An Approach to Discriminate GNSS Spoofing from Multipath Fading

Ali Broumandan, Ali Jafarnia-Jahromi
and Gérard Lachapelle
PLAN Group
University of Calgary, Calgary, Canada
{ajafarni, abrouman , lachapel}@ucalgary.ca

Rigas T. Ioannides
TEC-ETN ESA/ESTEC
European Space Agency
Noordwijk, The Netherlands
rigas.ioannides@esa.int

Abstract—GNSS signals are vulnerable to various types of interference including jamming and spoofing attacks. Spoofing signals are designed to deceive target GNSS receivers without being detected by conventional receiver quality monitoring metrics. This paper focuses on detecting an overlapped spoofing attack where the correlation peaks of the authentic and spoofing signals interact during the attack. Several spoofing detection and signal quality monitoring (SQM) metrics are introduced. This paper proposes a spoofing detection architecture utilizing combination of different metrics to detect spoofing signals and distinguish them from multipath signals. Experimental results show that the pre-despreading spoofing detection metrics such as variance analysis are not sensitive to multipath propagation and can be used in conjunction with post-despreading methods to correctly detect spoofing signals. Several test scenarios based on different spoofing and multipath cases are performed to demonstrate the effectiveness of the proposed architecture to correctly detect spoofing attack and distinguish them from multipath.

Keywords—GNSS, Authenticity Verification, Multipath, Spoofing

I. INTRODUCTION

Authenticity verification of received GNSS signals is gaining more importance as different types of interference signals such as spoofing and meaconing are becoming more feasible due to advances in software defined radio (SDR) technology. Spoofing and meaconing signals are structural types of GNSS interference that take advantage of the same structure as that of legitimate signals but try to deceive their target receiver into generating a fake position and/or timing solution. This type of attack is more dangerous than conventional interference signals since a spoofed receiver still provides a position solution without being aware that it is incorrect. This becomes much more important if the receiver is used in safety of life applications [1-5].

The features of structural interference signals are similar to those of authentic GNSS signals; therefore, a stand-alone GNSS receiver may face some challenges in detecting this type of interference. Spoofing signals can be designed to mislead the tracking procedure of GNSS receivers by generating synchronized PRN codes leading to counterfeit correlation peaks. This means the PRN index and signal parameters such as Doppler frequencies and code delays of spoofing signals match those of the authentic ones. These fake correlation peaks can overlay the authentic ones, distort the normal shape of authentic correlation peaks and gradually misdirect the tracking process of the target receiver. Detection and mitigation of spoofing attacks on GNSS receivers in tracking mode have become one of the important anti-spoofing topics [3-6], [6] has analysed the effect of interaction between authentic and spoofing peaks on the tracking process of a GNSS receiver. Various parameters such as relative power, delay and Doppler frequency of spoofing signals have been considered in this analysis. [7] showed that the interaction between authentic and spoofing correlation peaks is very similar to the case of direct and multipath signal component interaction. Therefore, it is highly challenging for a receiver to discriminate between an overlapping spoofing correlation peak and a specular multipath scenario.

Most spoofing detection metrics are designed to detect a spoofing attack assuming there are only two states, namely clean data or spoofing attack [11]. However, in operational conditions there might be several situations that may affect the performance of spoofing detection metrics. Amplitude based spoofing detection metrics such as SQM are originally designed to monitor the correlation peak quality affected by multipath [8][9]. These methods are modified to detect a spoofing attack. However, utilizing these does not guaranty correct spoofing detection. More specifically the spoofing detection flag may be raised even if a receiver is operating in a multipath environment. Pre-despreading methods, namely variance analysis and Structural Power Content Analysis (SPCA) methods, detect a spoofing attack if the signal variance is above a predefined value [15]. As will be shown in this paper utilizing GNSS data in realistic multipath environments, pre-despreading spoofing detection metrics are not affected by false spoofing detection and hence can be used to correctly detect spoofing signals from multipath signals. The main objective of this research is to provide a receiver architecture based on various observables at different processing levels of a receiver and distinguish multipath from spoofing attacks.

An overview of various spoofing detection methods at different operational levels of a GNSS receiver with focus on its tracking stage is provided. Pre-despreading metrics have been employed to detect the presence of excessive amount of power in GNSS bands. Afterwards, post-despreading methods are employed to detect an abnormal behaviour of correlation peaks which may be caused by multipath or overlapped spoofing signals. A modified version of the SQM technique is
used to detect an abnormally shaped correlation peak during tracking stage. Then a metric combining approach is proposed to simultaneously use both groups of pre-despreading and post-despreading metrics towards discriminating between spoofing and multipath interference signals. This approach focuses on the differences between spoofing and multipath signals that can be used for discrimination purpose. The detection thresholds have been tuned based on an acceptable false alarm probability under various urban and sub-urban multipath scenarios. Then the spoofing detection probability is calculated under overlapped spoofing scenarios wherein counterfeit correlation peaks try to misdirect the tracking process. The processing results show the effectiveness of the proposed metric combination in identifying spoofing attacks at the tracking level.

