GPS Solut (2015) 19:475–487
DOI 10.1007/s10291-014-0407-3

ORIGINAL ARTICLE

Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver

Ali Broumandan · Ali Jafarnia-Jahromi ·
Gérard Lachapelle

Received: 13 May 2014 / Accepted: 4 September 2014 / Published online: 23 September 2014

Abstract Spoofing in the form of transmitting fake GNSS signals is a deliberate attack that aims to mislead GNSS receivers into generating false position/time solutions. Current work on GNSS spoofing has mainly focused on spoofing detection where the proposed algorithms only indicate the presence of spoofing attacks. A new architecture consisting of spoofing detection, authentic/spoofing signal classification and spoofing cancelation known as spoofing detection, classification and cancelation for moving GNSS receivers is proposed. Predespreading and acquisition level analysis are performed to detect the presence of spoofing interference. The receiver motion is then used to classify the signals tracked into two groups, namely spoofing and authentic signal sets. A successive spoofing cancelation method is then developed to remove the spoofing signals from the raw digitized samples. It is shown that canceling out the spoofing signals removes multiple access interference and significantly improves the authentic signals' detectability and tracking performance. Finally, after spoofing cancelation, authentic signals are acquired and tracked and their corresponding measurements are passed to a PVT engine for a reliable position solution. The proposed receiver architecture is analyzed in the acquisition, tracking and positioning layers.

Keywords GNSS · Moving receiver · Spatial correlation · Spoofing Detection · Spoofing Mitigation · Successive Spoofing Cancelation

A. Broumandan (✉) · A. Jafarnia-Jahromi · G. Lachapelle
Schulich School of Engineering, Position Location and Navigation (PLAN) Group, University of Calgary, 2500 University Drive, N.W., Calgary, AB T2N 1N4, Canada
e-mail: abrouman@ucalgary.ca
URL: http://plan.geomatics.ucalgary.ca/

Introduction

GNSS receivers are highly vulnerable to structural interference signals such as spoofing and meaconing. A spoofing attack based on a set of synthesized GNSS signals, while not easily detectable, is an effective means of providing bogus position estimates to a victim receiver. Furthermore, cross-correlation and multiple access interference (MAI) of higher-power spoofing signals can increase receiver noise floor, which adversely affects the acquisition and tracking performance of authentic signals by reducing their effective carrier-to-noise (C/N_0) ratios.

Several civilian spoofing countermeasure techniques have been proposed in the literature (Scott 2003; Wen et al. 2005; Humphreys et al. 2008). These techniques focus on specific features of spoofing signals that can separate them from the authentic signals. In order to present a target receiver with a certain power level, a spoofer must know its approximate position as well as the propagation channel between the spoofer antenna and the receiver antenna pattern. These conditions are usually very difficult to meet in real-world spoofing situations, and as such, many spoofing countermeasure techniques rely on power level monitoring of the received GNSS signals in order to detect spoofing PRNs. Nielsen et al. (2012) detect the presence of high-power spoofing signals based on their abnormally high C/N_0 values. Jafarnia et al. (2014) propose a predespreading spoofing detection method that checks for the excessive structural power content of received GNSS signals.

In many practical cases, a spoofer generates multiple fake GNSS signals, which provide a consistent navigation solution and transmits them using a single antenna. As such, spoofing PRNs are spatially correlated since they all experience the same propagation channel. This feature is used in some research works to discriminate them from the spatially distributed authentic signals. McDowell (2007) and Montgomery et al. (2009) have taken advantage of multiple GNSS antennas to detect spoofing PRNs based on monitoring the phase difference between different antenna elements. Nielsen et al. (2011) and Broumandan et al. (2012) use the pairwise correlation between different PRNs received by a moving receiver as a means of detecting the spoofing signals being transmitted from a common direction. Jafarnia et al. (2013) have proposed a method based on monitoring the clock bias variations of a moving GNSS receiver in order to discriminate between the authentic and spoofed position solutions in the case where all of the PRNs are transmitted from a single source. Psiaki et al. (2013) have taken advantage of rapid oscillation of receiver antenna to discriminate spoofing signals based on their phase variations. Spatial null steering using antenna arrays is one of the most powerful countermeasure methods against spoofing signals, and it can effectively discard spoofing and other types of interference (Daneshmand et al. 2012). However, antenna array processing induces uncontrolled biases into receiver measurements, which is to be avoided in high-precision GNSS applications (O'Brien and Gupta 2011). Furthermore, antenna array processing adds additional hardware complexity and cost to the receiver that is not affordable in many commercial applications.

Although the aforementioned methods can effectively counter specific spoofing situations, limited work has been done toward the development of an anti-spoofing receiver structure that detects spoofing attacks, neutralizes them and provides a reliable position and navigation solution. Herein, such robust anti-spoofing receiver architecture for moving GNSS receivers is proposed. This technique takes advantage of different spoofing discrimination techniques to detect the presence or occurrence of spoofing signals and then utilizes the receiver motion to classify the spoofing signals based on the spatial correlation of spoofed PRNs. Afterward, a spoofing cancelation technique is proposed to track and remove the spoofed PRN signals and produce a spoof-free signal that is then tracked by the receiver to provide authentic position solutions. The only assumption on the spoofing generation is that all the spoofing signals are transmitted from a single source. As characterized by Nielsen et al. (2011), the spoofing detection and classification modules utilized here work well in different GNSS propagation conditions. The proposed method does not impose any additional hardware on the receiver, and its computational complexity is low. It is also shown that the proposed spoofing cancelation method does not distort the receiver measurements and, as such, it can be employed in high-precision carrier phase GNSS applications. The proper spoofing detection, classification and cancelation (SDCC) operation of the proposed receiver structure has been tested in real-world spoofing cases.

The received signal model in the presence of spoofing signals is first discussed. An overview of the proposed receiver architecture and its operational process is then provided. A discussion on the employed spoofing classification approach is also presented. The proposed successive spoofing cancelation (SSC) method used to discard the detected spoofing signals is finally introduced. Experimental measurements and results are provided to demonstrate the applicability of the method.

Signal model and problem definition

This section provides a model for received GNSS signals in presence of spoofing propagation. In addition, the cross-correlation effect of spoofing signals and their distortion of authentic GNSS signals are analyzed in this section.

Received signal model

Considering the GPS L1 C/A signal, the received signal subjected to a spoofing attack can be modeled as

$$r(nT_s) = \sum_{m \in \mathbf{J}^a} \sqrt{p_m^a} F_m^a(nT_s) + \sum_{q \in \mathbf{J}^s} \sqrt{p_q^s} F_q^s(nT_s) + \eta(nT_s) \tag{1}$$

where

$$\begin{aligned} F_m^a(nT_s) &= d_m^a(nT_s - \tau_m^a) c_m^a(nT_s - \tau_m^a) e^{j\phi_m^a + j2\pi f_m^a nT_s} \\ F_q^s(nT_s) &= d_q^s(nT_s - \tau_q^s) c_q^s(nT_s - \tau_q^s) e^{j\phi_q^s + j2\pi f_q^s nT_s} \end{aligned} \tag{2}$$

and $\mathbf{J}^a$ and $\mathbf{J}^s$ are authentic and spoofing signal sets, respectively. T_s is the sampling interval, and ϕ, f, p and τ are the carrier phase, Doppler frequency, signal power and code delay of the received signals, respectively, and the superscripts s and a refer to the spoofing and authentic signals, respectively. In this model, $d(nT_s)$ is the transmitted navigation data bit and $c(nT_s)$ is the PRN sequence at time instant nT_s. The subscripts m and q correspond to the mth authentic signal and the qth spoofing signal, respectively. $\eta(nT_s)$ is the complex additive white Gaussian noise with variance σ^2.

