# GNSS Spoofing Detection for Single Antenna Handheld Receivers

JOHN NIELSEN, ALI BROUMANDAN, and GÉRARD LACHAPELLE
University of Calgary, Calgary, Alberta, Canada, T2N 1N4

*Received June 2010; Revised July 2011*

ABSTRACT: *A spoofing source radiates a set of bogus GNSS signals that can deceive a GNSS receiver such that it outputs an incorrect navigation solution. If the jammer signals are sufficiently plausible then the GNSS receiver may not realize it has been insidiously duped before considerable mission cost has incurred. There are various means of detecting spoofing activity and hence providing effective mitigation methods. In this paper, a novel signal processing method applicable to a single antenna handset receiver for spoofing detection is described. Experimental measurements demonstrate the practical effectiveness of this processing, corroborating the theoretical conjectures.*

## INTRODUCTION

Spoofing threat detection and mitigation have been problems of interest since the early stages of GPS operation. Recently it has become evident that spoofing poses a significant threat to civilian GNSS applications. Hence, spoofing detection and mitigation has become an active area of research [1–5]. The authentic GNSS signal sourced from a satellite Space Vehicle (SV) is very weak at the location of the terrestrial receiver and is therefore vulnerable to hostile jamming based on narrowband noise transmission [1]. As the GNSS frequency band is known to the jammer, its effectiveness is easily optimized by confining its radiation to within the relatively narrow GNSS signal bands of interest. The transmit power requirements of a jammer placed several kilometers away from the GNSS receiver is modest with several Watts Equivalent Isotropically Radiated Power (EIRP) being sufficient to deny the GNSS receiver of any reliable pseudorange estimates. There are several means of mitigation of such noise jammers, namely:

1. **Increased processing gain based on using longer coherent integration times -** The processing gain of the GNSS spread spectrum receiver is given as the product of the bandwidth of the complex baseband signal and the coherent integration interval which can in principle be increased arbitrarily. However, there are a couple of limiting factors including unknown navigation data bits and receiver dynamics that practically restrict coherent integration gain. In dynamic platform scenarios, a minimum update rate must be maintained limiting the coherent integration interval. Considering a high dynamic case where a 1 ms update rate is required based on a GPS C/A signal with bandwidth of about 1 MHz then the processing gain is limited to about 30 dB. Hence, a jammer power of only −100 dBm at the GPS receiver antenna output will result in a signal to jammer ratio of approximately 0 dB which is insufficient.
2. **Adaptive null steering -** GNSS receivers equipped with multiple antennas can be utilized to detect jamming signals [2, 3]. Adaptive null steering that suppresses the jamming signal can then be implemented. As GNSS signals are approximately mutually orthogonal, adaptive processing can be applied to each SV signal independently with a minimum of two antennas required to null out the jammer in line of sight (LOS) conditions [6]. The depth of the achievable null of an array is a function of the platform dynamics of the jammer and GNSS receiver. In static scenarios 40 to 50 dB of nulling is possible, however very precise phasing of the antennas is required. A further disadvantage of array nulling is the required physical separation of the receiver antennas, which dominates the overall size of the receiver.
3. **GNSS diversity -** Recently more sources of GNSS signals have become available in different frequency bands which the receiver can exploit by limiting observables to signals that are not jammed. However, the jammer can easily counter this by simultaneously radiating noise in the various relevant GNSS bands.

NAVIGATION: *Journal of The Institute of Navigation*
Vol. 58, No. 4, Winter 2011
*Printed in the U.S.A.*

4. **Navigation diversity -** The user of the GNSS receiver may have alternate means of navigation which will be used instead of the compromised GNSS outputs, provided that the jammer is detected in the first place.
5. **Physically disabling jammer -** Ultimately the jammer can be located by various means and physically disabled.

While noise jamming of the GNSS receiver is a threat, the user is easily aware of its existence and characteristics, with the worst case being that GNSS based navigation is denied. A more significant threat that is currently emerging is that of the spoofing threat where bogus signals are transmitted from the jammer that emulate authentic GNSS signals. This is done with multiple SV signals in a coordinated fashion to synthesize a plausible navigation solution to the GNSS receiver. The objective of the jammer is then to cause the navigation solution as generated by the GNSS receiver to drift away from the true position. The drift is carefully orchestrated such that the GNSS receiver is unaware that it is being spoofed. The consequence of a drifting navigation solution believed to be authentic is generally more dire than the case of denied GNSS navigation that the user is aware of. Fortunately, spoofing is often detectable as the bogus SV signals generated by the jammer correspond to a navigation solution that is unexpected or implausible based on additional information available to the receiver [3]. Furthermore, to be effective, the bogus navigation solution synthesized by the jammer has to sweep through the truth solution currently tracked by the GNSS receiver and capture it similar to the classical range gate pull off methods applied to radar jamming [7]. The GNSS receiver tracking filter can further incorporate multiple ancillary sensor signals in addition to the GNSS signals to verify the likelihood of the computed navigation solution being accurate [4].

An exploitable weakness of spoofing is that for practical deployment reasons, spoofing signals generally come from a common transmitter source. Hence, a single jamming antenna sources the spoofing signals simultaneously. This results in a means of possible discrimination between the real and bogus GNSS signals as the authentic GNSS signals will emanate from known bearings distributed across the hemisphere. Furthermore, the bearing of the jammer as seen from the GNSS receiver will be different than the bearing to any of the tracked SVs. This provides the receiver with some real-time means of discriminating between the authentic and spoofing sourced GNSS signals and ultimately preventing spoofing signals from biasing the receiver navigation solution. These discrimination methods include:

1. Processing can be built into the GNSS receiver that estimates the bearing of each of the SV signals. Note that the relative bearings of the GNSS signals are sufficient in this case as the bogus GNSS signals will all have a common bearing while the authentic GNSS signals will always be at different bearings known from the ephemeris data and the approximate GPS time. If the GNSS bearings are not consistent with the expected distribution, then an alarm can be generated indicating the possibility of spoofing signals.
2. Unobstructed SV signals will reach the GNSS receiver with a signal strength that is known within a small range. If the received signal is significantly stronger than expected then spoofing can be suspected. If the spoofing signal is too weak it will not capture the GNSS receiver tracking.
3. If the GNSS receiver has multiple antennas and if the position of the antennas is such that there is an unobstructed line of sight (LOS) to the SVs then there are possibilities of detection of the spoofing signals based on the common bearing of the received GNSS signals and elimination of all the jammer signals simultaneously by appropriate combining of the receiver antennas to form a pattern null coincident with the jammer bearing as in the noise jammer case considered earlier.

