GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation

Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen and Gérard Lachapelle
Schulich School of Engineering
Position Location and Navigation (PLAN) Group
http://plan.geomatics.ucalgary.ca/
University of Calgary
2500 University Drive, N.W.,Calgary, Alberta, Canada, T2N 1N4

Abstract— **poofing and jamming in the form of transmitting counterfeit location information and denying services are an emerging threat to GNSS receivers. In general, spoofing is a deliberate attack that aims to coerce GNSS receivers into generating false navigation solutions. The spoofing attack is potentially more hazardous than jamming since the target receiver is not aware of this threat and it is still providing position/navigation solutions which seem to be reliable. One major limitation of spoofers is that they are required to transmit several highly correlated GNSS signals simultaneously often from a single source in order to present a truthful navigation solution to the receiver. Different GNSS signals sourced from a single transmitter have essentially the same spatial signature, which as shown in this paper, can be utilized to discriminate the spoofing signals. In this paper a moving antenna is investigated to discriminate between the spatial signatures of the authentic and the spoofing signals based on monitoring the amplitude and Doppler correlation of the visible satellite signals. The effectiveness of this detection method is studied and verified based on a set of experiments.**

Keywords- GNSS, Moving receiver, Spatial correlation, Spoofing

I. INTRODUCTION

Comn ercial GNSS receivers are prone to jamming and spoofing transmissions. Although a power jammer can easily disrupt service and deny the user of location estimates, its presence is nevertheless detectable by the user. Most of the current attention is on narrowband noise or tone jammers that only require a very small power to be effective as the authentic GNSS signals at the terrestrial level are very weak. As stated earlier, jammers can deny the GNSS receiver capability of providing location services, however they are readily detectable by the receiver. On the other hand, a spoofing attack based on a set of synthesized GNSS signals, while not easily detectable, is an effective means of presenting bogus position estimates to the user and therefore can be more effective in various scenarios [1]-[3]. The spoofer can fabricate a counterfeit navigation solution that the receiver presumes to be legitimate [5]. For instance, a fishing vessel that operates in illegal areas, or vehicles involved in criminal activities with tracking receivers that wish to present incorrect traveled routes to the activity monitoring GNSS receiver can utilize this form of spoofing attack.

Spoofing threats can be divided into three main categories, namely GPS signal generators, intermediate receiver based spoofers and sophisticated receiver based spoofers [6]. A GPS signal generator transmits counterfeit GPS signals that are not essentially synchronized to the current GPS constellation while the receiver based spoofers first synchronize to the current authentic GPS signals and then generate the spoofing signals knowing the approximate 3D pointing vector of their transmit antenna toward the target receiver antenna. Sophisticated spoofing sources are difficult to detect [5]. The sources are weak as they are most effective if they are only of slightly higher power than the authentic GNSS signals at the receiver. Spoofing signals that are too strong are easily detected and rejected by the GNSS receiver based on straightforward signal power measurements [7]. While it is naturally difficult for the spoofer to generate appropriate signals for an urban multipath environment, it can be statistically effective and still prove to be disruptive for the GNSS receivers attempting to segregate the authentic signals from the spoofing sources.

A major limitation of spoofers is that they are required to transmit several GNSS signals simultaneously in order to present a credible navigation solution to the receiver [1]. Of course a set of spoofers can be devised to implement this with each spoofer responsible for a single GNSS signal however this is not deemed practical, as different spoofing transmitters should be synchronized precisely. In addition the cost of the spoofer infrastructure and deployment is very high for this scenario [5].

If the spoofing signals are transmitted from a single source, the wireless communication channel is shared between all of the spoofing signals and as such, these signals will be spatially correlated at the receiver [8]. This characteristic of the spoofer signal is independent of the

978-1-4673-0387-3/12/$31.00 ©2012 IEEE

channel conditions, Line of Sight (LOS), non line of sight (NLOS) and can be exploitable to detect and mitigate the spoofing attack.

For the case of spoofing signals, since different GNSS signals are sourced from a single transmitter, they have essentially the same power spectral density (with the exception of a trivially small relative Doppler shift) and have virtually the same channel gain for any space-time point. This is exploited for spoofer detection as follows. When the receiver is stationary then the authentic GNSS signals channel gains should be highly correlated relative to each other in time. However, when the receiver starts moving, the relative authentic channel gains quickly decorrelate with time. If pairs of authentic signals do not decorrelate due to antenna movement, it implies that the propagation path must be very similar, which can be verified because the true GNSS signal bearings are known if the location of the receiver and time are approximately known. With the spoofer generating simultaneous GNSS signals, the channel phases corresponding to the pairs of spoofer signals do not decorrelate with time regardless whether the GNSS receiver is moving or not. Hence, the spoofer signals behave differently than the authentic signals, which is the essence of this form of spoofer detection [9].

This paper compares the amplitude and the Doppler measurements corresponding to different PRNs as a means of detecting the spoofing signals being transmitted from a comn on bearing (indicating that a spoofer source is present). Test measurements have been performed by combining authentic signals received from a rooftop antenna with spoofing signals radiated from an indoor directional antenna and received by a spatially translated single antenna. In this test, a hardware simulator output has been used as a spoofing generator, which is radiated indoor with a controlled power level. The test results show that the proposed technique can successfully discriminate the spoofing PRNs even in multipath environments.

The rest of the paper is organized as follows. Section II describes authentic and spoofing signal models and their corresponding considerations. In Section III, a spoofing detection method based on a spatial correlation is discussed. Experimental measurements and results are discussed in Section IV. Conclusions are given in Section V.