Cross-correlation effect of spoofing signal

GNSS receivers detect and track the signal parameters by synchronizing the replica signal with the incoming one. The spoofing transmitter tries to mimic the authentic signals' architecture and thus utilizes the same code structure of the authentic signal. Hence, one major harmful effect of spoofing signals is their cross-correlation effect. The cross-correlation of the GNSS signals, including the GPS Gold code, is not zero and thus causes MAI (Proakis and Salehi 2005). MAI increases the postprocessing noise floor and affects the signal quality measure metric such as C/N$_0$. The amount of MAI in a nominal receiver operation case (e.g., open sky) is not significant. However, in some particular cases, the problem of cross-correlation and MAI is not negligible where some work has been developed to remove this effect (Glennon and Dempster 2004, Mattos 2003; Lopez-Risue and Seco-Granados 2005).

To calculate the receiver postprocessing noise floor, the receiver correlates the received signal set with a normalized PRN signal, $c_\ell(nT_s - \tau_\ell)$, which is known to be absent in the received signal set. In this case, the correlator output can be written as (Van Dierendonck 2002)

$$u_l[\tilde{f}_l, \tilde{\tau}_l, k] = \sum_{m \in \mathbf{J}^a} \sqrt{p_m^a} \psi_{ml}^a[\tilde{f}_l, \tilde{\tau}_l, k] + \sum_{q \in \mathbf{J}^s} \sqrt{p_q^s} \psi_{ql}^s[\tilde{f}_l, \tilde{\tau}_l, k] + \bar{\eta}[k] \tag{3}$$

where

$$\psi_{ml}^a[\tilde{f}_l, \tilde{\tau}_l, k] = \frac{1}{N} \sum_{n=(k-1)N+1}^{kN} F_m^a(nT_s)\, c_l(nT_s - \tilde{\tau}_l) e^{-j2\pi\tilde{f}_l nT_s}$$
$$\psi_{ql}^s[\tilde{f}_l, \tilde{\tau}_l, k] = \frac{1}{N} \sum_{n=(k-1)N+1}^{kN} F_q^s(nT_s)\, c_l(nT_s - \tilde{\tau}_l) e^{-j2\pi\tilde{f}_l nT_s} \tag{4}$$

Therefore, the variance of the correlator output, $u_l[\tilde{f}_l, \tilde{\tau}_l, k]$, provides an estimate of the postcorrelation noise variance. The first term in (3) is the contribution of the authentic signals' cross-correlation; the second terms is spoofing signals' cross-correlation; and the third term is ambient noise to the postprocessing noise floor estimation. Assuming that the number of authentic and spoofing signals is large enough, the distribution of their cross-correlation terms (I and II) becomes an approximate complex Gaussian distribution (Jafarnia 2013). Therefore, the distribution of correlator output in (3) can be written as

$$u_\ell[f_\ell, \tau_\ell, k] \sim \mathrm{N}_c\left(0, \frac{N_0}{2NT_s} + \bar{\sigma}_\psi^2\left(\sum_{m \in \mathbf{J}^a} p_m^a + \sum_{q \in \mathbf{J}^s} p_q^s\right)\right) \tag{5}$$

where $\mathrm{N}_c\left(0, \widehat{\sigma}^2\right)$ is the zero mean circularly symmetric complex Gaussian distribution with a variance of $\widehat{\sigma}^2$. $\bar{\sigma}_\psi^2$ is a constant value representing the cross-correlation variance in either of in-phase or quadrature components for normalized power spreading Gold codes. Equation (5) shows that the variance of the postprocessing noise floor is directly affected by the transmitted power of the authentic and spoofing PRNs. The transmit power of GPS signals is designed such that the cross-correlation level of the authentic PRNs is insignificant. However, spoofing signals can be much more powerful than the authentic GPS signals. Therefore, their corresponding MAI level can overtake the ambient Gaussian noise floor and therefore decrease the authentic Signal-to-Noise Ratio(SNR) at the correlator output of conventional GPS receivers.

Spoofing detection, classification and cancelation receiver architecture

This section presents a general overview of the different blocks of the proposed SDCC receiver architecture. Details of each block are provided in successive sections. Figure 1 shows different block processing units, including spoofing detection, authentic/spoofing signal classification and spoofing mitigation.

The first stage of the SDCC architecture is detection of a spoofing attack. Among many spoofing detection methods proposed in the literature, three low computational complexity and effective techniques are considered where include automatic gain control (AGC) gain level or analog-to-digital convertor (ADC) sample histogram monitoring, structural power analysis (SPA) and acquisition level detection. The techniques check for abnormally high AGC gain levels or an unusual structural power content of the received signals to flag the presence of a possible spoofing attack. The modified signal acquisition stage includes searching all possible code phase and carrier Doppler bins and passing all the signals that are above the designated acquisition threshold to the tracking stage. Occurrence of two or more detectable signals in the acquisition stage may indicate that the receiver is under a spoofing attack and enables the spoofing detection flag.

After detecting all visible satellites which are above the acquisition threshold, all the detected signals including the authentic and spoofing signals will be tracked. In the case of a spoofing attack, the receiver requests the operator to briefly move the receiver antenna for authentic/spoofing classification. The input of the classification unit as shown in Fig. 1 is the tracked signal parameters including raw carrier Doppler measurements. The receiver motion can be detected by incorporating a low-cost IMU in the receiver. Nielsen et al. (2011) have proposed a method based on taking pairwise correlation between signal observations to discriminate the spoofing signals from the authentic ones. Based on the measured correlation coefficient values, signals are sorted in two groups, namely spoofing and authentic. The spoofing group is the signal set that is highly correlated, and the authentic group is the set that is uncorrelated. The proper placement of the members in the authentic and spoofing groups can be reassessed after the

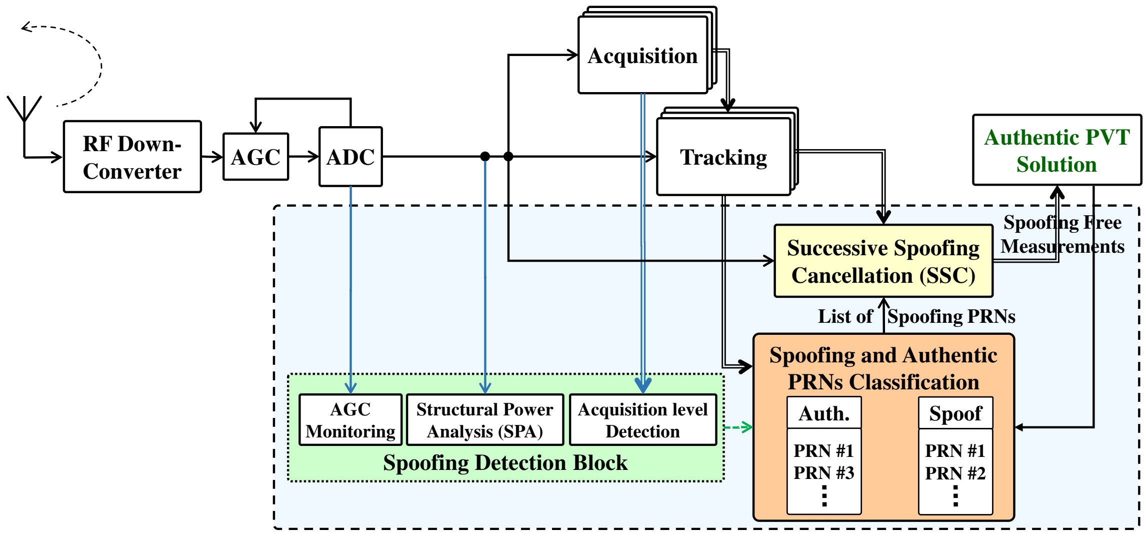

Acquisition
Tracking
RF Down-Converter
AGC
ADC
Authentic PVT Solution
Spoofing Free Measurements
Successive Spoofing Cancellation (SSC)
List of Spoofing PRNs
Spoofing and Authentic PRNs Classification
Auth.
PRN #1
PRN #3
Spoof
PRN #1
PRN #2
AGC Monitoring
Structural Power Analysis (SPA)
Acquisition level Detection
Spoofing Detection Block

Fig. 1 Block diagram of the SDCC receiver architecture

PVT solution as the set of measurements in each group should provide the lowest navigation solution residuals.