Section II describes the spoofing scenario and system model considered in this paper. Section III discusses the spoofing detection metrics in various operation layers of a receiver. Section IV introduces the proposed spoofing discrimination methodology. Section V describes experimental results in multipath fading environments. Section VI provides a performance analysis of the proposed metrics in the presence of an overlapping spoofing attack. Concluding discussions are provided in Section VI.

II. SPOOFING SCENARIO AND SYSTEM MODEL

The techniques discussed herein focus on open sky channel conditions wherein a receiver can observe both authentic and spoofing signals. In the following subsections the assumptions of spoofer signal parameters are provided.

A. Relative Doppler

Based on the discussions provided in [14,15], a spoofing attack on tracking receivers in terms of their relative Doppler frequencies can be generally divided into two categories, namely locked Doppler and consistent Doppler. In locked Doppler mode, a receiver based spoofer tries to align the Doppler frequency of the fake signal with that of the authentic GNSS signal while their relative code delay is changing. In consistent Doppler spoofing, the Doppler frequency and code delay rates of spoofing signals are consistent. In this analysis a consistent Doppler scenario is assumed where the Doppler differences between spoofing and authentic signals are less than 5 Hz. This is a practical assumption since depending on the spoofing scenario the spoofing knowledge of the receiver carrier Doppler could be within this range of accuracy.

B. Relative Power

Spoofing power is an essential feature in order to misdirect its target receiver into tracking the counterfeit PRNs. The relative power level of spoofing signals with respect to that of the authentic ones can highly affect the effectiveness and error limit of spoofing interference. Adjustment of the spoofing power level at a target receiver is challenging since it requires information about the propagation channel between the spoofer and target receiver, the antenna gain pattern and its orientation. A powerful spoofing interference can generate a dominant correlation peak that is more powerful than the authentic peak and can mislead the tracking point of the target receiver into an arbitrary point determined by spoofing signals. In an ideal case, the power level of the spoofing signal should be slightly higher than that of the authentic signals but it should not excessively overpower the authentic peak in order to avoid being detected by power monitoring anti-spoofing techniques. A lower power spoofing interference is not able to take away the tracking point of the receiver but it can distort the shape of the correlation peak and lead to a biased pseudorange measurement [6]. This type of spoofing interference has a similar effect as multipath interference and may lead to several metres of pseudorange measurement error [10]. Here, relative spoofing power in the range of -1 dB to +3 dB is considered.

C. Relative Delay

The main goal of a spoofing attack is to misdirect the observations of a target receiver and this is associated with the relative delays of spoofing signals with respect to those of the authentic ones. A spoofing signal may slightly change its relative code delay with respect to the authentic signal in order to gradually take away the tracking point of the target receiver’s DLL without causing loss of lock. An accurately designed spoofing attack can change its relative power level as it changes its relative delay with respect to that of the authentic ones. Here it is assumed that the relative spoofing code delay is within 0.3 chip.

D. System Model

Considering civilian Galileo E1 signals, the received signal affected by a spoofing attack can be modeled as

$$ r(nT) = \sum_{n \in J} \sqrt{p_n} F_n^s(nT)$$

$$+ \sum_{q \in J} \sqrt{p_q} F_q^s(nT) + \eta(nT) $$

where

$$F_n^s(nT) = \begin{cases} d_n^s(nT_c - \tau_n^s)c_n^s(nT_s - \tau_n^s) & \text{if } n \in J \\ -d_n^s(nT_c - \tau_n^s)c_n^s(nT_s - \tau_n^s) & \text{if } n \notin J \end{cases}$$

$$F_q^s(nT) = \begin{cases} d_q^s(nT_c - \tau_q^s)c_q^s(nT_s - \tau_q^s) & \text{if } q \in J \\ -d_q^s(nT_c - \tau_q^s)c_q^s(nT_s - \tau_q^s) & \text{if } q \notin J \end{cases}$$