Unfortunately, discrimination based on GNSS bearing is not an option when the jammer signal or SV signals are subjected to spatial multipath fading. In this case, the perceived bearings of the jammer and individual SV signals are random with unreliable correlation with the actual bearing. Furthermore, there may be multiple simultaneous bearings of each GNSS signal in a multipath fading case such that adaptive nulling fails. Another problem is that if the GNSS receiver is constrained by the form factor of a small handset device, an antenna array is not an option. As the carrier wavelength of GNSS signals is on the order of 18 to 25 cm, at most two antennas can be considered for the handset receiver which can be considered as an interferometer that has some ability of relative signal bearing estimation as well as nulling at specific bearings. However, such an antenna pair is not well represented by independent isotropic field sampling nodes but will be significantly coupled and strongly influenced by the arbitrary orientation that the user dynamically imposes. Hence, the handset antenna is poorly suited for discrimination of the spoofing signal based on bearing. Furthermore, the handheld receiver is typically

used in areas of multipath or foliage attenuation and therefore the SV signal bearing and strength are random with significant variation. However, as will be developed and demonstrated in this paper, effective spoofing detection is still possible for a single antenna GNSS receiver, even in multipath environments where conventional methods based on bearing estimation would fail. The basic assumption is that a single handheld antenna is spatially moving as it is collecting a snapshot of the GNSS signals. Hence, the moving antenna generates a signal snapshot output similar to that of a synthetic array (SA) [8, 9] which, under some additional constraints, is able to provide an effective means of discriminating between authentic and jammer sourced GNSS signals. The essence of this discrimination is based on determining the differences in spatial correlation of the snapshot signal rather than relying on bearing estimation via beamforming.

## SYSTEM DESCRIPTION

Consider the GNSS handset receiver shown in Figure 1 consisting of a single antenna that is spatially translated in time along an arbitrary trajectory as the signal is processed by the GNSS receiver. There are $L$ authentic GNSS SV signals that the receiver can see along with a jammer source that transmits spoofing replicas of the same $L$ authentic signals. It is assumed that the number of spoofed signals ranges from 1 to $L$ which are coordinated such that they correspond to a realistic but deceptive navigation solution at the output of the receiver processing. For each of the $L$ GNSS PRNs, there is the potential of a pair of despread signals as indicated in Figure 1. The pair of signals will correspond to the authentic and spoofing sources. Clearly the existence of a full set of $L$ pairs of despread outputs is a strong indication of the presence of spoofing. This can of course be used as a warning to the user. However, there are issues with this. The pair for a given GNSS signal consisting of an authentic and spoofing signal will only result when 1) the jammer is transmitting a spoofing signal for the specific GNSS code, 2) the receiver acquisition has searched over a suitable range in code delay and Doppler to despread both the spoofing signal and the authentic signal, 3) the Doppler and code delay of the spoofer and authentic signals are sufficiently separated such that distinguishable correlation peaks results in the despreading processing, and 4) the spoofing and authentic signals are not blocked from reaching the receiver antenna. On the other hand, a pair can be complete with only the existence of the authentic signal if it is subject to multipath distortion resulting in two or more resolvable correlation peaks in the despreading processor. Consequently, there are many reasons why reliance on the detection of pairs at each of the $L$ GNSS signals is not generally a reliable indication of the existence of a spoofing source.

In this paper, it will be assumed that the receiver will search for $L$ potentially visible GNSS signals. The despreading process will track the correlation peaks in small search windows around the $L$ GNSS signals such that the authentic and spoofing signals will be simultaneously tracked if they exist and are suitably resolvable. As will be discussed later, it is not strictly necessary that the spoofer and authen-

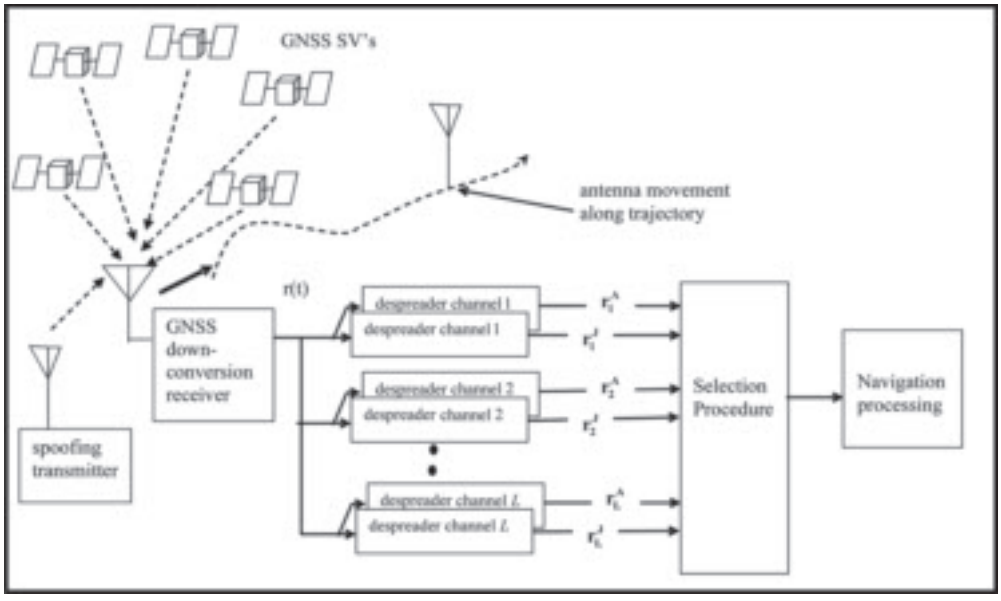


*Fig. 1–2*L *parallel despreading channels estimating signal parameters of* L *authentic and* L *spoofing signals while a single antenna is moved along an arbitrary trajectory*