After authentic and spoofing signal classification, SDCC enters the spoofing cancelation stage using the SSC method. The input of this processing unit, as shown in Fig. 1, is raw IF samples, the list of spoof PRNs and the tracked signal parameters of all channels. In this stage, the receiver continuously tracks all spoofing and authentic signals to provide accurate measurements of the signal parameters including code offset, Doppler frequency, carrier phase and signal amplitude. After reaching a reliable tracking performance for each individual spoofing channel, the tracked spoofing signals are reconstructed and removed from the original digitized intermediate frequency (IF) samples to provide a spoofing-free IF sample set. After spoofing mitigation, the SDCC architecture runs acquisition again to detect potential authentic and spoofing signals that were not detected in the first acquisition process.

Spoofing detection

Spoofing detection is performed based on the aggregation of several test statistics described in this section. If any of these methods detects the presence of a possible spoofing attack, the receiver enters into the classification stage.

AGC/ADC level analysis

Accurate power level adjustment at the target receiver antenna is a very challenging problem for spoofers. The complexity of this problem increases for the case of a moving target receiver where the spoofer does not have real-time information regarding the targeted receiver location and antenna orientation. Based on the analysis provided by Akos (2012), in most spoofing cases, the AGC level monitoring can be a very powerful indicator of a spoofing attack. Furthermore, since a spoofer is usually a terrestrial transmit source, its received power can highly vary based on the variation of the propagation distance between the spoofer antenna and the target receiver antenna. Therefore, the movement of the receiver with respect to the spoofer antenna can considerably change the AGC gain (or ADC histogram if the AGC is disabled) of the target receiver and reveal the presence of a potential spoofing source.

Structural power analysis (SPA)

The structure of spoofing signals is very similar to that of authentic GNSS signals. The presence of additional spoofing PRNs increases the power content of structural signals in the GNSS frequency band. This excessive amount of power can be detected prior to the despreading process using the authenticity verification method proposed by Jafarnia et al. (2014). To this end, the following processing steps are taken into account:

1. Removing the Doppler frequency of individual PRN signals as

$$y(nT_s) = \mathrm{Re}\{r(nT_s) \times r^*(nT_s - T_c)\} \qquad (6)$$

Herein, $\mathrm{Re}\{\bullet\}$ represents the real part of its argument and T_c represents a code chip duration.

2. Passing the signals through two comb filters tuned on signal and noise components as follows

$$\begin{aligned} g_s(nT_s) &= \sum_{l=0}^{L-1} y(nT_s - lT_e) \\ g_\eta(nT_s) &= \sum_{l=0}^{L-1} (-1)^l y(nT_s - lT_e) \end{aligned} \tag{7}$$

where T_e represents signal epoch length and L defines the filter length. Considering the cyclostationary feature of GNSS signals, $g_s(nT_s)$ contains the signal and noise components and $g_\eta(nT_s)$ contains the noise only components.

3. Normalizing the signal components in order to compensate for the unknown AGC gain variations

$$x(nT_s) = \frac{g_s(nT_s)}{\sqrt{E\{g_\eta(nT_s)\}}} \tag{8}$$

4. Spoofing detection test statistic calculation

$$T(\mathbf{x}) = \frac{1}{N}\sum_{n=0}^{N-1} x^2(nT_s) > \gamma \tag{9}$$

If this test statistic is higher than the detection threshold γ, a warning for a spoofing attack will be generated.

Acquisition stage spoofing detection

A spoofing attack may be detectable during the acquisition stage depending on the spoofing case. This research takes advantage of two detection approaches to warn of the presence of counterfeit spoofing signals. First, the receiver searches over the entire cross-ambiguity function (CAF) range, and detects and verifies all correlation peaks above the detection threshold. Another spoofing detection method at the acquisition level relies on observing an abnormal total number of detected correlation peaks. For instance, for the case of GPS L1 C/A signals, if more than 15 correlation peaks are detected, a spoofing attack will be flagged (the threshold on the number of satellites of course depends on the location of the receiver and can be improved by prior knowledge of the observable satellites).

Authentic and spoofing signal classification

For practical deployment reasons, spoofing signals are radiated from a common transmitter source that can be utilized to detect the spoofing attack. Herein, a method based on the synthetic array process utilizing a single antenna receiver introduced by Broumandan et al. (2012) has been developed to discriminate between authentic and spoofing signals. Consider a GNSS receiver that is spatially moving along an arbitrary trajectory as the signal is processed. Assume there are N authentic and spoofing signals that are available to the receiver. Nielsen et al. (2011) have formulated a binary detection problem based on selecting each of the tracked signals with either of the two plausible hypotheses of authentic and spoofing, as the antenna is spatially moving along an arbitrary trajectory. If the random antenna trajectory is of sufficient length (few meters), then the authentic signal spatial characteristics due to the antenna motion will be uncorrelated. Herein, the correlation coefficient metric has been utilized to measure the correlation between different PRNs parameters as the spoofing detection metric.

Successive spoofing cancelation

As discussed previously, the cross-correlation effect of high-power spoofing signals can highly deteriorate the postprocessing SNR of the authentic signals. Hence, after classification of spoofing and authentic signals, the spoofing signals need to be removed from the IF samples to enhance authentic signal detection and parameter estimation performance. The application of successive interference cancelation (SIC) has been extensively used in CDMA communication channels (Moshavi 1996; Duel-Hallen et al. 1995). SIC has also been used in GNSS for near-far problems in pseudolites applications. In Madhani et al. (2003), a method based on SIC has been applied to the signal processing and tracking stage of the receiver to reduce the effects of structured GPS-like signals whose power is higher than the ambient noise. Herein, a similar approach known as SSC has been implemented to cancel out the spoofing contributions from the received IF samples. Figure 2 shows the operational block diagram of the proposed SSC process. The input of this block is the raw IF samples and signal parameters from the tracking loops. The buffer stores IF data samples from which the reconstructed spoofing signals are subtracted.

The operation of SSC algorithm is as follows:

1. *Spoofing signal reconstruction* having a list of spoofed PRNs from the classification block and the spoofing signal estimated parameters (i.e., code phase $\hat{\tau}_m$, amplitude $\sqrt{\hat{p}_m}$, carrier phase $\hat{\varphi}_m$ and Doppler frequency $\hat{f}_m$) from the tracking loops, an estimate of the spoofing signals is generated as

$$\hat{r}_s = \sum_{m \in \mathbf{J}^s} \sqrt{\hat{p}_m}\hat{d}_m(nT_s - \hat{\tau}_m)c_m(nT_s - \hat{\tau}_m)e^{j\hat{\varphi}_m + j2\pi\hat{f}_m nT_s} \tag{10}$$

2. *Spoofing Removal* the reconstructed spoofing signal $\hat{r}_s$ is subtracted from the total received signal yielding a partially cleaned version of the buffered data.