and $J^a$ and $J^s$ are authentic and spoofing signal sets, respectively. $T_a$ is the sampling interval and $\phi, \varphi, p$ and $\tau$ are the carrier phase, Doppler frequency, signal power and code delay of the received signals; the superscripts ‘$s$’ and ‘$a$’ refer to the spoofing and authentic signals. In this model, $d(nT)$ is the transmitted E1-B navigation data bit at time instant $nT$ and $c(nT)$ is the E1-B spreading code sequence modulated by the E1-B CBOC subcarrier. The circumference accent of navigation bit and spreading code refers to the E1-C signal. The subscripts $m$ and $q$ correspond to the $m$th authentic signal and the $q$th spoofing signal. $\eta(nT)$ is the complex additive white Gaussian noise and $j$ is the square root of -1. During the despreading process, a Galileo receiver correlates the received signal with locally generated synchronized replicas of E1-B and E1-C signals and then performs low pass filtering. The complex correlator output, $u[k]$, can be written as
where $P$ determines the coherent integration interval and $k$ is a short representation of $kPT_i$ which is the time instant at which the correlator output is updated. $\Delta t_i$ and $\tilde{f}_n$ are the code delay and Doppler frequency of locally generated replicas. Assume that the PRN number $l$ is present at both spoofing and authentic signal sets; also assume that the code delays and Doppler frequencies of the spoofing and the authentic signals are very close to those of the local replica. Without loss of generality and for the sake of notation simplicity, only E1-B correlator outputs are analyzed in the sequel.

During the spoofing attack on the receiver in tracking mode and assuming the signal is initially locked onto the $i$th authentic PRN Doppler frequency, the correlator output of Equation (3) can be approximately written as

\[ u_{\text{r}}^{l,\text{A}}[k] = \frac{1}{P} \sum_{n=(k-1)P}^{(k-1)P+1} r(nT_i) c_i (nT_i - \Delta t_i) e^{-j2\pi \tilde{f}_n nT_i}, \]

\[ u_{\text{r}}^{l,\text{C}}[k] = \frac{1}{P} \sum_{n=(k-1)P}^{(k-1)P+1} r(nT_i) \tilde{c}_i (nT_i - \Delta t_i) e^{-j2\pi \tilde{f}_n nT_i}, \]

(3)

where $P$ determines the coherent integration interval and $k$ is a short representation of $kPT_i$ which is the time instant at which the correlator output is updated. $\Delta t_i$ and $\tilde{f}_n$ are the code delay and Doppler frequency of locally generated replicas. Assume that the PRN number $l$ is present at both spoofing and authentic signal sets; also assume that the code delays and Doppler frequencies of the spoofing and the authentic signals are very close to those of the local replica. Without loss of generality and for the sake of notation simplicity, only E1-B correlator outputs are analyzed in the sequel.

During the spoofing attack on the receiver in tracking mode and assuming the signal is initially locked onto the $i$th authentic PRN Doppler frequency, the correlator output of Equation (3) can be approximately written as

\[ u_{\text{r}}^{l,\text{A}}[k] = \sqrt{P} d_{\text{f}}^l[k] + \eta_{\text{f}}[k] + \left( \frac{\Delta r_{\text{f},l} [k]}{P} \right) + \left( \frac{\Delta \Phi_{\text{f},l} [k]}{P} \right) + e^{-j(\Delta r_{\text{f},l} [k]/24\pi - 1) - j(\Delta \Phi_{\text{f},l} [k]/8\pi)}, \]

\[ u_{\text{r}}^{l,\text{C}}[k] = \sqrt{P} d_{\text{f}}^l[k] + \eta_{\text{f}}[k] + \left( \frac{\Delta r_{\text{f},l} [k]}{P} \right) + \left( \frac{\Delta \Phi_{\text{f},l} [k]}{P} \right) + e^{-j(\Delta r_{\text{f},l} [k]/24\pi - 1) - j(\Delta \Phi_{\text{f},l} [k]/8\pi)}, \]

(4)

where $d_{\text{f}}^l[k]$ and $d_{\text{f}}^l[k]$ represent authentic and spoofing data bits at the $i$th integration interval. $\eta_{\text{f}}[k]$ represents the low pass filtered Gaussian noise component with variance $\sigma^2$ at the output of the $i$th PRN correlator. $\Delta r_{\text{f},l}^i$, $\Delta r_{\text{f},l}^i$ and $\Delta \Phi_{\text{f},l}^i$ represent the differences between code delays, Doppler frequencies and initial carrier phase values of spoofing signals and those of the locally generated replica. $R(.)$ is the correlation function which is closely related to the choice of the GNSS signal’s subcarrier.