tic signals be resolvable in order to successfully detect the spoofing condition. This is an important attribute as the objective of the coordinated spoofing jamming is to sweep the $L$ GNSS signals through the same code delay and Doppler point as the $L$ authentic signals, capturing the navigation tracking point. The resulting pairs of despread and tracked signals shown in Figure 1 are then individually tested for authenticity. Ideally, the $L$ authentic signals will be segregated as the set of signals used by the navigation processor. These signal discrimination decisions are based on observations of the tracked GNSS signals as the antenna is spatially moved through the trajectory.

The complex baseband signal at the output of the antenna, denoted by $r(t)$, can be expressed as [10]

$$r(t) = \sum_{i=1}^{L} A_{A,i}(\mathbf{p}(t),t)c_i(t-\tau_{A,i})d_{A,i}(t-\tau_{A,i})e^{j2\pi f_{d,A,i}t} + \sum_{i=1}^{L} A_{J,i}(\mathbf{p}(t),t)c_i(t-\tau_{J,i})d_{J,i}(t-\tau_{J,i})e^{j2\pi f_{d,J,i}t} + w(t) \quad (1)$$

wheres $A_{A,i}(\mathbf{p}(t),t)$ and $A_{J,i}(\mathbf{p},t)$ represent the $i^{\text{th}}$ channel gain for authentic and spoofing GNSS, respectively. The physical position of the phase center of the antenna at the time $t$ is denoted by $\mathbf{p}(t)$. $c_i(t)$ is spread spectrum coding modulation, $\tau_{A,i}$ and $\tau_{J,i}$ indicate code delay of $i^{\text{th}}$ SV signal of authentic and spoofing signals, $d_{A,i}$ and $d_{J,i}$ represent the navigation bit corresponding to authentic and spoofing signals, $f_{d,A,i}$ and $f_{d,J,i}$ are the Doppler frequency of the $i^{\text{th}}$ SV signal, and $w(t)$ is the complex baseband representation of the additive channel and receiver noise that is independent of the demodulated GNSS signal.

For convenience, it is assumed that the signal index $i \in [1,2,\ldots,L]$ is the same for the spoofing and authentic GNSS signals. The spoofer being aware of which signals are potentially visible to the receiver will transmit up to $L$ different spoofing signals out of this set. The objective of the despreading operation of the receiver is to isolate the channel gains, $A_{A,i}(\mathbf{p},t)$, which are raw observables that are used in the subsequent navigation tracking processing. The despreading operation is based on the multiplication of $c_i^*(t-\tau_i)d_i^*(t-\tau_i)\exp(-j2\pi f_{di}t)$ where * denotes the complex conjugate followed by a low pass filter operation denoted as $LPF\{\}$ which has a bandwidth much smaller than the bandwidth of $c_i^*(t)$ but larger than that of the channel gain fluctuations. The two outcomes of the $i^{\text{th}}$ despreading channel are denoted as $r_i^A(t)$ and $r_i^J(t)$ which are expressed as

$$\begin{aligned} r_i^A(t) &= LPF\{r(t)c_i^*(t-\tau_{A,i})\exp(-j2\pi f_{d,A,i}t)\} \\ &\approx A_i^A(\mathbf{p}(t),t)d_i^A(t) + w_i^A(t) \end{aligned} \quad (2)$$

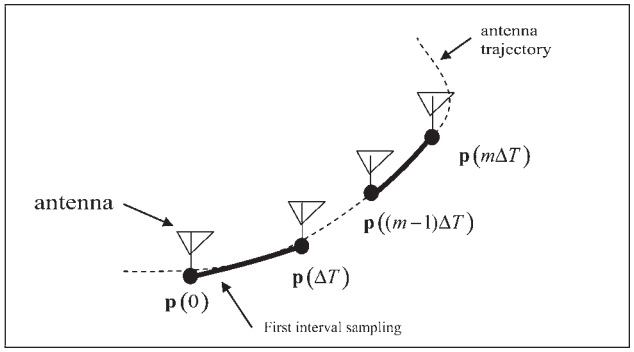


*Fig. 2–Spatial sampling of the synthetic array into* M *subinterval segments*

and

$$\begin{aligned} r_i^J(t) &= LPF\{r(t)c_i^*(t-\tau_{J,i})\exp(-j2\pi f_{d,J,i}t)\} \\ &\approx A_i^J(\mathbf{p}(t),t)d_i^J(t) + w_i^J(t) \end{aligned} \quad (3)$$

where $w_i^A(t)$ and $w_i^J(t)$ are given as

$$w_i^A(t) = LPF\{w(t)c_i^*(t-\tau_{A,i})\exp(-j2\pi f_{d,A,i}t)\} \quad (4)$$

and

$$w_i^J(t) = LPF\{w(t)c_i^*(t-\tau_{J,i})\exp(-j2\pi f_{d,J,i}t)\} \quad (5)$$

As indicated in Figure 1, it is assumed that there are $2L$ despreader channels simultaneously processing the authentic and spoofing GNSS signals. In this formulation it is assumed that the data coding, code phase of the spreading signal, and Doppler are known inputs in the despreading operation. Justification of this simplification is based on the assumption that the GNSS receiver is in a state of tracking the $L$ available GNSS signals. Also the despreading channels are arranged in pairs with labels $A$ and $J$ representing the authentic and jammer outputs, respectively. This notation is used for convenience and not to imply that the receiver has knowledge of which of the pair of GNSS signals corresponds to the authentic or spoofer cases. The data selection processing block, tests the $2L$ candidate signals for authenticity and then selects the $L$ most likely authentic signals that are then passed to the navigation processing.