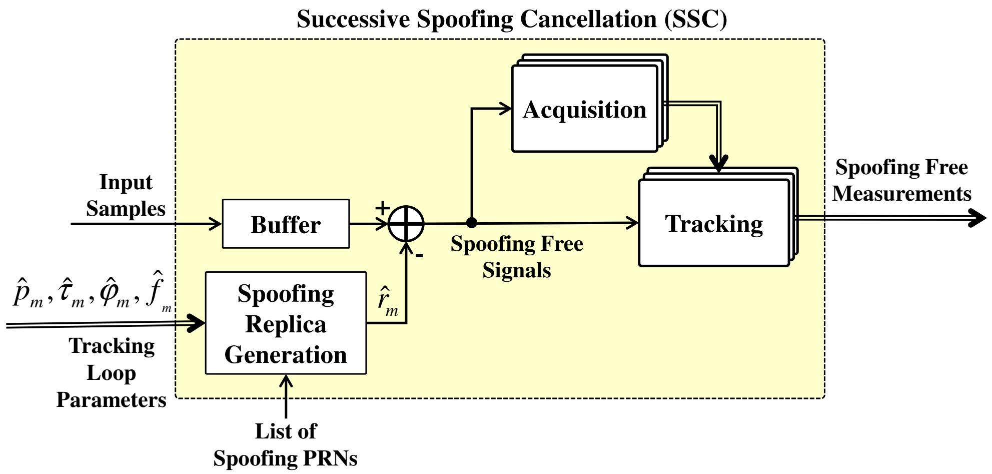

Successive Spoofing Cancellation (SSC)
Input Samples
Buffer
+
-
Acquisition
Tracking
Spoofing Free Measurements
Spoofing Free Signals
$\hat{p}_m, \hat{\tau}_m, \hat{\varphi}_m, \hat{f}_m$
Tracking Loop Parameters
Spoofing Replica Generation
$\hat{r}_m$
List of Spoofing PRNs

Fig. 2 Block diagram of the SSC algorithm

3. *Acquisition* the receiver enters the second stage of the acquisition process to detect possible authentic and spoofing signals, which were not detected due to the spoofing signals' cross-correlation.
4. *Tracking* the cleaned IF samples are used to continue tracking of the previously detected authentic signals and the newly detected correlation peaks.

The signal parameters corresponding to newly detected PRNs are then fed to the classification module in order to discriminate between the authentic and spoofing PRNs.

Experimental results

Experimental results of the SDCC receiver performance are provided in this section. The experimental measurements are based on the reception of GPS L1 C/A signals. Testing an anti-spoofing algorithm in a real case is challenging since outdoor radio transmission in the GNSS frequency bands is not allowed. Therefore, special considerations have to be taken into account.

Data collection setup

This section provides the test method used to evaluate the performance of the SDCC method in real-world cases. The measurements were made to analyze the behavior of spoofing signals initiated from a single-source antenna. For these measurements, Spirent hardware simulator signals (HWS) were radiated deep indoor at a controlled power level using a directional antenna. The spoofing signals were received and then combined with authentic signals coming from a rooftop antenna. Both the authentic and spoofing receiving antennas were briefly moved in a random fashion for spoofing/authentic classification. The random motion causes the authentic signals' parameter to decorrelate rapidly while all spoofing signals are highly correlated due to similar propagation channels. Figure 3 shows the spoofing test situation where a single rover antenna was placed inside a laboratory.

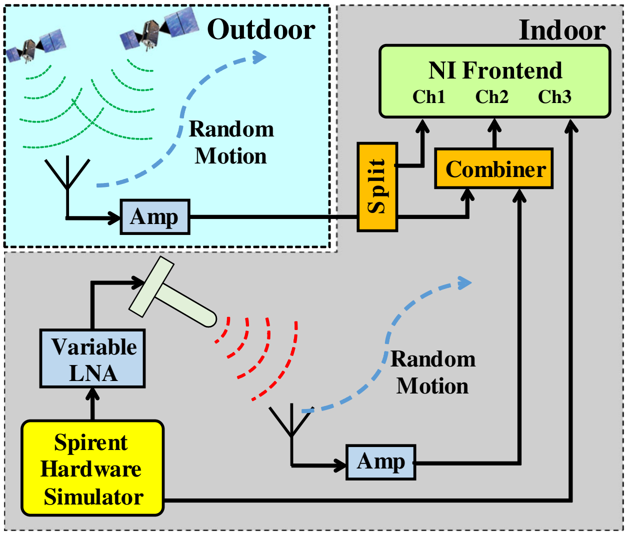


Fig. 3 Data collection case

In all tests, the HWS generated 12 PRNs at the highest level in order to maximize the structural power content of the spoofing signal set. This resulted in C/N$_0$ values of about 52 dB-Hz reported by a NovAtel OEM V3 receiver directly connected to the HWS. The output signal was fed to a variable amplifier with a maximum 60 dB gain and was then propagated indoor via a directional antenna. It should be noted that the variable LNA only adjusts the spoofing propagation power and does not improve the spoofing signals' C/N$_0$. The propagated spoofing signals were received by the rover antenna, the output of which was connected to a combiner. The other input of the combiner was fed by a rooftop rover antenna collecting authentic signals as shown in Fig. 3. Both of the rover antennas consisted of active NovAtel-GPS 701/702 GGL series antennas. The combined signals are then fed to the second channel of a three-channel NI front-end. For comparison, pure authentic and spoofing signals were also connected to two other channels of the FE as shown in Fig. 3. More specifically, the first channel of the FE was connected to the roof top antenna to provide a reference channel for further investigation. The second channel was connected to the combined rover antennas where emulates a GPS receiver under spoofing attack. The third channel of the FE was directly connected to the HWS output. In this experiment, a RF front-end with a 12-bit ADC, 10 MHz sampling frequency and disabled AGC was used.

As discussed before, it is important for an effective spoofer to slightly overpower the authentic signals power level and, at the same time, it does not considerably affect the input AGC gain of the target receiver. To this end, two data sets were collected. The first data set was intended to adjust the spoofing and authentic signals' power levels to provide a realistic spoofing situation and to evaluate the performance of different spoofing detection metrics. In this data set, the variable LNA gain was changed to find the proper power level for spoofing transmission. After spoofing and authentic signal power level adjustment, another data set was collected where the spoofing and authentic signals were sampled with the three-channel front-end as explained previously. Figure 4 shows a photo of data collection environment, and available authentic and spoofing satellites during the test. As shown in Fig. 4, there were 10 authentic and 12 spoofing signals. Without loss of generality and practicality of the proposed method, only one common PRN (PRN 25) between the spoofing and authentic signals occurred.

SDCC receiver performance analyses

A conventional GPS software receiver was modified to incorporate the proposed SDCC receiver architecture. More specifically, predespreading spoofing detection was implemented to detect the spoofing attack and set the spoofing flag. In addition, the acquisition process of the receiver was also modified to detect all available signals above the acquisition threshold and pass them to the tracking process. Specific considerations in the acquisition process were taken into account to avoid frequency side-lobe tracking. If there was more than one peak in the acquisition process, the spoofing attack alarm was set and the receiver went into the authentic/spoofing classification process mode.