II. SIGNAL DESCRIPTION

Consider a GNSS receiver consisting of a single antenna that is spatially translated along an arbitrary trajectory as the signal is processed by the receiver. Assume that L authentic GNSS signals are visible to the receiver. Further assume that a spoofing source replicates up to L copies of the same authentic signals. Also, it is assumed that the spoofing signals are coordinated such that they correspond to a realistic navigation solution. In general, the authentic and the spoofing signals are separated in the Code-Doppler-Space (CDS).

This paper develops a technique that enables a stand-alone receiver to verify the authenticity of the GNSS signals present. Therefore, a binary detection problem is formulated based on branding each of the $2L$ signals with either of the two plausible hypotheses of authentic (H_0) and spoofing (H_1), as the antenna is spatially translated on an arbitrary trajectory.

The complex received signal is denoted by $r(t)$ [10],

$$r(t) = \sum_{i=1}^{L} \alpha_i^A(t) A_i^A(\mathbf{p}(t),t) c_i\left(t-\tau_i^A\right) d_A\left(t-\tau_i^A\right) e^{j(2\pi f_{di}^A t+\theta_i^A)} + \sum_{i=1}^{L} \alpha_i^S(t) A_i^S(\mathbf{p}(t),t) c_i\left(t-\tau_i^S\right) d_S\left(t-\tau_i^S\right) e^{j(2\pi f_{di}^S t+\theta f_{di}^S t)} + w(t) \quad (1)$$

where t is time, i indicates the index of the GNSS signals, and $\mathbf{p}(t)$ is the position vector of the phase center of the moving antenna. Note that the superscripts 'A' and 'S' represent the authentic and spoofing signals. $\alpha_i^A(t)$ and $\alpha_i^S(t)$ are random complex scintillation applied to the i-th authentic and spoofing signals, respectively. $A_i^A(\mathbf{p},t)$ and $A_i^S(\mathbf{p},t)$ are channel gains for the authentic and spoofing GNSS signals. $c_i(t)$ is the spread spectrum coding modulation of the i-th GNSS signal, and $d(t)$ indicates the navigation data bits. τ_i^A and τ_i^S are code delays of the i-th authentic and spoofing signals, respectively. f_{di}^A and f_{di}^S are the Doppler frequencies associated with the i-th authentic and spoofing signals. Finally, $w(t)$ is the additive white Gaussian noise. For convenience, it is assumed that the signal index $i \in [1,2,...,L]$ 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. Figure 1 shows the spoofing and the receiver processing scenarios.

The objective of the receiver despreading operation is to isolate the channel gains A_i^A, which are raw observables that are used in the subsequent detection algorithm. The despreading operation is based on the form $c_i^*(t-\tau_i)\, d^*(t-\tau_i) \exp\left(-j2\pi f_{d,i} t - j\theta_i\right)$ where $*$ denotes a complex conjugate. Consequently the despread authentic and spoofer signals are

$$x_i^A(t) \approx \alpha_i^A(t) A_i^A(\mathbf{p}(t),t) + \eta_i^A(t) \quad (2)$$

and

$$x_i^S(t) \approx \alpha_i^S(t) A_i^S(\mathbf{p}(t),t) + \eta_i^S(t), \quad (3)$$

Here, $\eta_i^{A/S}(t)$ are the noise terms at the output of the correlators. In this formulation it is assumed that the data coding, code phase of the spreading signal and Doppler are known a-priori.

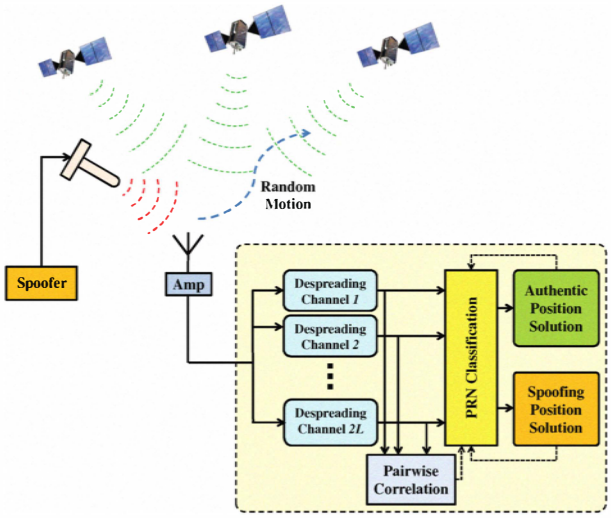

Figure 1: GNSS receiver with a single antenna and $2L$ parallel despreading channels

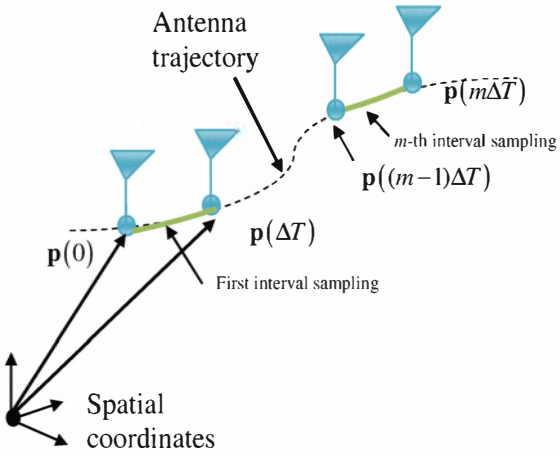

Figure 2: Spatial sampling of the antenna trajectory into M subinterval segments

Justification of this is based on the assumption that the GNSS receiver is tracking both the authentic and the spoofing signals associated with each PRN.