The despread signals, $r_i^A(t)$ and $r_i^J(t)$, are collected over a snapshot interval of $t \in [0,T]$. As the notation is simplified if discrete samples are considered, this interval is divided into $M$ subintervals each of duration $\Delta T$ such that the $m^{\text{th}}$ subinterval extends over the interval of $[(m-1)\Delta T, m\Delta T]$ for $m \in [1,2,\ldots,M]$. The collection of signals over the first and $m^{\text{th}}$ subintervals is illustrated in Figure 2. $\Delta T$ is considered to be sufficiently small such that $A_i^A(\mathbf{p}(t),t)$ or $A_i^J(\mathbf{p}(t),t)$ is approximately constant over this interval leading a set of $M$ discrete samples for each

despreading output. Define $r^A_{m,i}$ as the $m^{\text{th}}$ time sample of the $i^{\text{th}}$ despreader channel for the authentic GNSS signal such that

$$r^A_{m,i} = \frac{1}{\Delta T}\int_{(m-1)\Delta t}^{m\Delta T} r_i(t|H0)dt$$
$$\approx A_{A,i}(\mathbf{p}(m\Delta t), m\Delta t)d_{A,i}(m\Delta t) + w^A_i(m\Delta t). \quad (6)$$

Likewise $r^J_{m,i}$ is defined for the jammer despreading channel as

$$r^J_{m,i} = \frac{1}{\Delta T}\int_{(m-1)\Delta t}^{m\Delta T} r_i(t|H1)dt$$
$$\approx A_{J,i}(\mathbf{p}(m\Delta t), m\Delta t)d_{J,i}(m\Delta t) + w^J_i(m\Delta t). \quad (7)$$

The following vector forms of the sample sets are introduced for notational convenience as

$$\mathbf{r^A_i} = \left[r^A_{0,i}, ..., r^A_{M-1,i}\right]^T$$
$$\mathbf{a}_{A,i} = \left[A_{A,i}(\mathbf{p}(\Delta T), \Delta T), ..., A_{A,i}(\mathbf{p}(M\Delta T), M\Delta T)\right]^T$$
$$\mathbf{a}_{J,i} = \left[A_{J,i}(\mathbf{p}(\Delta T), \Delta T), ..., A_{J,i}(\mathbf{p}(M\Delta T), M\Delta T)\right]^T$$
$$\mathbf{w}_i = [w_i(\Delta T), ..., w_i(M\Delta T)]^T$$

where the superscript $T$ (in this context) denotes transpose. With these definitions, the detection problem is stated as

$$\mathbf{r}_i = \begin{cases} \mathbf{a_J}_{,i} + \mathbf{w}_i & under\, H_1 \\ \mathbf{a_A}_{,i} + \mathbf{w}_i & under\, H_0 \end{cases}. \quad (9)$$

It is convenient to express the overall amplitude scaling of the authentic and jammer signals such that the channel gain vectors can be normalized as

$$E\left[\mathbf{a_i^{J,}}^H\mathbf{a_i^J}\right] = 1$$
$$E\left[\mathbf{a_i^{A,}}^H\mathbf{a_i^A}\right] = 1 \quad (10)$$

where $E[\ ]$ denotes the expected value and the superscript $H$ denotes the Hermitian transpose. With this normalization, $\mathbf{a_i^A}$ represents the instance of the array manifold vector for the GNSS signal of the $i^{\text{th}}$ SV as the antenna is moved through its trajectory. Likewise $\mathbf{a_i^J}$ represents the instance of the array manifold vector for the $i^{\text{th}}$ GNSS signal generated by the spoofer.

## SINGLE SNAPSHOT DETECTION HYPOTHESIS STATEMENT

The central tenet of the proposed spoofing detection is that the array manifold vector for the jammer, $\mathbf{a_i^J}$, will be the same for all of the $L$ GNSS signals while the array manifold vector for the authentic signals, $\mathbf{a_i^A}$, will be different for each of the $L$ authentic signals. If the random antenna trajectory is of sufficient length, then the authentic signal array manifold vectors will be uncorrelated such that

$$E\left[\mathbf{a_i^{A,}}^H\mathbf{a_j^A}\right] \approx \delta_{ij} \quad for \quad 1 \le i,j \le L. \quad (11)$$

On the other hand, as the jammer signals emerge from the same source they will all have the same array manifold vector regardless of the random antenna trajectory and also regardless of the spatial fading conditions present. Hence,

$$E\left[\mathbf{a_i^{J,}}^H\mathbf{a_j^J}\right] \approx 1 \quad for \quad 1 \le i,j \le L. \quad (12)$$

This would indicate that a method of detecting that a spoofer is present is to form the $M \times 2L$ data matrix of all of the $L$ pairs of channel vectors denoted by $\mathbf{A}$ and given as

$$\mathbf{A} = \left[\left\{\mathbf{a_1^J}\ \ \mathbf{a_1^A}\right\}\ \ \left\{\mathbf{a_2^J}\ \ \mathbf{a_2^A}\right\}\ \ \cdots\ \ \left\{\mathbf{a_L^J}\ \ \mathbf{a_L^A}\right\}\right]. \quad (13)$$

Note that some of the columns may be zero where the signal pairs do not exist. Also the receiver does not know which column of each of the pairs corresponds to the authentic or the jammer components. Finally, it is assumed that the number of trajectory samples is such that $M \ge 2L$.