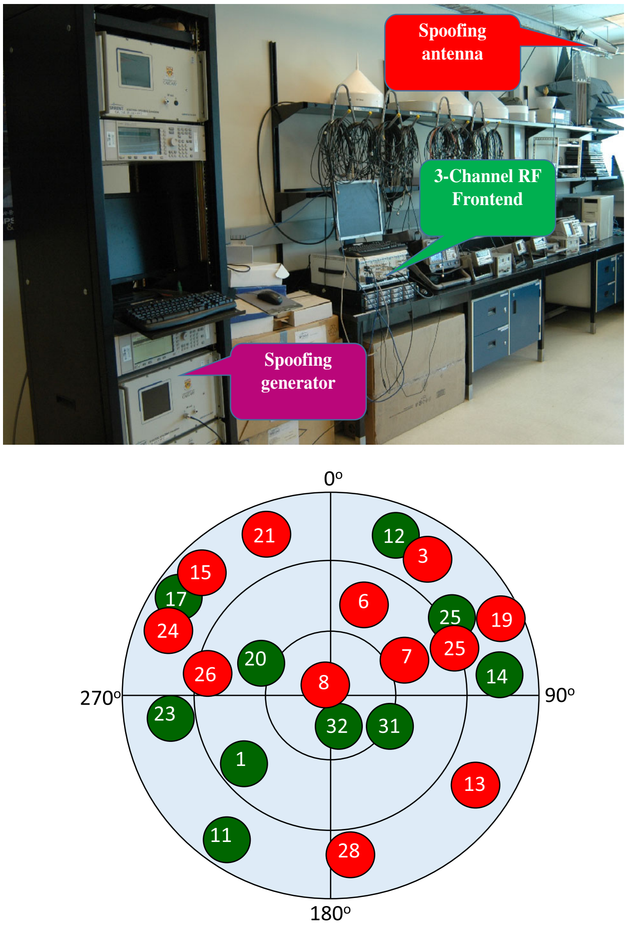
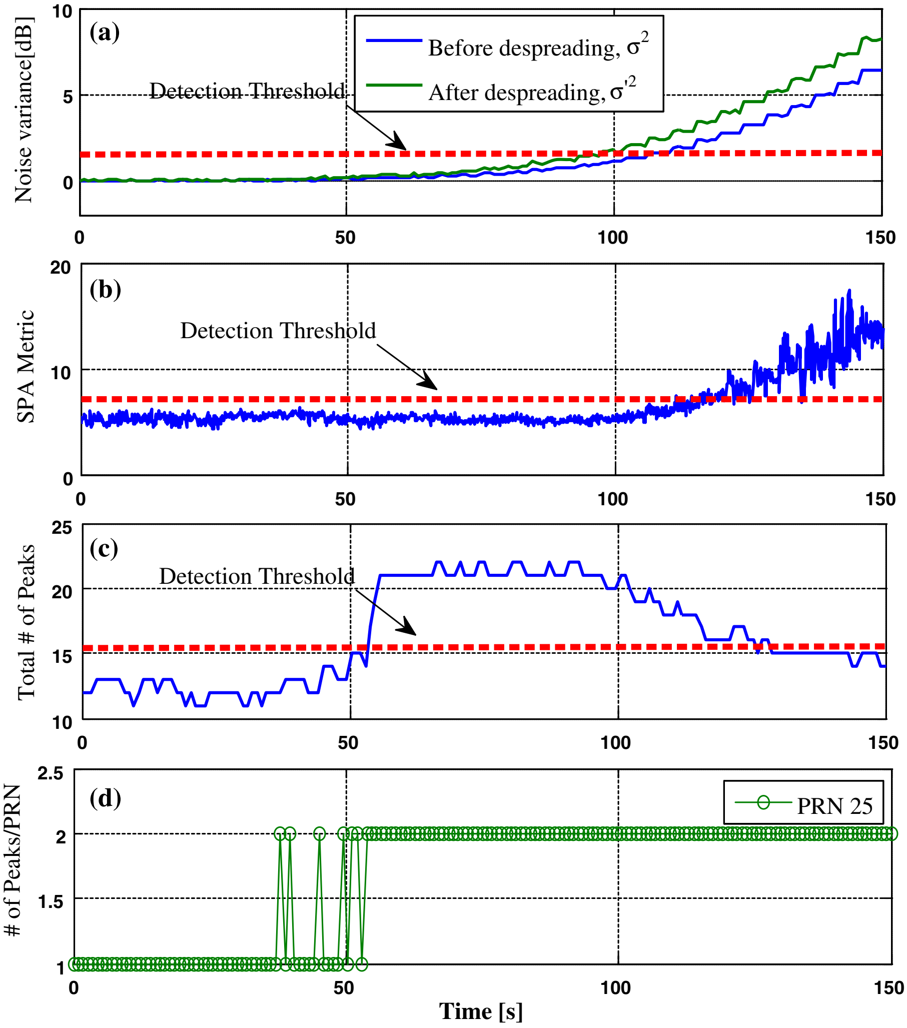


Fig. 4 Data collection setup, location and sky plot of the authentic signals (*green* and *red* PRNs are authentic and spoofing, respectively)

Spoofing detection

To evaluate the detection performance of the SDCC receiver and adjust the spoofing and authentic signals' power levels, the variable LNA power was increased from 30 to 60 dB in 1 dB steps every 5 s in the first data set. The sampled data set from the second channel of the NI front-end was fed to the SDCC receiver. Figure 5 shows the performance of the implemented spoofing detection metrics. The first spoofing detection metric shown in Fig. 5a is the plot of IF samples noise variance (σ^2) and postprocessing noise variance (σ'^2) as a function of time (LNA power). As mentioned before, since the utilized front-end AGC was off, the raw IF sample variance was changed by increasing the LNA gain. This is equivalent to the changes in the AGC gain variation in the case of an enabled AGC. As shown in Fig. 5a, by increasing the LNA power, both predespreading and postdespreading noise variances increase. This increase in the noise floor estimate is insignificant in the first 50 s of the data set (30–40 dB LNA gain). This is due to fact that the received spoofing signal power is less than that of the authentic ones. After 50 s

Fig. 5 Spoofing detection metrics



(40 dB LNA gain), the noise variances start to gradually increase. This is the epoch where the spoofing propagation power is comparable to that of the authentic ones. After 100 s (50 dB LNA gain), the predespreading and postdespreading noise variance increases with steeper slopes. In this case, the spoofing propagation power is getting much higher than that of the authentic signal and starts to jam it. The postprocessing noise variance increases faster since it consists of both the cross-correlation effect as well as the in-band thermal noise effect.

Figure 5b shows the SPA metric as a function of the LNA power. It is observed that the SPA metric gradually increases after about 100 s from the start of the data set. This metric exceeds the detection threshold after 120 s, which shows the excessive amount of structural signal power in the received data set. The SPA metric does not use any knowledge of AGC gain; therefore, this metric is useful for the case when only digital samples are available, and the AGC gain is not accessible by the preprocessing detection technique.

As described before, one can detect a spoofing attack by monitoring the total number of detectable signals and set a spoofing flag. Figure 5c shows the total number of acquired signals as a function of the LNA gain. In this experiment, the acquisition sensitivity was 38 dB-Hz for a 5-ms coherent integration time. The issue of data bit transition is also considered in the acquisition process. Here, the spoofing detection threshold is 15, which means that if there are more than 15 detectable signals in the cross-ambiguity function after processing all 32 GPS PRNs, the spoofing flag will be set. This method can detect the spoofing attack much faster than the two earlier methods and almost after 50 s the spoofing flag is set. This spoofing detection metric is reliable in the 50 to 140 s time window. As shown in Fig. 5c, by increasing the spoofing propagation power, the total number of detectable signals is reduced. This is due to the fact that as the spoofing propagation power increases, it jams the authentic signals and affects their detectability. In this experiment, there is only one common PRN-25 between the authentic and spoofing

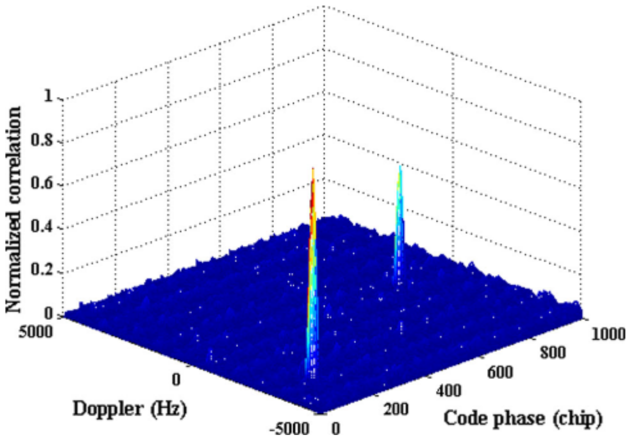


Fig. 6 Cross-ambiguity function of PRN 25 after power level calibration

signals. Figure 5d shows the number of detectable peaks above the acquisition threshold for this PRN as a function of the LNA power. The receiver sets the spoofing flag when there are more than one detectable signal in the cross-ambiguity function per each PRN. As shown, this method can detect the spoofing propagation as early as 35 s from the beginning of the data set and is reliable through it all.