The despread signals, $x_i^A(t)$ and $x_i^S(t)$ 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 ΔT such that the m-th subinterval extends over the interval of $[(m-1)\Delta T, m\Delta T]$ for $m \in [1,2,...,M]$. The collection of signals over the first and m-th subintervals is illustrated in Figure 2. ΔT is considered to be sufficiently small such that $A_i^A(\mathbf{p}(t),t)$ and $A_i^S(\mathbf{p}(t),t)$ are approximately constant over this interval. Define $x_{m,i}^A$ as the m-th time sample of the i-th correlator under H_0

$$x_{m,i}^A \mid H_0 \approx A_i^A(\mathbf{p}(m\Delta t), m\Delta t)\alpha_i^A(m\Delta t) + \eta_i^A(m\Delta t). \quad (4)$$

Similarly, $x_{m,i}^S$ under H_1 can be defined as

$$x_{m,i}^S \mid H_1 \approx A_i^S(\mathbf{p}(m\Delta t), m\Delta t)\alpha_i^S(m\Delta t) + \eta_i^S(m\Delta t).. \quad (5)$$

Also let us define the following

$$\mathbf{x}_i^A = \left[x_{1,i}^A,...,x_{M,i}^A\right]^\dagger$$

$$\mathbf{a}_i^A = \left[A_i^A(\mathbf{p}(\Delta T),\Delta T),...,A_i^A(\mathbf{p}(M\Delta T),M\Delta T)\right]^\dagger$$

$$\boldsymbol{\alpha}_i^A = \left[\alpha_i^A(\Delta T),...,\alpha_i^A(M\Delta T)\right]^\dagger$$

$$\mathbf{a}_i^S = \left[A_i^S(\mathbf{p}(\Delta T),\Delta T),...,A_i^S(\mathbf{p}(M\Delta T),M\Delta T)\right]^\dagger$$

$$\boldsymbol{\alpha}_i^S = \left[\alpha_i^S(\Delta T),...,\alpha_i^S(M\Delta T)\right]^\dagger$$

$$\boldsymbol{\eta}_i^A = \left[\eta_i^A(\Delta T),...,\eta_i^A(M\Delta T)\right]^\dagger$$

$$\boldsymbol{\eta}_i^S = \left[\eta_i^S(\Delta T),...,\eta_i^S(M\Delta T)\right]^\dagger$$

where '†' denotes a matrix transpose. Consequently, the detection problem can be defined as

$$\mathbf{x}_i = \begin{cases} \mathbf{a}_i^S \odot \boldsymbol{\alpha}_i^S + \boldsymbol{\eta}_i^S = \boldsymbol{\Lambda}_i^S + \boldsymbol{\eta}_i^S & H_1 \\ \mathbf{a}_i^A \odot \boldsymbol{\alpha}_i^A + \boldsymbol{\eta}_i^A = \boldsymbol{\Lambda}_i^A + \boldsymbol{\eta}_i^A & H_0 \end{cases} \quad (6)$$

where $\odot$ denotes the Hadamard vector product operator. The scintillation $\boldsymbol{\alpha}_i^A$ is a slowly varying random process consisting of receiver clock instability. Consequently, the elements of $\boldsymbol{\alpha}_i^A$ can be construed as a set of highly correlated random variables during the snapshot period. Note that the objective of isolating the channel gain vector $\mathbf{a}_i^A$ is not possible as the available observable $\boldsymbol{\Lambda}_i^A = \mathbf{a}_i^A \odot \boldsymbol{\alpha}_i^A$ is corrupted by additive noise. Of course for the specific cases where the antenna is static and the channel is stationary, $\mathbf{a}_i = a_{oi}\mathbf{1}_\mathbf{M}$ where a_{oi} is a constant for the i-th SV channel and $\mathbf{1}_\mathbf{M}$ is a column vector of length M as $\mathbf{1}_\mathbf{M} = [1,...,1]^\dagger$.

The spoofer scintillation, $\boldsymbol{\alpha}_i^S$, on the other hand is arbitrary and unpredictable as it is set by the spoofing algorithm. If there is no scintillation applied to the spoofing signal then $\boldsymbol{\alpha}_i^S$ will include only the receiver clock instability such that the random elements of $\boldsymbol{\alpha}_i^S$ will be highly correlated. However, there could be an advantage for the spoofer of purposely applying a modest amount of random scintillation to the individual spoofing signals as this will slightly decorrelate the received spoofing signals making the discrimination of H_0 and H_1 more difficult. However, excessive scintillation to the spoofing signals allows for spoofer detection when the antenna is static. Of course the spoofer can scintillate which would cause some decorrelation, however, such scintillation is typically detrimental to the spoofer as it makes the spoofer signal detectable as such if the GNSS receiver antenna is stationary. Therefore in the remainder

of this paper it is assume that the spoofer scintillation is not effective. Based on this it is convenient to include in $\boldsymbol{\alpha}_i^A$ and $\boldsymbol{\alpha}_i^S$ the overall amplitude scaling of the authentic and spoofing signals such that the channel gain vectors can be normalized as

$$E\left[\left(\mathbf{a}_i^A\right)^H \mathbf{a}_i^A\right]=1$$
$$E\left[\left(\mathbf{a}_i^S\right)^H \mathbf{a}_i^S\right]=1 \tag{7}$$

where $E[\ ]$ denotes an expected value operator and the superscript '*H*' denotes a Hermitian transpose. With this normalization, $\mathbf{a}_i^A$ represents the instance of the moving antenna manifold vector for the GNSS signal of the *i*-th SV as the antenna moves through a random trajectory. Likewise $\mathbf{a}_i^S$ represents the instance of the moving antenna manifold vector for the *i*-th GNSS signal generated by the spoofer.