Initially assuming that the $L$ pairs are complete, then $\mathbf{A}$ will have $2L$ singular values. If there is a dominant singular value of value $\sqrt{L}$ times larger than the other singular values and $L - 1$ singular values close to zero then this is an indication that $L$ of the array manifold vectors are closely collinear differing only by a scaling constant which is indicative of the spoofing threat. The receiver having detected the likelihood of a spoofer can then proceed to sort the pairs of sample vectors to separate the authentic set from the spoofing set. A possible method could be to remove the rightmost vector of $\mathbf{A}$ and then recalculate the singular components. If the maximum singular value decreases slightly by a ratio $\sqrt{(L-1)/L}$ and one of the singular values near zero disappears, then the removed manifold vector corresponds to a spoofing signal. If the maximum singular value remains at the same level and the number of singular values remains the same then the manifold vector corresponds to an authentic signal. Once the identity of the removed vector has been identified it is reinserted into $\mathbf{A}$ and another vector from a different pair is removed and identified with the same procedure.

Unfortunately there are issues with this simple direct method that will affect the detectability of

the spoofing signals. As the spoofer is attempting to pull the tracking point off of the authentic signals, the spoofer and authentic signals for a period of time will have approximately the same code offset and Doppler. Consequently, during this time the corresponding manifold vectors of $\mathbf{a_i^A}$ and $\mathbf{a_i^J}$ will add into a superposition manifold vector for the $i^{\text{th}}$ GNSS signal such that $\mathbf{a_i^A}$ and $\mathbf{a_i^J}$ cannot be extracted. Essentially the two signal vectors of the pair will degenerate into a single output with the other component of the pair being zero. Also the additive noise in the despreading outputs will reduce the correlation amount of the spoofing signals such that the smallest $L$-1 singular values will be further from zero. Finally, as stated earlier, the assumption of $L$ pairs is not reliable. Some of the $L$ expected authentic SV signals may not be present due to shadowing of particular sectors of the sky. In addition, the spoofer is unpredictable and may only transmit a subset of the $L$ possible GNSS signals.

Due to these issues, direct application of the SVD based algorithm is unlikely to provide robust spoofing detection and signal sorting. Fundamentally what can be assumed is that, if there is a spoofer from a common source that transmits more than one GNSS signal simultaneously, there will be some spatial correlation of the observables of $\mathbf{a_i^J}$ with other despreader outputs of the receiver. Therefore, if operations of pairwise correlations of all of the $2L$ despreader outputs result in cases of high pairwise correlation then there is a corresponding high likelihood of the existence of spoofing signals. These pairwise correlations can also be used to sort the spoofing from the authentic signals. Two additional factors make pairwise correlation testing attractive. First, during the time when the spoofing and authentic signals have the same Doppler and code offset such that the $\mathbf{a_i^A}$ and $\mathbf{a_i^J}$ degenerate into a single vector, a partial correlation exists with other spoofing vectors that may also have combined with the corresponding authentic vector of the pair. Secondly, the pairwise correlation is not affected by spatial multipath fading which will be discussed later.

Consider the problem of taking two output vectors from the set of $2L$ possible despreader outputs from different signal pairs. These are arranged into an $M \times 2$ sample matrix denoted as $\mathbf{r}$. The $m^{\text{th}}$ row of $\mathbf{r}$ is denoted as $\mathbf{r_m}$ such that $\mathbf{r}$ can be expressed as

$$\mathbf{r} = \begin{bmatrix} \mathbf{r}_0 \\ \mathbf{r}_1 \\ \vdots \\ \mathbf{r}_{M-1} \end{bmatrix} = \begin{bmatrix} r_{0,0} & r_{1,0} \\ r_{0,1} & r_{1,1} \\ \vdots & \vdots \\ r_{0,M-1} & r_{1,M-1} \end{bmatrix}. \tag{14}$$

It will be assumed that the trajectory and spatial multipath fading is random and stationary such that the sequences of $r_{0,m}$ and $r_{1,m}$ can be approximated as wide sense stationary discrete random sequences. Essentially there are two states. $H_0$ denotes the case where there is no correlation between the pair of selected despreading vectors and $H_1$ is the case where there is some correlation. $H_1$ would only occur if the two selected vectors were from the same spoofing source. $H_0$ would occur if the vectors are from the set of authentic signals or if one of the pairs was an authentic signal and the other was a spoofing signal.

Based on the validity of these assumptions each of the sample pairs of $\mathbf{r_m}$ in (14) are bivariate circularly normal (CN) with zero mean and a covariance matrix denoted by $\mathbf{C}$ which is conditioned on the source state $H_0$ and $H_1$ as

$$\mathbf{C} = E\left[\mathbf{r}_i^T \mathbf{r}_i\right] = \begin{cases} \mathbf{C_0} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & under\, H_0 \\ \mathbf{C_1} = \begin{bmatrix} 1 & \rho \\ \rho & 1 \end{bmatrix} & under\, H_1 \end{cases} \tag{15}$$

for $i \in [0,..M-1]$ and where $\rho$ is the correlation coefficient. $\rho$ is the single parameter that distinguishes between the two states $H_0$ and $H_1$ given $\mathbf{r}$. Consider $\rho$ as a parameter such that the log likelihood ratio (LLR) of the conditional PDFs results in the test statistic, denoted as $T(\mathbf{r}; \rho)$ which is given as

$$T(\mathbf{r}; \rho) = \ln \frac{f_{\mathbf{r};\rho|H1}(\mathbf{r})}{f_{\mathbf{r}|H0}(\mathbf{r})}. \tag{16}$$

As each of the rows of data in $\mathbf{r}$ is independent, then $T(\mathbf{r}; \rho)$ can be expressed as

$$T(\mathbf{r}; \rho) = \frac{N}{2} \left| \frac{\mathbf{C_0}}{\mathbf{C_1}(\rho)} \right| + \frac{1}{2} \sum_{n=0}^{N-1} \mathbf{r}_\mathbf{n}^T \left( \mathbf{C_0}^{-1} - \mathbf{C_1}(\rho)^{-1} \right) \mathbf{r_n}. \tag{17}$$