Figure 5 shows that, for a successful spoofer, the spoofing propagation power should be in an acceptable range. The experimental result outcomes of this data set can be divided into three regions. The first region is the case where the spoofing propagation power is lower than that of the authentic signal. This is shown in the first 50 s of the data set. The second region is the case where the spoofing and authentic signal powers are matched as shown in the 50–120 time period. This is the region where an effective spoofer would operate since it is difficult for the most spoofing detection methods to recognize the spoofing attack. In the third region, the spoofing power is higher than that of the authentic ones, and hence, the spoofer jams the authentic signals (after 120 s of data). Thus, to provide a realistic spoofing propagation setup and to avoid jamming the authentic signals, the variable amplifier gain is fixed at 50 dB for the rest of the tests. Figure 6 shows the CAF after the calibration process for PRN 25 where both the authentic and spoofing signals are detectable. As shown, two distinctive peaks are visible in CAF where the stronger signal is the spoofing one. The SDCC architecture has detected both signals and set the spoofing flag.

Spoofing classification

This section demonstrates the SDCC receiver performance utilizing the second data set after authentic/spoofing power adjustment. In this test, the authentic and spoofing rover antennas were static for about 1 min and then were moved in a random fashion simultaneously for about 30 s and after that the antennas were static for about 10 min. The total data record was fed to the proposed SDCC receiver to detect and classify the authentic and spoofing signals and subsequently remove the spoofing signals from the IF samples. The stored IF samples are then processed with a software receiver, GSNRx^{TM} in this case (Petovello et al. 2008), to characterize the signals conditions before and after applying SDCC. Figure 7 shows detectable PRNs and average C/N$_0$ values for three different channels, namely purely authentic (Ch1), combined spoofing plus authentic (Ch2) and purely spoofing (Ch3) before spoofing mitigation.

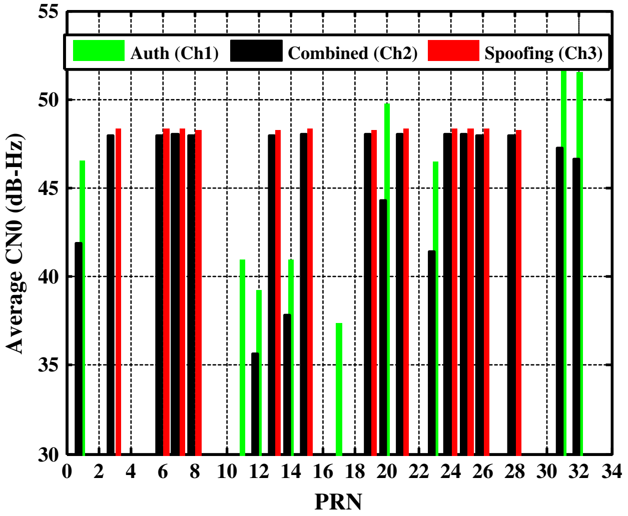


Fig. 7 C/N$_0$ values of the authentic (Ch1), combined (Ch2) and the spoofing signals (Ch3) before SDCC operation

GSNRx^{TM} tracks all spoofing signals (12 PRNs) and seven authentic ones in the combined mode (Ch2). As shown, GSNRx^{TM} could not detect and track three authentic signals, namely PRNs 11, 17 and 25. This is due to the fact that the cross-correlation of the spoofing signals has increased the postprocessing noise variance and reduces the effective C/N$_0$ values of these PRNs, so that they are not detectable. Comparing the C/N$_0$ values of the PRNs in Ch1 and Ch3 with Ch2, it is evident that the C/N$_0$ of the authentic signals is reduced by about 5 dB due to cross-correlation effect of the spoofing signals and noise propagation. The GSNRx^{TM} position solution of the combined channel (Ch2), which received both authentic and spoofing signals, was spoofed. This shows that the spoofer had effectively misled the target receiver.

Signal classification is performed by monitoring the carrier Doppler variation of the moving receiver. It is assumed that the spoofer is propagated from a single-source transmitter. Hence, the Doppler variation due to the

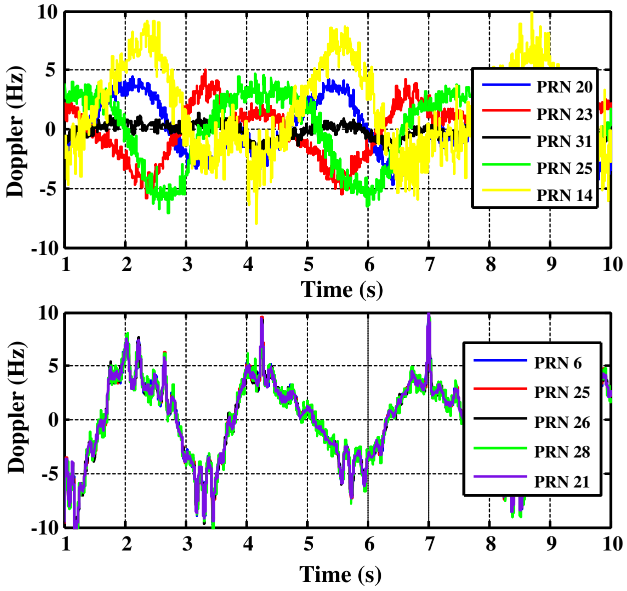


Fig. 8 Carrier Doppler variation in the spoofing and authentic signal successive spoofing cancelation (SSC)

moving antenna follows the same pattern for all spoofing PRNs. This is shown in the bottom part of Fig. 8. In the case of the authentic signals, since different satellites transmit signals from different sources, the Doppler response to the receiver motion will be different for each PRN. In this implementation, raw Doppler measurement outputs from the tracking loops were used as a test statistics to discriminate between the authentic and spoofing signals. In order to observe Doppler variations due to the antenna motion, the carrier Doppler contribution of the satellite motion and clock drift was estimated and removed from the Doppler outputs of the tracking loops. This was done by estimating and interpolating the clock drift and satellite-induced Doppler when the antenna is static. Figure 8 shows the Doppler values of some PRNs due to the user motion for the authentic and spoofing signals. As shown, the spoofing Doppler variations are highly correlated unlike the case for the authentic signals.

After detecting the spoofing propagation and classifying the spoofing and authentic signals, the spoofing signals are removed from the IF samples using the proposed SSC method. Then, the receiver performs acquisition and tracking on the spoofing-free IF samples to detect the authentic signals, which could not be detected in the initial acquisition process.

Acquisition level analysis

As shown in Fig. 7, PRN 17 was not detected due to an increase in noise level. Figure 9 shows the correlation output in the case of PRN 17 before and after applying spoofing cancelation as a function of code phase. Figure 9 also shows the acquisition threshold γ before and after SDCC. The threshold is based on the coherent integration process and is calculated using $\gamma = -2\sigma^2 \ln P_{FA}$ where $P_{FA} = 10^{-8}$ (Kay 1998; Kaplan and Hegarty 2006). It is shown that, before applying SDCC, the correlation peak is below the acquisition detection threshold and hence is not detectable. However, the noise variance is reduced by 3.5 dB after applying the SDCC. The noise reduction is due to removing the spoofing signal's cross-correlation, and it reduces the detection threshold, which makes this PRN detectable by a conventional acquisition process.