III. SPOOFING DETECTION METRICS

Several spoofing detection metrics in different operation layers of a receiver have been proposed. These metrics can generally be divided in two categories, namely pre-despreading and post-despreading techniques. In the following, the different metrics used in this investigation are defined.

A. Pre-Despreading Spoofing Detection

This section focuses on different spoofing detection methods based on monitoring the received signal strength (RSS). These techniques generally rely on the assumption that spoofing signals are more powerful than the authentic ones and a successful spoofing attack transmits several fake PRN signals in order to mislead a target receiver into providing a false PVT solution. Pre-despreading methods evaluate the overall power content of the received signal set without separately analyzing different PRN signals. This category of spoofing detection looks for any abnormal variation in the received signal power prior to the despreading process in the receiver. At this stage, the GNSS signals are buried under the noise floor and a spoofing detection test is performed based on the analysis of the power content of received baseband signals. Two spoofing detection metrics are analysed here.

1) Baseband Variance Analysis

This method continuously monitors the variance of baseband signals in order to detect additional power injected by interference signals. Most commercial GNSS receivers are equipped with an AGC module that adaptively changes the receiver input gain based on the variance of the received signal in order to efficiently use the quantization levels of the input ADC module. A feedback circuit controls the AGC gain and monitoring this gain value can be used for detection of the inclined signal variance due to the presence of spoofing interference (Akos 2012). Assuming that the received signal is zero mean, the input signal variance can be represented as

\[ \sigma^2 = \frac{1}{N} \sum_{n=1}^{N} r(nT_i) \times r^*(nT_i) \]

(5)

wherein $N$ represents the number of temporal samples over which the expectation is performed. This method does not take advantage of any spoofing signal features and simply assumes that the spoofing signals’ power content elevates the ambient noise floor. A spoofing (or generally interference) attack will be detected if the estimated variance is higher than a predefined detection threshold. Defining a proper detection threshold requires an initial power level calibration in the presence of authentic Galileo signals in a typical operational environment. Another limitation of this method is that it cannot distinguish a spoofing attack from other interfering sources.

2) Structural Power Content Analysis (SPCA)

This section discusses a low complexity pre-despreading spoofing detection approach that takes advantage of the cyclo-stationarity of GNSS signals in order to detect excessive amount of structured signal power in the received sample set. In this approach, the received raw signal samples are first filtered within the GNSS signal bandwidth and then multiplied by their one-chip delayed version in order to remove the effect of Doppler frequency. It will be shown that the resulting signal has a line spectrum since it is generated by multiplication of cyclo-stationary signals. In the next stage, the signal and noise components are filtered by suitably designed comb filters. A detection test statistic is calculated based on the filter outputs and is then compared to a threshold in order to differentiate between the presence and absence of spoofing signals [1]. Since each PRN signal is received from a different satellite with different relative dynamics with respect to a user, their corresponding Doppler frequencies are different from each other. Therefore, in order to concentrate all signal components on the same spectral lines and facilitate spectral filtering, the Doppler shifts of the signals should be removed. To this end,
the sampled baseband signal components are first multiplied by the complex conjugate of their one (or more) chip delayed version as [1]

\[
y(nT_s) = r(nT_s) \times r(nT_s - T_c) = y_a(nT_s) + y_{sa}(nT_s) + y_{a\eta}
\]

(6)

where \(T_c\) is the chip duration, which is equal to 1/1023 ms for Galileo E1 signals. The term \(y_a(nT_s)\) represents the sum of products of individual Galileo signals in their delayed conjugate version. \(y_{sa}(nT_s)\) is the cross correlation of different PRN signals. Since Galileo spreading codes are periodic sequences, their products into their delayed version also remains periodic. Therefore, \(y_{a\eta}(nT_s)\) still obtains spectral lines with the same frequency spacing as original Galileo signals. Typical Doppler shifts for baseband Galileo signals are a function of user and satellite dynamics and are normally between -5 kHz and +5 kHz. Therefore, it can be written that \(f_s T_c = 1\). This operation removes the phase rotation due to the Doppler frequency of received Galileo signals. It also removes the navigation data bits and secondary codes and Galileo subcarriers that are modulated on each Galileo spreading code. Figure 1 shows the operational block diagram of the SPCA method. SPCA does not need a clean data set for the spoofing detection threshold calculation. In addition, it is not sensitive to other types of interfering signals such as narrowband jamming. Hence, compared to the variance analysis method, the SPCA technique provides spoofing detection with a higher reliability.

B. Post-despreading spoofing detection

The post-despreading methods take advantage of the known signal structure of spoofing signals and analyze the power content of each PRN in order to discriminate between authentic and spoofing signals. In the following, two post-despreading spoofing detection metrics are discussed.