The first term does not involve the data and may therefore be discarded leaving

$$T(\mathbf{r}; \rho) = \tfrac{1}{2} \sum_{n=0}^{M-1} \mathbf{r}_\mathbf{n}^T \left( \mathbf{C_0}^{-1} - \mathbf{C_1}(\rho)^{-1} \right) \mathbf{r_n} \tag{18}$$

which is expanded and stripped of unnecessary scaling and additive constants resulting in

$$T(\mathbf{r}; \rho) = \sum_{n=0}^{M-1} \left( \frac{2 r_{0,n} \ r_{1,n}}{\rho} - r_{0,n}^2 - r_{1,n}^2 \right). \tag{19}$$

Note that the PDF of $T(\mathbf{r}; \rho)$ conditioned on either $H_0$ or $H_1$ cannot be expressed in closed form and must therefore be numerically determined. This makes it difficult to set a threshold that $T(\mathbf{r}; \rho)$ can be compared against to decode $H_0$ or $H_1$. Furthermore, in all practical applications $\rho$ will be unknown. The conventional approach is to generate a suboptimal test statistic based on the generalized LRT (GLRT) formulation which is expressed as

$$T(\mathbf{r}) = \ln \frac{f(\mathbf{r}|\widehat{\rho}(\mathbf{r}), H1)}{f(\mathbf{r}|H0)} \tag{20}$$

where $\widehat{\rho}(\mathbf{r})$ is the maximum likely estimate (MLE) of $\rho$ based on the data samples in $\mathbf{r}$. The GLRT is not applicable for the present case as the MLE of $\rho$ results in an expression that is independent of $\mathbf{r}$. An alternate approach is to use an asymptotic form of the GLRT, resulting in the Wald test [11]. Essentially the Wald test results in the intuitive approach of generating the MLE estimate of $\widehat{\rho}(\mathbf{r})$ and then using this directly as a measure of the likelihood of $H_1$ as opposed to $H_0$. This likelihood measure can then subsequently be compared against a threshold for a hard decoded decision regarding the correlation of the pair of signals. Note that the optimum threshold depends on various factors such as SNR and the coherency between the suites of spoofing signals. At this point the threshold level is determined experimentally. Furthermore, for a given signal to be considered to be sourced by a spoofer, multiple pairwise correlations can be done with signals from other GNSS signals. Hence an accumulation of MLE correlation estimates from each of the possible correlations can be the threshold for a better performing detector. The pairwise correlation method is summarized as follows:

1. Data vectors can be sorted into two groups. The $J$ group is the data set that is highly correlated and the $A$ group is the set that is uncorrelated. Note that the trajectory is assumed to be sufficiently large such that the array manifold vector associated with the authentic signals from different sky bearings are approximately orthogonal. In other words, the equivalent beamwidth of a synthetic array composed from the trajectory can sufficiently resolve the various GNSS satellite signals.
2. The $A$ group will be constrained in size base on the number of observable GNSS satellites. Usually this is known and $L$ can be set. Note that the receiver has control over this by setting the bank of despreaders. If an SV signal is known to be unobtainable due to position in the sky it is eliminated by the receiver. Hence the $A$ group can be assumed to be constrained in size to $L$. The overall objective is to minimize errors where authentic signals are discarded by incorrectly placing them in the $J$ group and where spoofing signals are erroneously placed in the $A$ group resulting in a biased navigation solution.
3. A further option is for the navigation solution to create two solutions, one corresponding to the $A$ group and the other corresponding to the $J$ group. Individual members of either group can be tested for integrity to determine if their code delays and Doppler values correspond to the computed navigation solution.
4. The proper placement of the members in the $J$ and $A$ groups can also be continuously assessed as the set of members in the $A$ group should provide the lowest variance navigation solution. Hence in general there will be a spoofing and authentic signal that corresponds to the GNSS signal of index $i$. If the spoofing signal in group $J$ appears to have marginal correlation with its peers in group $A$ and, when interchanged with its corresponding signal in the $A$ group, it generates a lower variance navigation solution, then an exchange should be made.

## EXPERIMENTAL RESULTS

Experimental results of spoofing detection based on utilizing a single antenna that is spatially translated will be given in this section. Two measurement scenarios will be given with the aim of demonstrating the practicality of detecting a spoofing signal based on the spatial signal correlation discriminator introduced in the previous section. The experimental measurements are based on the reception of GPS L1 C/A signals.

### *Data Collection of Spoofing Signals Under Non-Line-of-Sight Conditions*

The first measurements were directed to analyze the behavior of the spoofing signal initiated from a single source antenna and were conducted inside a modern three story commercial building. The layout of the office and lab facilities are given in Figure 3. The dark grey triangular symbol labeled '$T_x$' is the location of the spoofing source. The light grey triangular symbol labeled '$R_x$' is the location of the receiver which is moved along the dashed line. The signals for the spoofing transmission were generated by a Spirent hardware simulator (HWS) which were radiated for a few minutes by a highly directional antenna downward to affect only a small area of the laboratory. At the particular instance of the measurements, the SVs were distributed as per the sky plot shown in Figure 4. The intention of this indoor setup of the spoofing source was to generate NLOS propagation conditions with significant multipath. The GNSS receiver consisted of an active patch Right-Hand Circular Polarized (RHCP) antenna and a National Instrument down conversion channelizer receiver that sampled the raw complex baseband signal $r(t)$. The total data record was subsequently processed and consisted of acquiring the correlation peak based on 20 ms coherent integration of the GNSS spoofing signals and extracting the channel gains $\mathbf{a}_{\mathbf{J},i}$ as a function of time.