III. Spoofing Detection Based on Pairwise Correlation

The central tenet of the proposed spoofing detection technique is that the spatial signature present in the manifold vector of the spoofing signal, $\mathbf{a}_i^S$, is the same for all of the *L* counterfeit GNSS signals. On the contrary, the array manifold vector corresponding to the authentic signal, $\mathbf{a}_i^A$, is significantly 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

$$E\left[\boldsymbol{\Lambda}_i^{A^H}\boldsymbol{\Lambda}_j^A\right]\approx\delta_{ij} \quad for \quad 1\le i,j\le L \tag{8}$$

On the other hand, as the spoofing signals arrive from the same source, they will all have the same array manifold vector regardless of the random antenna trajectory and of the spatial fading conditions present, hence

$$E\left[\boldsymbol{\Lambda}_i^{S^H}\boldsymbol{\Lambda}_j^S\right]\approx 1 \quad for \quad 1\le i,j\le L \tag{9}$$

The basic assumption is that if more than one spoofing signals is transmitted from a common source, the observables of $\boldsymbol{\Lambda}_i^S$ and $\boldsymbol{\Lambda}_j^S$ are spatially correlated. In other words, if the pairwise correlation of the 2*L* correlator outputs result in cases of high correlation, then the spoofer existence is likely. These pairwise correlations can also be used to sort the spoofing from the authentic signals. Note that, even during the time when the spoofing and authentic signals have the same Doppler and code offset, the superposition manifold vector of $\mathbf{a}_i^A$ and $\mathbf{a}_i^S$ will be correlated with other spoofing manifold vectors.

Consider the problem of taking the output vectors from the set of 2*L* possible despreader outputs and arranging these into a $M\times 2L$ sample matrix denoted as $\mathbf{x}$. Assume that the sample vectors are selected from different despreader channels of the receiver corresponding to different GNSS signals; $\mathbf{x}$ can then be expressed as

$$\mathbf{x}=\begin{bmatrix} x_{1,1} & x_{2,1}\cdots x_{2L,1} \\ x_{1,2} & x_{2,2}\cdots x_{2L,2} \\ \vdots & \vdots\ \ddots\ \vdots \\ x_{1,M} & x_{2,M}\cdots x_{2L,M}\end{bmatrix} \tag{10}$$

A statistical detection metric to discriminate spoofing signals from the authentic ones is discussed in Appendix A.

Herein a standard correlation coefficient is utilized to measure the correlation between different PRNs parameters as the spoofing detection metric. The correlation coefficient between signal parameters of PRN *i* and PRN *j* is defined as

$$\rho_{ij}=\frac{E\left[\mathbf{x}_i\mathbf{x}_j^H\right]}{\sqrt{E\left[\mathbf{x}_i\mathbf{x}_i^H\right]}\sqrt{E\left[\mathbf{x}_j\mathbf{x}_j^H\right]}}. \tag{11}$$

where $\mathbf{x}_i$ is the *i*-th column of $\mathbf{x}$.

The spoofing detection methodology based on the correlation coefficient metric is summarized as follows:

1. In the acquisition stage define the number of correlation peaks higher than a threshold
2. Track all detected signals
3. Based on the measured correlation coefficient values, signals from each PRN are sorted intoa two groups. The ***Spoofing*** group is the data set that is highly correlated and the ***Authentic*** group is the set that is uncorrelated. Note that it is necessary that the trajectory is of sufficient length such that *M* is large.
4. The ***Authentic*** group will be constrained in size based 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 its current position, it is eliminated by the receiver. Hence, the ***Authentic*** group can be assumed to be constrained in size to *L*. There is the possibility that a spoofer generates a signal that is clear while the SV signal is shadowed and therefore not visible to the receiver. Under these circumstances, a spoofing signal can inadvertently be placed in the ***Authentic*** group. However, as this signal will be correlated with other signals in the ***Spoofing*** group then it can be pulled from the ***Authentic*** group.
5. The proper placement of the members in the ***Authentic*** and ***Spoofing*** groups can be reassessed because the set of members in the ***Authentic*** group should provide the lowest variance navigation solution. Hence in general there might be a spoofing and authentic signal that

corresponds to the GNSS signal of index *i*. If the spoofing signal in the ***Authentic*** group appears to have marginal correlation with its peers in the ***Spoofing*** group and when interchanged with its corresponding signal in the ***Authentic*** group generates a lower variance navigation solution, then an exchange should be made.

Figure **3** shows the block diagram of the proposed method.

IV. Experimental Results

Experimental results of a single antenna spoofing detection that is spatially translated are provided in this section. The experimental measurements are based on the reception of GPS L1 C/A signals. The measurements were directed to analyze the behavior of the spoofing signal initiated from a single source antenna. For this measurement, Spirent hardware simulator (HWS) signals were radiated indoors at a controlled power level using a directional antenna. The spoofing signals were received by a randomly moving antenna and then combined with the authentic signals coming from a randomly moving rooftop antenna. The random motion causes the authentic signals to decorrelate rapidly while all spoofing signals are highly correlated due to similar propagation channel. This test scenario satisfies the requirements for a real world spoofing experiment without the need for outdoor transmission in the GPS bands.