1) Effective C/N0 Analysis

Effective C/N0 is a common signal strength monitoring metric that is available in most commercial receivers. Herein, the effectiveness of this metric toward detection of a spoofing signal is investigated. The Effective C/N0 of the \(m\)th authentic PRN in the presence of spoofing interference assuming a large front-end bandwidth can be written as (Betz 2001)

\[
\left( \frac{C}{N_0} \right)_m^\ast = \frac{p_{\ast m}}{N_0 + \sum_{q \neq m} p_q \int_{-\beta \omega_0}^{\beta \omega_0} G_q^\ast (f) G_m^\ast (f) df + \sum_{k \neq m} p_{\ast k} \int_{-\beta \omega_0}^{\beta \omega_0} G_{\ast k}^\ast (f) G_m^\ast (f) df}
\]

(7)

\(G_m^\ast (f)\) is the PSD of the desired Galileo signal normalized to unit area over infinite bandwidth limits.

2) SQM for Spoofing Detection

The interaction between authentic and spoofing signals causes distortion on the shape of the correlation function. Signal Quality Monitoring (SQM) tests focus on this feature in order to detect any asymmetry and/or abnormally sharp or elevated correlation peaks due to the presence of undesired signals [12]. This metric is originally designed to monitor the correlation peak quality affected by multipath signals. One of the advantages of SQM tests is that they are not highly dependent on training or a calibration process based on a clean dataset [6]. It is assumed here that the receiver is initially tracking authentic signals. Five correlator outputs were used to detect malicious activity on the correlator outputs. \(\Delta\) tests, symmetric and asymmetric ratio tests were implemented to detect a spoofing attack [6]. They are divided into three categories in order to find asymmetric and/or flattened correlation peaks. These metrics are listed in Table 1.

Figure 1: Operational block diagram of structural power content analysis approach

The thermal noise power density is assumed to be \(N_0\) and \(G_q^\ast (f)\) is the normalized spectral density of \(q\)th spoofing signal. \(\beta_\omega\) is the front-end bandwidth. \(G_m^\ast (f)\) refers to the normalized PSD of the \(k\)th authentic PRN. The denominator of Equation (7) consists of three terms, the first one corresponds to the ambient noise component, the second refers to the cross correlation between spoofing signals and authentic replica and the third to the cross correlation caused by other authentic signals. Equation (7) shows that the cross correlation term caused by high power spoofing signals can become the dominant term in the denominator which is directly proportional to the power level of spoofing signals. This term considerably reduces the effective C/N0 of authentic PRNs and leads to saturation of spoofing C/N0 values. The upper limit of a GNSS signal power level is known a priori. Hence, for a given receiver, an upper limit for the C/N0 value can be defined. The spoofing detection metric based on C/N0 monitoring works based on this fact. An abnormally high C/N0 value can be an indication of a spoofing attack. A constructive multipath signal can cause a C/N0 value to exceed the spoofing detection threshold and result in a false alarm. Hence, this metric should be used in conjunction with other spoofing detection metrics to reduce false alarm probability.
Table 1: List of proposed SQM metrics

<table>
<thead>
<tr>
<th>Test Type</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>ΔΔ tests</td>
<td>[ m_i = \frac{(I_{0.05} - I_{0.01}) - (I_{0.05} - I_{0.01})}{I_0} ]</td>
</tr>
<tr>
<td>Symmetric ratio tests</td>
<td>[ m_1 = \frac{I_{0.05} - I_{0.01}}{I_0} ]</td>
</tr>
<tr>
<td>Asymmetric ratio tests</td>
<td>[ m_1 = \frac{I_{0.05}}{I_0}, m_6 = \frac{I_{0.01}}{I_0} ]</td>
</tr>
</tbody>
</table>

\[ I_d \] is in-phase value of the correlator output spaced by \[ d \] chip from the prompt correlator. As mentioned previously, SQM metrics are originally designed to monitor correlation peak quality affected by multipath. Hence, it is very challenging to discriminate a spoofing attack from a multipath interference using only this method.