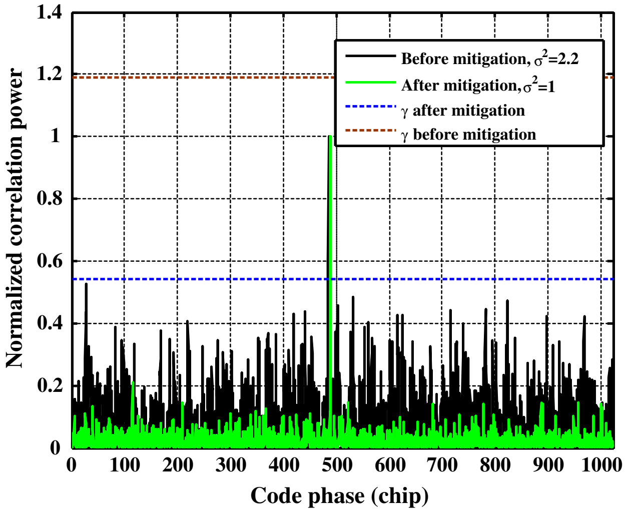


Fig. 9 Code phase correlation output for PRN 17 before and after applying SDCC

Tracking level analysis

In the tracking stage, it is of interest to monitor the tracking performance after applying SDCC. There are different metrics to evaluate the tracking performance; however, the most important one that characterizes the tracking loop performance is C/N$_0$. Figure 10 shows time series of the C/N$_0$ variation for PRN 31 before and after spoofing mitigation. It also shows the C/N$_0$ values of the reference channel for this PRN. After applying SDCC, the C/N$_0$ values are improved by about 3.5 dB. Also, it is evident that the C/N$_0$ values of the reference channel are slightly higher. This may be due that fact that the authentic signal of the second channel of the FE is passed through the combiner, which increases the noise level. Also, it might be due to slight wide-band noise propagation by the spoofer, which is not removable by SSC process.

After SDCC implementation, all the 10 authentic signals were detected and tracked while the tracking loops stayed in the PLL mode and did not lose lock. Figure 11 shows average C/N$_0$ values before and after spoofing cancelation

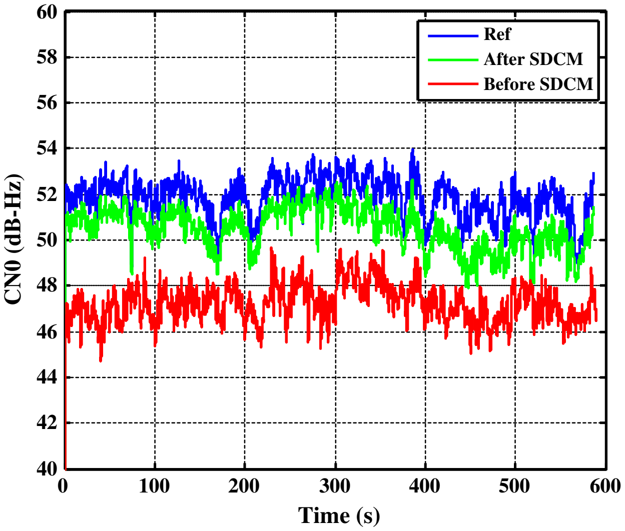


Fig. 10 C/N$_0$ variation before and after SDCC

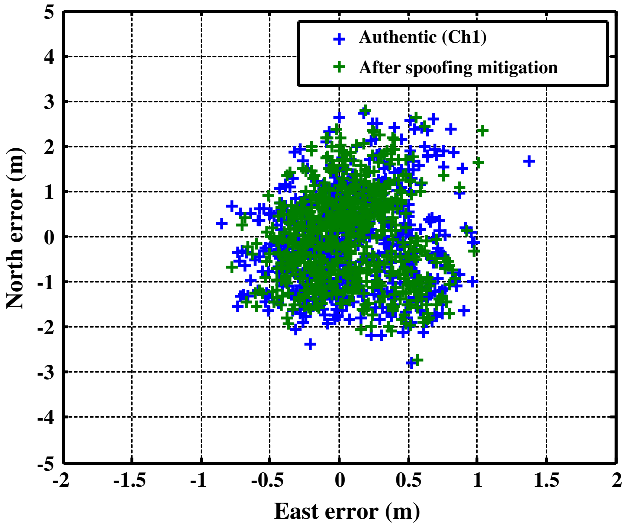


Fig. 12 Reference authentic and SDCC code-based positions

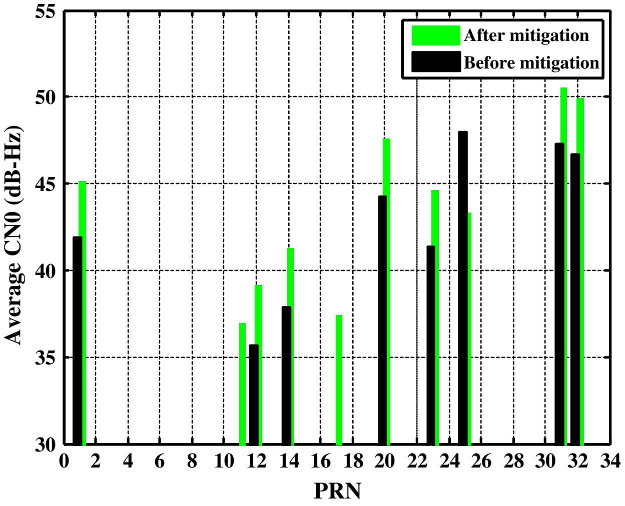


Fig. 11 Average authentic C/N$_0$ before and after spoofing cancelation

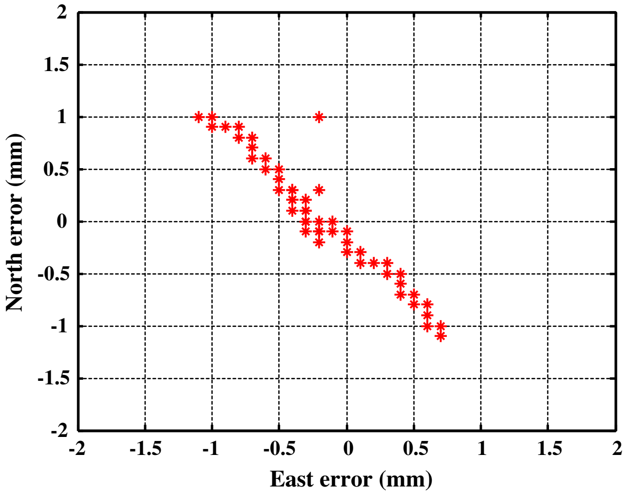


Fig. 13 Carrier phase ambiguity-fixed horizontal errors

for all PRNs. An average 3.5-dB C/N$_0$ improvement is also observable in these plots.

Position level performance analysis

The measurement outputs of the SDCC receiver after spoofing cancelation were passed to RTKlib (http://www.rtklib.com), an open-source position calculation software. Figure 12 compares the code-based position solution of the authentic signal (Ch1) and the receiver under spoofing attack after SDCC operation. The horizontal positioning errors in both cases are very close.