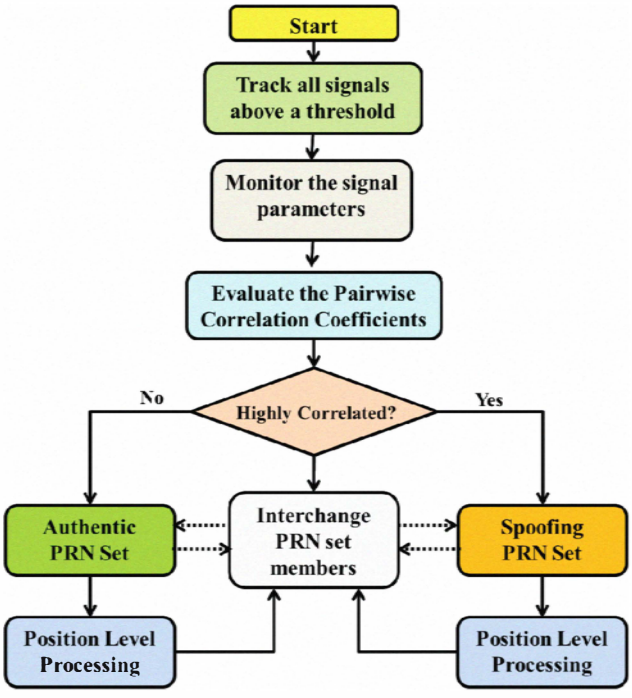

Figure 3: Processing Technique Flowchart

Figure 4: Sky plot of authentic PRN satellites numbers

Five PRNs namely PRN 15, PRN 16, PRN 18 PRN 21 and PRN 24 that are common with the authentic PRNs were propagated. Figure 4 shows the sky plot of the authentic satellites available during the experiment. The GPS receiver consisted of an active NovAtel-GPS 701/702 GGL series 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 tracking the correlation peaks of the authentic and spoofing signals and extracting the channel gains as a function of time. The data collection scenario is illustrated in Figure 5. During the data collection process the antenna was randomly moved by hand along an arbitrary arc of approximately 2 m. 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.

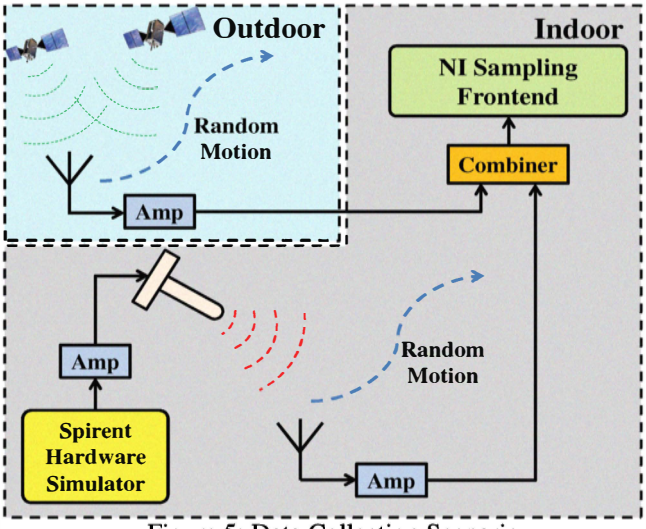

Figure 5: Data Collection Scenario

Figure 6 shows the correlation output of PRN 15 for the authentic GPS 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 constitute a tracked signal pair.

The correlation coefficient of the received signals can be measured based on the numerical estimate of the correlation coefficient given in (13).

Figure 7 shows the magnitude of the prompt correlator for different PRNs for authentic and spoofing signals as the antenna was randomly moved. As evident, in the spoofing case shown in Figure 7b, the signal amplitudes are highly correlated. This is expected as the spoofing signals are all radiated from the same location. However, in the case of the authentic signal (Figure 7a) amplitudes are changing independently.

Figure 8 shows the measured correlation coefficients values of signal amplitude shown in Figure 7 for the set of authentic and spoofing signals. As shown, as expected, the pairwise correlation coefficients in the case of authentic signals are much smaller than that of the spoofing signals.

Figure 9 shows the Doppler measurements due to the antenna motion for the authentic and spoofing signals. Note that all other Doppler frequency contributions such as satellite motion and clock drift have been wiped off. As shown the measured Doppler values of the authentic SV signals are uncorrelated over the measurement interval while the spoofing ones are highly correlated. As observed the authentic and spoofing signal Doppler variations are mutually uncorrelated as expected since the spoofing transmitter is at a different bearing than those of of the visible SVs.