IV. SPOOFING DISCRIMINATION METHODOLOGY

Several spoofing detection metrics have now been introduced in the literature. Each is effective for some specific spoofing scenarios while some of the metrics are not capable of distinguishing spoofing from other interference sources. For instance, pre-despreading methods such as IF sample variance analysis based on increased power in IF samples. In the presence of both spoofing and jamming signals the variance analysis spoofing detection method detects additional power content in the GNSS frequency band. Hence, when a spoofing detection flag is raised, either a spoofing or jamming attack may have occurred. On the other hand, other spoofing detection methods including post-despreading techniques detect spoofing attacks when the correlator outputs deviate from their nominal values. However, the correlator outputs can be distorted not only by the spoofing attacks but also by other types of interfering signals such as multipath. To enhance spoofing discrimination accuracy and reduce false alarm probability, the combination of different metrics at different operation layers of the receiver is proposed. The main motivation is to come up with a methodology to discriminate spoofing from multipath signals affecting the correlation peaks. The proposed methodology is summarized in Table 2 where the combination of four different metrics, namely variance analysis, SPCA, C/N₀ and SQM, are suggested for spoofing discrimination and to reduce the false alarm probability. In Table 2, 1 and 0 define whether the test statistic value for each metric is above the threshold or not. In case 1 none of the metrics detect any test statistics above the threshold, hence the receiver is operating on clean data. In case 2 the spoofing detection flag based on variance analysis is set. In this case the receiver is most probably affected by a jamming or non-overlapped spoofing attack. It should be noted that the non-overlapped spoofing attack or in general jamming signals affect the C/N₀ and this can be used to detect interference signals. The main difference between jamming and overlapped spoofing signals is that the jamming signals elevate the noise floor and consequently reduces the effective C/N₀ values; in the overlapped spoofing scenario, the effect of spoofing signals on C/N₀ observables are twofold. The presence of spoofing signals enhances the noise floor which reduces the effective C/N₀, and the construction and destruction of spoofing signals due to frequency difference between spoofing and authentic signals causes C/N₀ values fluctuation. In this paper the C/N₀ metric detects spoofing signals if C/N₀ values pass a pre-defined threshold. Case 3 considers a multipath scenario where the construction and destruction of multipaths signal with the desired signal may raise the SQM and C/N₀ detection flags. However, according to the measurement and simulation results provided in the next section, the pre-despreading metrics do not increase in multipath fading environments. Case 4 detects correct spoofing attack when all detection flags are raised. Note that the above procedure is one of many possible approaches to identify spoofing signals. Other spoofing and interference scenarios and detection metrics can be added.

<table>
<thead>
<tr>
<th>Table 2: Spoofing detection architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>case</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

V. MEASUREMENT RESULTS

In the proposed spoofing detection methodology tabulated in Table 2, the pre-despreading metrics status is the main differentiation factor between spoofing and multipath signals. More specifically, it is assumed that in typical multipath environments the pre-despreading spoofing detection metrics, namely variance analysis and SPCA, are not affected whereas in a spoofing scenario the metrics exceed the predefined threshold. This is justified since in typical multipath environments only some of satellite signals are affected by low power multipath signals and some of the satellite signals are blocked by surrounding obstructions. As a result, the total signal power is not increased compared to the open sky clean data set. To validate this assumption, GNSS signal sets at L1 were collected in various locations in the Calgary area. The first and last data sets were collected in an open sky condition in an empty parking lot and serve as clean reference data sets. Another 13 data sets were collected in various suburban, urban and downtown locations. A NovAtel 702 GG antenna was placed on the roof of a vehicle which, during the tests moved with a speed of up to 50 km/h. A front-end using an 8-bit ADC, disabled AGC and 10 MHz bandwidth was used to collect digital samples. A sample data collection location in multipath environments is shown in Figure 2. The data collection environment was surrounded by up to 30 story concrete
buildings. Each data set consist of 40 s of raw IF samples. The IF samples were passed to pre-despreading spoofing detection metrics, namely variance analysis and SPCA. Each metric analysed 1 s of IF samples to output decision statistics. Hence, for each data sets, there were 40 detection metric outputs.

