer.de/de/bf/ln/technologie/gnss.html, 2009.

[19] Proakis, John G., Digital Communications, *MC Graw-Hill*, 2001.

[20] Franz, Walter and Hartenstein, Hannes and Mauve, Martin, "Inter-Vehicle Communications Based on Ad Hoc Networking Principles", The FleetNet Project, Karlsruhe, Germany, 2005.

[21] Tawk Youssef , Jovanovic Aleksandar, Tome Phillip, Leclere Jerome, Botteron Cyril, Farine Pierre-Andre, Riem-Vis Ruud and Spaeth Bertrand, 'A New Movement Recognition Technique for Flight Mode Detection', International Journal of Vehicular Technology, Hindawi, 2012.