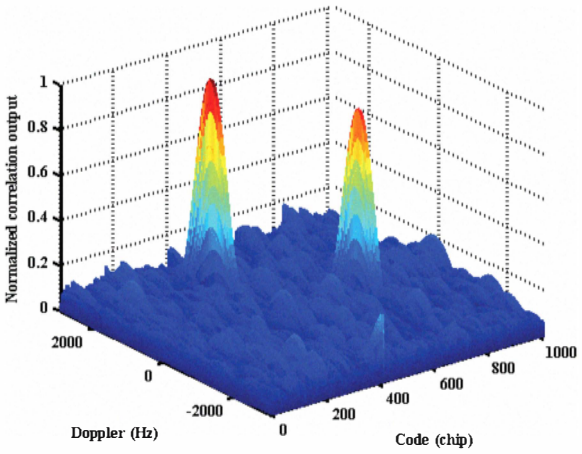

Figure 6: Correlation output of the authentic and spoofing signals in the case of PRN 15

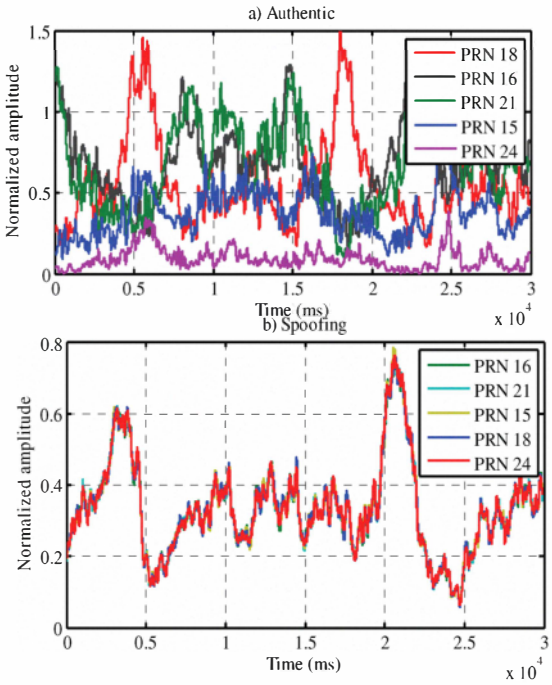

Figure 7: Normalized amplitude value for different PRNs: a) Authentic b) Spoofing

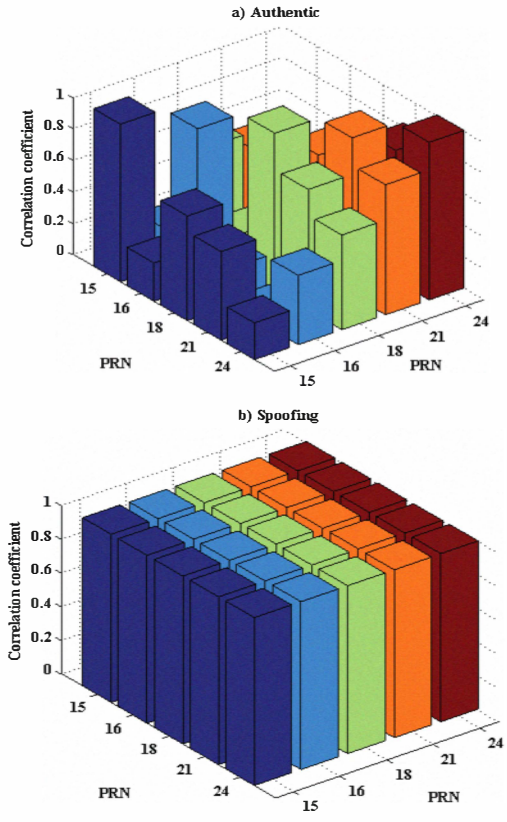

Figure 8: Correlation coefficient values of the signal magnitudes: a) Authentic b) Spoofing signals

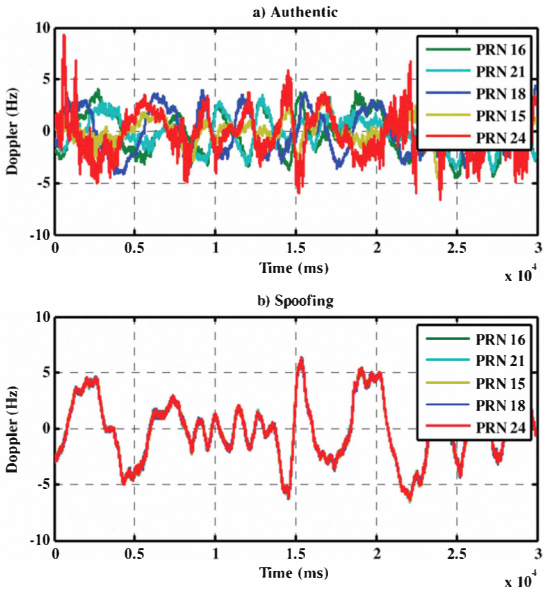

Figure 9: Doppler measurements due to the receiver motion: a) Authentic b) Spoofing

Figure 10 shows the correlation coefficients values of the Doppler measurements of Figure 9 for the set of authentic and spoofing signals. As expected, the pairwise correlation coefficients in the case of authentic signals are much smaller than those of the spoofing signals.