Figure 2: Data collection in multipath environments

Figure 3 shows IF sample variance (above) and SPCA metric (below) outputs as a function of time for various data sets. There are a few data sets with variance metric outputs above the pre-defined threshold indicating there are high power signals in the bandwidth. The signal variance has its highest values for data set 10. Existence of excessive power in the bandwidth can be due to the existence of spoofing or jamming signals. The SPCA metrics outputs shown in Figure 3 interestingly do not show the same pattern as the variance output analysis. In fact, the SPCA metric outputs are high in open sky conditions (data sets 1 and 15) and low during the data collection in dense multipath environments. This is justified since in dense urban environments some of the satellite signals were blocked by surrounding buildings and as a consequence, the GNSS signal power content in the frequency band decreased. Comparing the results of variance and SPCA outputs, one concludes that the increase in the IF samples variance in dense urban environments is due to jamming signals of unknown sources which affected the samples during the test. The power spectral density of received signals for data set 1 (clean data) and data set 10 (affected by jamming) were also analyzed and the results are shown in Figure 4, which shows the power spectral density (PSD) of data set 1 where the PSD of 40 epoch outputs are overlaid. The main peak of GPS signals with a 2 MHz bandwidth is observable. Figure 4 also shows PSD plots of data set 10 for 40 epochs. Comparing the results of data set 1 and 10 reveals that the signals of data set 10 are affected by interfering signals spread all over the signal bandwidth. The existence of these jamming signals elevated the IF samples level and hence at various epochs the variance detection metric values exceeded the detection threshold. It should be noted that this is not due to multipath but jamming signals as observed in Figure 4.
The existence of CW jamming signals did not affect the SPCA metric outputs since SPCA is sensitive to a structural signal type such as multipath and spoofing signals. As shown, the SPCA metric values in all of the 15 data sets were below the threshold. Considering the collected data sets pre-despreading metrics are not affected by multipath distortion. This experimental results justifies use of pre-despreading metrics to discriminate between spoofing and multipath signals as suggested in Table 2.

VI. SIMULATION RESULTS

In order to test the performance of the previously discussed spoofing detection methodology, authentic Galileo signals were collected using a rooftop antenna and then down-converted and sampled using a National Instrument (NI) sampling front-end. The authentic signals were acquired and tracked in a software receiver and different spoofing scenarios were generated and added to the authentic signals using a custom designed spoofing generation software. The spoofing signals are generated based on authentic signal information including Doppler frequency, code delay and amplitude of authentic signals. The block diagram of data collection and spoofing generation software is provided in Figure 5. The sampling frequency is $F_s = 12.5$ MHz and the spoofing attack is generated on both E1-B and E1-C channels corresponding to Galileo PRN-12. The multipath signals are also generated utilizing the same software considering different multipath signal parameters.

![Figure 5: Spoofing generation system](image)

A. Spoofing and multipath scenarios

Figure 6 shows the trend of spoofing signal parameters with respect to that of authentic signals. The spoofing attack takes place over a 200 s interval and the relative delay of spoofing signals with respect to the authentic ones is generated using a first order polynomial. The spoofing signal delay starts at -0.3 chips and gradually increases to completely align with the authentic signal at $t=100$s and then starts to deviate from the authentic correlation peak and end up with a +0.3 chips relative delay at $t=200$s. The relative Doppler of spoofing and authentic signals is also shown in the figure. The carrier Doppler frequency of spoofing signals is consistent with their code rate and has a 5 Hz frequency offset from the authentic carrier Doppler. In this simulation eight spoofing signals corresponding to different PRNs were generated.

Figure 6: Spoofing signal parameters

Three different scenarios with different relative power of spoofing to authentic signals, namely SP1=+3 dB, SP2=+1 dB and SP3=-1 dB, are considered. Herein, it is of interest to distinguish a spoofing attack from a signal affected by multipath signals. To this end, a multipath propagation scenario where the LOS correlation peak is affected by several multipath reflections in a dynamic scenario is considered. The multipath scenario is simulated by considering three multipath rays with various Doppler, delay and amplitude values with respect to the LOS signal. The multipath parameters are provided in Table 3. The multipath signal (MP) generated by combining three multipath rays was added to the clean IF digital samples. There are three signal states namely clean data, multipath affecting clean data and spoofing affecting clean data. The thresholds of the pre-despreading spoofing detection metrics were adjusted in the state of multipath affected signals. Figure 7 shows the normalized IF samples variance for different spoofing and multipath scenarios. The detection threshold is determined to satisfy $P_{FA}=10^{-3}$ in the case of signals affected by multipath. The presence of multipath propagation does not considerably affect the variance based metric. As expected, decreasing the spoofing signal power decreases the test statistics distance from the threshold.

Table 3: Multipath scenario parameters

<table>
<thead>
<tr>
<th>Relative Doppler (Hz)</th>
<th>Relative Doppler rate</th>
<th>Initial Delay (Chips)</th>
<th>Relative power (dB)</th>
<th>Initial code phase (Chip)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP 1</td>
<td>2</td>
<td>0.01</td>
<td>0.3</td>
<td>-6</td>
</tr>
<tr>
<td>MP 2</td>
<td>-1</td>
<td>0.01</td>
<td>0.05</td>
<td>-7</td>
</tr>
<tr>
<td>MP 3</td>
<td>-3</td>
<td>0.01</td>
<td>0.01</td>
<td>-8</td>
</tr>
</tbody>
</table>
Figure 7: Variance analysis metric under dynamic multipath and various spoofing power values (SP: Spoofing, MP: Multipath, Th: Threshold)