To demonstrate the application of the proposed method in high-precision GNSS applications requiring carrier phase ambiguity resolution, the carrier phase and pseudorange measurements of the SDCC receiver measurements after spoofing cancelation were converted to the RINEX format. The measurements were then analyzed with RTKlib for carrier phase ambiguity resolution in a zero-baseline static mode test. This is of particular importance since the spoofing cancelation approaches based on other techniques such as antenna array processing are prone to measurement distortions, which cause biases in the carrier and code measurements. Figure 13 shows the horizontal errors when the carrier phase ambiguities were fixed. The SDCC receiver output can fix the carrier phase ambiguities, and the rms position error is in the order of a few millimeters.

Conclusions

A spoofing aware receiver architecture was introduced that is able to detect spoofing attacks, classify the spoofing and authentic signals and mitigate the harmful effect of counterfeit spoofing signals. It was shown that the spoofing signals generated from a single-point source can be effectively detected using different metrics, namely AGC level, structural power content and acquisition level analyses. The acquisition level spoofing detection can effectively detect the presence of a spoofing attack in matched power spoofing propagation whereas the AGC level analysis is more reliable in overpowered spoofing propagation. A thorough analysis on the spoofing cross-correlation effect on the receiver sensitivity and effective C/N_0 values based on real data analysis was investigated. Spoofing and authentic signals' classification was implemented by utilizing a spatial pairwise correlation of the signal parameters. Spoofing cancelation was implemented based on introducing the successive spoofing cancelation method that continuously tracks the spoofing signals and removes their effect from the IF samples. Experimental measurement results in a realistic spoofing case revealed that utilizing the proposed architecture improves the detection sensitivity, whereby the C/N_0 values of the authentic signal are improved by about 3.5 dB. The proposed receiver measurements were passed to a RTK position engine to demonstrate the applicability of the SDCC receiver architecture in high-precision GNSS applications.

References

Akos DM (2012) Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). Navigation 59(4):281–290

Broumandan A, Jafarnia A, Dehghanian V, Nielsen J, Lachapelle G (2012) GNSS spoofing detection in handheld receivers based on signal spatial correlation. Proc. IEEE/Ion Plans, Myrtle Beach, South Carolina, pp. 479–487

Daneshmand S, Jafarnia A, Broumandan A, Lachapelle G (2012) A low-complexity GPS anti-spoofing method using a multi-antenna array. Proc. ION GNSS 2012, Institute of Navigation, Nashville TN, pp. 1233–1243

Duel-Hallen A, Holtzman J, Zvonar Z (1995) Multiuser detection for CDMA systems. Proc. IEEE Pers Commun 46–58

Glennon EP, Dempster AG (2004) A review of GPS cross correlation mitigation techniques. In Proceedings 2004 International Symposium on GPS/GNSS, Sydney, Australia

Humphreys TE, Ledvina BM, Psiaki ML, O'Hanlon BW, Kintner PM (2008) Assessing the spoofing threat: development of a portable GPS civilian spoofer. In Proceedings of ION GNSS 2008, Institute of Navigation, Savannah, GA, pp. 2314–2325

Jafarnia A (2013) GNSS signal authenticity verification in the presence of structural interference. PhD Thesis, Report No. 20385, Department of Geomatics Engineering, University of Calgary

Jafarnia A, Daneshmand S, Broumandan A, Nielsen J, Lachapelle G (2013) PVT solution authentication based on monitoring the clock state for a moving GNSS receiver. In Proceedings of European Navigation Conference (ENC2013). Vienna, Austria, p. 11

Jafarnia A, Broumandan A, Nielsen J, Lachapelle G (2014) Pre-despreading authenticity verification for GPS L1 C/A signals. Navigation 61(1):1–11

Kaplan E, Hegarty CJ (2006) Understanding GPS: principles and applications. Artech House Publishers, London

Kay SM (1998) Fundamentals of statistical signal processing: detection theory. Prentice Hall, Upper Saddle River

Lopez-Risue G, Seco-Granados G (2005) CN0 estimation and near-far mitigation for GNSS indoor receivers. Proc IEEE Veh Technol Spring Conf 4:2624–2628

Madhani PH, Axelrad P, Krumvieda K, Thomas J (2003) Application of successive interference cancellation to GPS pseudolite near-far problem. IEEE Trans Aerosp Electron Syst 39(2):481–488

Mattos GP (2003) Solutions to the cross-correlation and oscillator stability problems for indoor C/A Code GPS Proc. ION GNSS 2003, Institute of Navigation, Portland, OR, pp. 654–659

McDowell CE (2007) GPS spoofer and repeater mitigation system using digital spatial nulling. US Patent 7250903 B1, p. 7

Montgomery PY, TE Humphreys, Ledvina BM (2009) Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil gps spoofer. In Proceedings ION ITM 2009, Institute of Navigation, Anaheim, CA, pp. 124–130

Moshavi S (1996) Multi-user detection for DS-CDMA communications. IEEE Commun Mag 34(10):124–136

Nielsen J, Broumandan A, Lachapelle G (2011) GNSS spoofing detection for single antenna handheld receivers. Navigation 58(4):335–344

Nielsen J, Dehghanian V, Lachapelle G (2012) Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements. Int J Navig Obs 501679:9

O'Brien AJ, Gupta IJ (2011) Mitigation of adaptive antenna induced bias errors in GNSS receivers. IEEE Trans Aerosp Electron Syst 47(1):524–538

Petovello M, O'Driscoll C, Lachapelle G, Borio D, Murtaza H (2008) Architecture and benefits of an advanced GNSS software receiver. J Glob Position Syst 7(2):156–168

Proakis J, Salehi M (2005) Fundamentals of communication systems. Prentice Hall Inc, Upper Saddle River

Psiaki ML, Powell SP, O'Hanlon BW (2013) GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In Proceedings ION GNSS 2013, Institute of Navigation, Nashville, TN, pp. 2949–2991

Scott L (2003) Anti-spoofing and authenticated signal architectures for civil navigation systems. In Proceedings ION GPS/GNSS 2003, Institute of Navigation, Portland, OR, pp. 1543–1552

Van Dierendonck AJ (2002) Determination of C/A code self-interference using cross-correlation simulations and receiver bench tests. In Proceedings ION GPS 2002, Institute of Navigation, Portland OR, pp. 630–642

Wen H, Huang PY, Dyer J, Archinal A, Fagan J (2005) Countermeasures for GPS signal spoofing. In Proceedings ION GNSS 2005, Institute of Navigation, Long Beach, CA, pp. 1285–1295

Ali Broumandan received his both B.Sc. and M.Sc. degrees in Electrical Engineering. He received his Ph.D. degree from the Geomatics Engineering Department of University of Calgary in 2009. From 2009 to 2012, has was a senior research associate in Position, Location And Navigation (PLAN) Group of the University of Calgary where his research focused on signal processing aspects of GNSS receiver. From May 2012 to October 2013, he was involved in GNSS industry as a senior GNSS specialist where his work focused on different signal processing aspects of high precision GNSS receivers. Since November 2013, he is with PLAN group of the University of Calgary as a senior research associate where his research focuses on GNSS interference mitigation utilizing antenna array processing. He has been involved in several industrial research projects focusing on spatial/temporal GNSS signal processing.

Ali Jafarnia-Jahromi is a senior research associate/post-doctoral fellow in the Position, Location and Navigation (PLAN) Group of the University of Calgary. He holds B.Sc. and M.Sc. degrees in Telecommunications Engineering from Amirkabir University of Technology. He obtained his Ph.D. degree in Geomatics Engineering from the University of Calgary. His current research focuses on statistical signal processing in GNSS applications, GNSS receiver design and detection and estimation theory.

Gérard Lachapelle holds a Canada Research Chair in Wireless Location in the PLAN Group of the University of Calgary. He has been involved with GPS developments and applications since 1980. His research ranges from precise positioning to GNSS signal processing. More information is available on the PLAN Group website (http://plan.geomatics.ucalgary.ca).