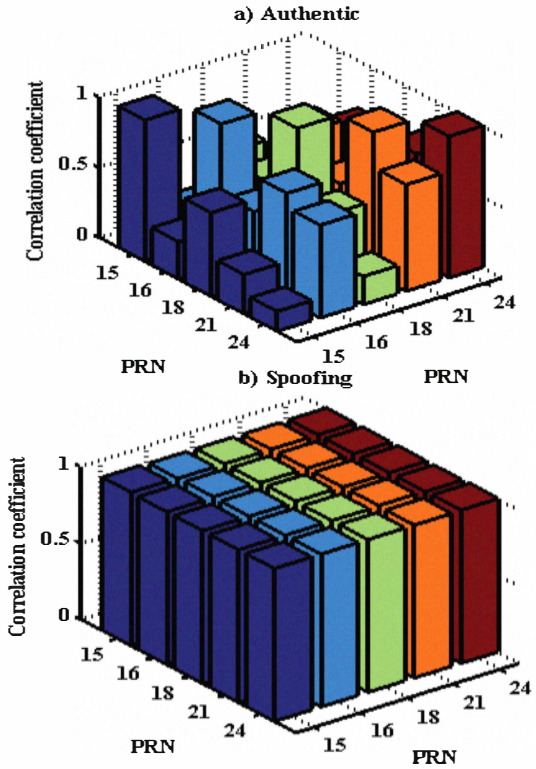

Figure 10: Correlation coefficient values of the Doppler measurements: a) Authentic b) Spoofing signals

V. CONCLUSIONS

A spoofing detection method based on a single moving antenna was investigated. It was shown that spoofing signals generated from a single point source can effectively be detected based on the spatial correlation of the signal parameters. The unique characteristic exploited in this paper is that the spoofing signals are spatially correlated while the authentic signals are not. Through a process of sorting the authentic and spoofing signals based on the pairwise signal parameters correlation, it is possible to sort the signals such that only the authentic signals are passed to the navigation solution. A key observation is that the detection performance of the developed method is not affected by spatial multipath fading that the GNSS signals are subjected to. 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] G. R. Hartman, *Spoofing Detection for a Satellite Positioning System*, US patent, 17 Sept 1996.

[2] E. C. McDowell, *GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling*, US patent, 31July 2007.

[3] S. Lo, D. DeLorenzo, P. Enge, D. Akos, P. Bradley, "Signal Authentification, a secure civil GNSS for today," Inside GNSS Sept/Oct 2009

[4] P. Montgomery, T. Humphreys, B. Ledvina, "A multi-antenna defense – receiver autonomous GPS spoofing detection," InsideGNSS March/April 2009,pp.40-46

[5] T. Humphreys, B. Ledvina, M. Psaiki, B. Hanlon, P.Kintner "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," Proceedings of ION GNSS 2008, Institute of Navigation, Savanna, Georgia, USA, 2008

[6] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers," in Proceedings of ION ITM 2010, 26 Jan, San Diego, CA, 2010.

[7] H. Wen, P. Y. Huang, J. Dyer, A. Archinal and J. Fagan "Countermeasures for GPS Signal Spoofing" in ION GNSS 18th International Technical Meeting of the Satellite Division, 13-16 September, Long Beach, CA, 2005

[8] H. L.V. Trees, *Optimum Array Processing, part IV, Detection, Estimation, and Modulation Theory*, John Wiley & Sons, Inc., New York, 2002

[9] J. Nielsen, A. Broumandan and G. Lachapelle "GNSS Spoofing Detection for Single Antenna Handheld Receivers" NAVIGATION, 58, 4, 335-344,2011.

[10] E. D. Kaplan, and C. Hegarty, *Understanding GPS Principles and Applications,* 2nd ed., Artech House 2006.

[11] H. L. V. Trees, *Detection, Estimation, and Modulation Theory, part I*. John Wiley & Sons, Inc., New York, 2001.0

[12] S. M. Kay, *Fundamentals of Statistical Signal Processing Detection Theory*, Prentice-Hall, Inc, 1998.

Appendix A:

A statistical decision for spoofing detection based on the correlation coefficient metric is developed for the special case when x is an L by 2 matrix . It is assumed that the trajectory and spatial multipath fading is random and stationary such that the sequences of $x_{1,m}$ and $x_{2,m}$ in (10) can be assumed to be wide sense stationary discrete random sequences. Essentially there are two states: H_0 denotes the case when there is no correlation between the pair of selected despreading vectors and H_1 is the case when 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.

Each of the sample pairs of $\mathbf{x}$ in (10) is 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

$$\mathbf{C} = E\left[\mathbf{x}_i^{\,H}\mathbf{x}_i\right] = \begin{cases} \mathbf{C_0} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \text{under } H0 \\ \mathbf{C_1} = \begin{bmatrix} 1 & \rho \\ \rho & 1 \end{bmatrix} & \text{under } H1 \end{cases} \quad \text{(A-1)}$$

for $i \in [1,...,M]$ and where ρ is the correlation coefficient. ρ is the single parameter that distinguishes between the two states H_0 and H_1 given $\mathbf{x}$. Initially assume ρ to be known such that the log likelihood ratio (LLR) of the conditional PDFs results in the following test statistic:

$$T(\mathbf{x};\rho) = \ln \frac{f_{\mathbf{x};\rho|H1}(\mathbf{x})}{f_{\mathbf{x}|H0}(\mathbf{x})} \quad \text{(A-2)}$$

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

$$T(\mathbf{x};\rho) = \frac{N}{2}\left|\frac{\mathbf{C_0}}{\mathbf{C_1}(\rho)}\right| + \frac{1}{2}\sum_{m=1}^{M} \mathbf{x}_m{}^T\left(\mathbf{C_0}^{-1} - \mathbf{C_1}(\rho)^{-1}\right)\mathbf{x}_m \,. \quad \text{(A-3)}$$

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

$$T(\mathbf{x};\rho) = \tfrac{1}{2}\sum_{m=1}^{M} \mathbf{x}_m{}^T\left(\mathbf{C_0}^{-1} - \mathbf{C_1}(\rho)^{-1}\right)\mathbf{x}_m \quad \text{(A-4)}$$

which can be expanded and stripped of unnecessary scaling and additive constants as

$$T(\mathbf{x}) = \sum_{m=1}^{M}\left(\frac{2x_{1,m}\ x_{2,m}}{\rho} - x_{1,m}{}^2 - x_{1,m}{}^2\right). \quad \text{(A-5)}$$