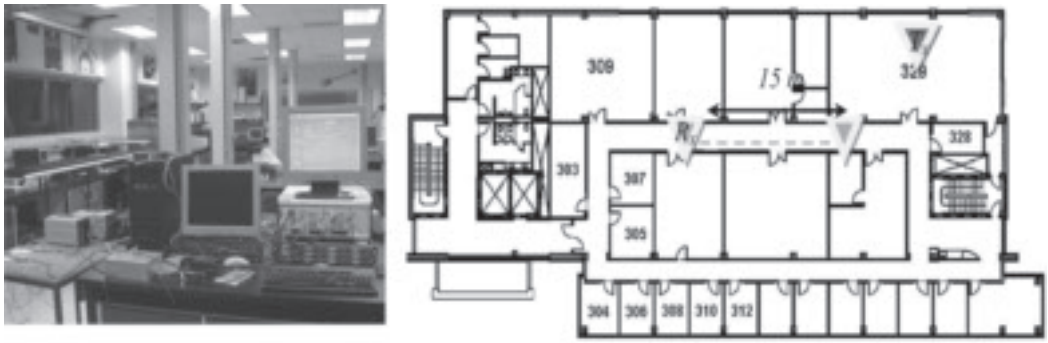


*Fig. 3–a) Indoor laboratory facilities and data collection location, b) Floor plan indicating the location of the spoofing source by* $T_x$ *and receiver by* $R_x$

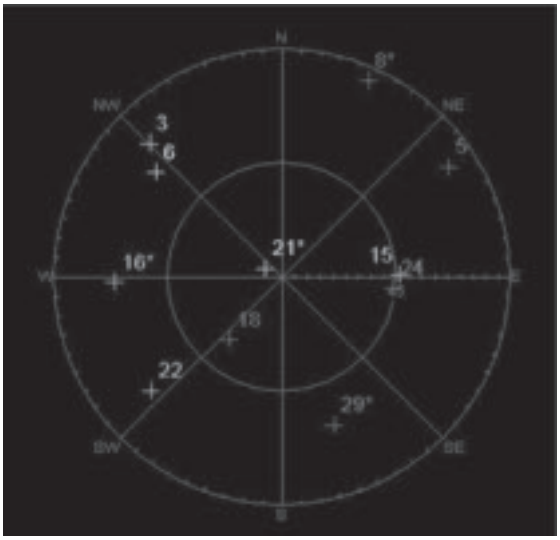


*Fig. 4–Sky plot of transmitted spoofing GNSS signals as simulated by the spirent HWS*

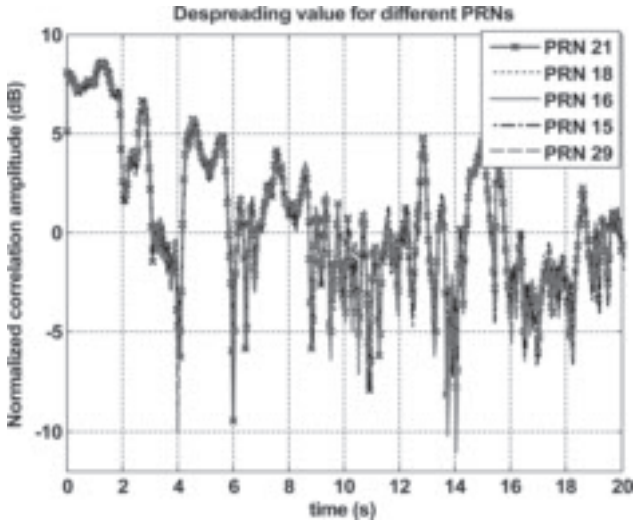


*Fig. 5–Normalized amplitude value of the correlation function for different PRNs generated from the same antenna*

Figure 5 shows a plot of the samples of the magnitude of $\mathbf{r}_i$ for the various SV signals generated by the spoofing threat. Note that the magnitudes of the $\mathbf{r}_i$ values are obviously highly correlated as expected since the jammer signals are all emanating from a common antenna. Also the SNR values are high, indicating that the decorrelation due to the channel noise is not significant.

The correlation of the various spoofing signals can be quantified based on the standard numerical estimate of the correlation coefficient given as

$$\rho_{ij} = \frac{E\left[\mathbf{r}_i \mathbf{r}_j^H\right]}{\sqrt{E\left[\mathbf{r}_i \mathbf{r}_i^H\right]}\sqrt{E\left[\mathbf{r}_j \mathbf{r}_j^H\right]}}. \qquad (21)$$

These are calculated for the measurement results represented in Figure 5 and tabulated in Table 1. As evident, and as expected, the correlations are all very high. This is anticipated as the spoofing signals all occupy the same frequency band with the exception of small incidental shifts due to the SV Doppler values.

Table 1—Correlation Coefficient Determined for the Set of Transmitted Spoofing Signals

| PRN | 21 | 18 | 16 | 15 | 29 |
|---|---|---|---|---|---|
| 21 | 1 | 0.98 | 0.98 | 0.96 | 0.98 |
| 18 | 0.98 | 1 | 0.97 | 0.94 | 0.97 |
| 16 | 0.98 | 0.97 | 1 | 0.98 | 0.99 |
| 15 | 0.96 | 0.94 | 0.98 | 1 | 0.98 |
| 19 | 0.98 | 0.96 | 0.99 | 0.98 | 1 |

### *Data Collection of Authentic and Jamming Signals Under LOS Conditions*

For this measurement, the Spirent HWS signal was radiated for a few brief periods from the same highly directional antenna transmitting downward

*Fig. 6–Rooftop mounting of HWS spoofer transmitter*

in order to cover a 4 m × 4 m area of the building roof as shown in Figure 6, hereby avoiding any effect outside the test area. Three PRNs with false navigation messages were propagated. The GPS receiver consisted of the same active GPS patch antenna used in the previous measurement as well as a National Instrument channelizer. During the data collection process the antenna was randomly moved by hand along an arbitrary trajectory. The received complex baseband signal was collected over a time interval of several seconds, which consisted of a superposition of authentic signals from the visible SVs as well as the spoofing signal. Figure 7 shows the correlation output of the authentic GPS SV signal in addition to the correlation peak of the spoofing signal programmed to synthesize a spoofing replica. Two detectable peaks corresponding to the authentic and the spoofer signals are clearly resolvable and would constitute a tracked signal pair.