Figure 8: SPCA analysis metric under dynamic multipath and various spoofing power values

Figure 9: C/N₀ variations under dynamic multipath scenarios

Figure 10: Doppler values for different spoofing scenarios

detection threshold. C/N₀ fluctuations for the multipath and spoofing scenarios are very similar and it is not possible to distinguish spoofing from multipath signals based on this metric. As is clear from Figure 9 the P_D based on monitoring C/N₀ during the entire data set is not 1. More specifically the C/N₀ values passes the threshold several times. This is due to the changes in the relative phase of the spoofer/multipath signal with respect to the desired one.

Figure 10 shows the Doppler values of different scenarios. In the case of SP1 and SP2 where the spoofing power is higher than the authentic signal, the spoofing signal grabs the tracking control and causes a Doppler difference of about 5 Hz between spoofing and authentic signals. The SP1 scenario takes over the tracking loop control at about 35s from the beginning of the data. This value in the case of SP2 happens a bit later at about 50s from the start of the data set. This is justified since the spoofer power in the SP1 case is higher than that of the SP2. SP3 disturbs the tracking loop performance but since the spoofing power is less than that of the authentic one, the spoofer cannot take control of the tracking loop.

Figure 8 shows SPCA metric outputs under various spoofing and multipath test scenarios. The SPCA outputs are based on 256 ms signal processing. The detection threshold is adjusted to satisfy P_F = 10⁻³ in the case of signal affected by multipath. Comparing the results of Figure 7 and Figure 8, both pre-despreading metrics can detect spoofing signals with P_D = 1. However, the performance of SPCA is better than that of the variance based spoofing detection metric since the distance of the test statistics from the threshold in the SPCA case is larger than that of the variance case. SPCA metric does not need any calibration and hence preferred in practical cases. In addition, as shown in the previous section, SPCA is not sensitive to high power jamming signals such as CW and wideband interference signals.

Figure 9 shows C/N₀ values for various spoofing and multipath scenarios. Here the detection threshold is 50 dB-Hz. The constructive and destructive interaction of multipath and LOS components highly affects the observable C/N₀ values and at several epochs, the effective C/N₀ exceeds the spoofing
Figure 11: Range errors in different scenarios

Figure 11 shows the range error for different spoofing and multipath scenarios. For this analysis, an early-late coherent code discriminator with 0.2 chip spacing was used. The maximum multipath range error is about 30 m. The range error in the case of SP3 is similar to that of the classical multipath error envelope for the case of the narrow correlator [14]. The range error in the case of the SP1 and SP2 scenarios reaches 100 m at the end of scenario. This is because the spoofing power values in the SP1 and SP2 scenarios are higher than those of the authentic signals and consequently it grabs and moves away the tracking point. This was also observed for the Doppler values of Figure 10. Hence, the range error induced by a spoofer depends on its relative power, delay and phase.

Figure 12 shows the probability of detection for each SQM metric defined in Table 1 for the spoofing case. The spoofing detection thresholds for the SQM tests were calculated in the presence of clean data to satisfy $P_{FA}=10^{-3}$.

VII. CONCLUSIONS

The focus was on discriminating spoofing attacks from multipath interference. To this end pre-despreading and post-despreading spoofing detection metrics were incorporated to discriminate between spoofing and multipath signals based on the assumption that the pre-despreading metrics are not affected in typical multipath scenarios. This assumption was validated by collecting actual data sets in different multipath fading environments. Four different spoofing detection metrics, namely variance analysis, SPCA, $C/No$ and SQM, were implemented. The probability of detection of each metric for a given probability of false alarm was investigated. The interaction between authentic and counterfeit signals at the correlator level was analysed and various parameters that can affect the tracking process of a typical Galileo receiver in the presence of structural interference were discussed. A software based spoofing scenario with various relative power values was generated and it was shown that a moderate power spoofing attack can simultaneously raise the pre-despreading and post-despreading spoofing detection metrics. It was also shown that, when the spoofing power level is higher than that of the authentic signals, the spoofing signals can induce a considerable pseudorange error in the target receiver.

ACKNOWLEDGMENT

The work reported in this paper has been performed under a contract from the European Space Agency in the framework of the Announcement of Opportunities on GNSS Science and Innovative Technology within the European GNSS Evolutions Programme (EGEP). The views presented in the paper represent solely the opinion of the authors.

REFERENCES


NAVITEC2016, ESA/ESTEC, Noordwijk, 14-16Dec2016 9/10