The PDF of $T(\mathbf{x})$ 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 $T(\mathbf{x})$ can be compared against to decode H_0 or H_1. Furthermore, in all practical applications ρ will be unknown such that a generalized LLR (GLRT) is required where $T(\mathbf{x})$ would be expressed as

$$T(\mathbf{x};\rho) = \ln \frac{f\left(\mathbf{x}\,|\,\hat{\rho}, H_1\right)}{f(\mathbf{x}\,|\,H_0)} \quad \text{(A-6)}$$

where $\hat{\rho}$ is the maximum likely estimate (MLE) of ρ. Unfortunately (A-6) does not generate a useful test statistic as $T(\mathbf{x};\rho)$ results in a constant independent of the data $\mathbf{x}$.

An alternative approach based on the Wald test is possible as M can be assumed to be moderately large and ρ is also the only parameter that distinguishes $f(\mathbf{x}\,|\,H_1)$ from $f(\mathbf{x}\,|\,H_0)$ [12]. The Wald test applied to this case is given as

$$T(\mathbf{x}) = \left(\hat{\rho}(\mathbf{x}) - \rho_0\right)^2 J\left(\hat{\rho}(\mathbf{x})\right) \quad \textbf{(A-7)}$$

where ρ_0 is the known value of ρ under H_0 such that in this case $\rho_0 = 0$. $J\left(\hat{\rho}(\mathbf{r})\right)$ is the Fisher Information Matrix (FIM) of the unknown variables which in this case is a scalar as ρ is the only unknown parameters. The FIM of $J(\rho)$ is easily determined for the case where the observables are jointly CN with a covariance matrix that depends on the parameter to be estimated. This relation is given as [11]

$$J(\rho) = tr\left(\mathbf{C_x}^{-1}(\rho)\frac{\partial \mathbf{C_x}(\rho)}{\partial \rho}\mathbf{C_x}^{-1}(\rho)\frac{\partial \mathbf{C_x}(\rho)}{\partial \rho}\right). \quad \text{(A-8)}$$

Then (A-8) can be expressed as

$$J(\rho) = Mtr\left(\left(\frac{1}{1-\rho^2}\begin{bmatrix} 1 & -\rho \\ -\rho & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)^2\right). \quad \text{(A-9)}$$

Evaluating this at $\rho = 0$ yields

$$J(0) = Mtr\left(\left(\frac{1}{1-0}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right)^2\right)$$
$$= Mtr\left(\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right) \quad \text{(A-10)}$$
$$= Mtr\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right) = 2M$$

The MLE of ρ is required for the Wald test, which is determined from

$$f_{\mathbf{x}}(\mathbf{x} \mid H1) = \left|2\pi\mathbf{C}_1\right|^{-\frac{M}{2}} \prod_{m=0}^{M-1} \exp\left(-\tfrac{M}{2}\mathbf{x}_m{}^T\mathbf{C}_1{}^{-1}\mathbf{x}_m\right). \quad \text{(A-11)}$$

Taking the log of this results in

$$\ln f_{\mathbf{x}}(\mathbf{x} \mid H_1) = -\frac{M}{2}\ln(2\pi) - \frac{M}{2}\ln\left(1-\rho^2\right)$$
$$-\sum_{m=0}^{M-1} \frac{x_{1,m}{}^2 + x_{2,m}{}^2 - 2\rho x_{1,m}x_{2,n}}{2\left(1-\rho^2\right)} \quad \text{(A-12)}$$

The MLE would result by determining ρ that satisfies

$$\frac{\partial}{\partial\rho}\ln f_{\mathbf{x}}(\mathbf{x} \mid H_1) = -\frac{M}{2}\frac{2\rho}{1-\rho^2} + \sum_{m=1}^{M} x_{1,m}x_{2,m} = 0. \quad \text{(A-13)}$$

This will require a numerical root finding procedure that does not lead to any further simplification.

However as M is moderately large and ρ is relatively small, (A-13) can be approximated as

$$0 = -M\rho + \sum_{m=1}^{M} x_{1,m}x_{2,m}, \quad \text{(A-14)}$$

resulting in

$$\hat{\rho} = \frac{1}{M}\sum_{m=1}^{M} x_{1,m}x_{2,m}{}^* \quad \text{(A-15)}$$

Then $T(\mathbf{x})$ can be written as

$$T(\mathbf{x}) = \left(\frac{1}{M}\sum_{m=1}^{M} x_{1,m}x_{2,m}^*\right)^2 M = \frac{1}{M}\left(\sum_{m=1}^{M} x_{1,m}x_{2,m}^*\right)^2. \quad \text{(A-16)}$$

This is the same as before, however the asymptotic conditional PDFs of $T(\mathbf{x})$ are derivable in closed form based on the Wald test formulation. When M becomes large these reduce to

$$T(x) \overset{a}{\sim} \begin{cases} \chi^2_{2M} & under\ H_0 \\ \chi'^2_{2M}(\lambda) & under\ H_1 \end{cases} \quad \text{(A-17)}$$

with λ given as the noncentrality factor of

$$\lambda = (\rho_1 - \rho_0)^2 J(\rho_0) \quad \text{(A-18)}$$
$$= \rho^2 2M$$