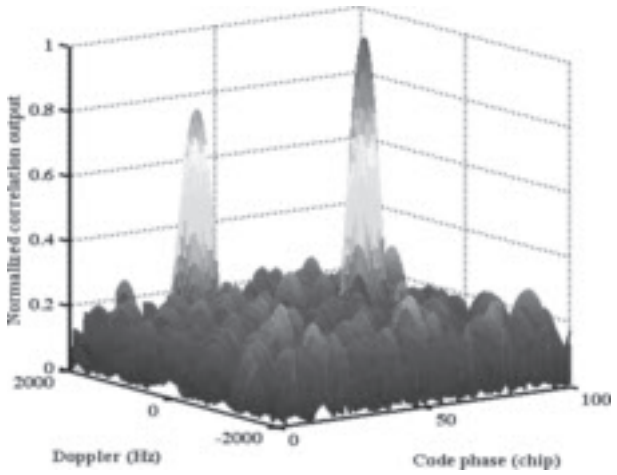


*Fig. 7–Correlation output of authentic GPSPRN 4 in the presence of a spoofing*

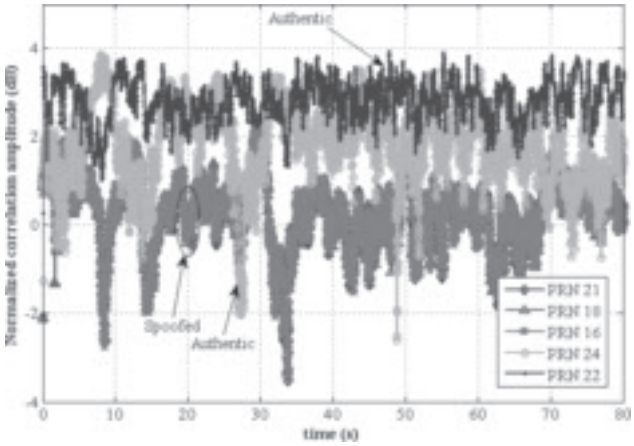


*Fig. 8–Magnitude of the correlation function for the spoofed and the authentic GPS signals*

Table 2—Correlation Coefficient for Different PRNS

| PRN | 21 | 18 | 16 | 22 | 24 |
|---|---|---|---|---|---|
| 21 | 1 | 0.89 | 0.90 | 0.22 | 0.21 |
| 18 | 0.89 | 1 | 0.83 | 0.23 | 0.19 |
| 16 | 0.90 | 0.83 | 1 | 0.21 | 0.20 |
| 22 | 0.22 | 0.23 | 0.21 | 1 | 0.23 |
| 24 | 0.21 | 0.19 | 0.20 | 0.23 | 1 |

Figure 8 shows the magnitude of the correlation peaks of different SV signals generated from the spoofer (PRNs 16, 18, and 21) as the receiver antenna was randomly moved. As evident, the channel gains of the set of spoofer signals during the measurement interval are highly correlated. This is expected as the spoofing signals are all radiated from the same location via the antenna in Figure 6. Figure 8 also shows the channel gains of the authentic SV signals that were present during the measurement interval (PRNs 22 and 24) overlaid with the spoofing signals. Note that the channel gain functions of the authentic SV signals are uncorrelated over the measurement interval while the spoofing signal channel gains are highly correlated. Also note that the authentic and spoofing signal channel gains are mutually uncorrelated as expected since the spoofing transmitter is at a different bearing than any of the visible SVs.

Table 2 shows the magnitude of the correlation coefficients for the set of authentic SVs as calculated using Eq. (21). Note that, as expected, the correlation coefficients are much smaller than those shown in Table 1 for the indoor measurement case.

## CONCLUSIONS AND FUTURE WORK

It was shown herein that spoofing generated from a common source can be effectively detected by using a synthetic array antenna. Through a process of sorting the authentic and spoofing signals based

on pairwise signal correlation, it is possible to sort the signals such that only the authentic signals are passed to the navigation solution. This form of detection and mitigation of GNSS spoofing can be achieved by a single antenna handset, provided that the antenna moves during data collection. The key differentiating attribute exploited herein is that the spoofing signals are spatially correlated while the authentic signals are not. A key observation is that the detection performance of the developed method is not affected by spatial multipath fading to which the GNSS signals are subjected. Also the trajectory of the receiver antenna can be random and does not have to be jointly estimated as part of the overall spoofing detection.

## REFERENCES


1. Hartman, R. G., "Spoofing Detection for a Satellite Positioning System," *U.S. Patent 5,557,284*, 17 September 1996.
2. McDowell, C. E., GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling, *U.S. Patent 7,250,903*, 31 July 2007.
3. Montgomery, P., Humphreys, T., and Ledvina, B., "A Multi-Antenna Defense – Receiver Autonomous GPS Spoofing Detection," *InsideGNSS,* March/April 2009, pp. 40–46.
4. Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner, P. M., Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, September 2008, pp. 2314–2325.
5. Lo, S., DeLorenzo, D., Enge, P., Akos, D., and Bradley, P., "Signal Authentification, A Secure Civil GNSS for Today," *Inside GNSS*, Sept/Oct 2009, pp. 30–39.
6. Trees, H. L. V., *Optimum Array Processing, part IV, Detection, Estimation, and Modulation Theory*, John Wiley & Sons, Inc., New York, 2002.
7. Skolnik, M., *Radar Handbook*, Third Ed., McGraw Hill, 2008.
8. Broumandan, A., Nielsen, J., and Lachapelle, G., "Signal Detection Performance in Rayleigh Multipath Fading Environments with a Moving Antenna," *IET Signal Processing Journal*, May 2009.
9. Broumandan, A., Nielsen, J., and Lachapelle, G., "Performance of Narrowband Signal Detection under Correlated Rayleigh Fading based on Synthetic Array," *International Journal of Antennas and Propagation*, Vol. 2009, Article ID 610109, 13 pages.
10. Kaplan, E. D., and Hegarty, C., *Understanding GPS Principles and Applications*, 2nd Ed., Artech House, 2006.
11. Kay, S. M., *Fundamentals of Statistical Signal Processing Detection Theory*, Prentice-Hall, Inc., 1998.