Hindawi Publishing Corporation
International Journal of Navigation and Observation
Volume 2012, Article ID 313527, 8 pages
doi:10.1155/2012/313527

Research Article

GNSS Spoofing Detection Based on Signal Power Measurements: Statistical Analysis

V. Dehghanian,[1, 2] J. Nielsen,[1] and G. Lachapelle[1]

[1] *Position Location And Navigation (PLAN) Group, University of Calgary, Calgary, AB, Canada T2N 1N4*
[2] *Department of Math Physics and Engineering, Calgary, Mount Royal University, AB, Canada T3E 6K6*

Correspondence should be addressed to V. Dehghanian, vdehghanian@mtroyal.ca

Received 18 June 2012; Revised 14 September 2012; Accepted 15 September 2012

Academic Editor: Jinling Wang

A threat to GNSS receivers is posed by a spoofing transmitter that emulates authentic signals but with randomized code phase and Doppler values over a small range. Such spoofing signals can result in large navigational solution errors that are passed onto the unsuspecting user with potentially dire consequences. An effective spoofing detection technique is developed in this paper, based on signal power measurements and that can be readily applied to present consumer grade GNSS receivers with minimal firmware changes. An extensive statistical analysis is carried out based on formulating a multihypothesis detection problem. Expressions are developed to devise a set of thresholds required for signal detection and identification. The detection processing methods developed are further manipulated to exploit incidental antenna motion arising from user interaction with a GNSS handheld receiver to further enhance the detection performance of the proposed algorithm. The statistical analysis supports the effectiveness of the proposed spoofing detection technique under various multipath conditions.

1. Introduction

The received GNSS signal power at the output of a 3 dB gain hemispherical linearly polarized antenna at ground level is approximately -130 dBm [1]. This makes GNSS receivers susceptible to nearby noise jammers and standoff spoofers (SS) that can easily transmit power levels well above -130 dBm. A high processing gain based on a long integration time is often the only option available to overcome a noise jammer. Nevertheless, if the GNSS receiver undergoes random motion, then the channel decorrelates quickly such that attaining such large processing gains to overcome jamming is neither feasible nor desirable from an operational perspective. Also a jammer is relatively easy to locate with radio direction finding and to potentially disable as its spectrum is significantly larger than the ambient noise [2, 3]. In addition, the noise jammer is at least detectable as the spectral power in the affected GNSS receiver band will be abnormally high. Hence the jammer can deny service but the user is aware of being jammed, limiting the damage potential of the jammer. A more insidious threat is the standoff spoofer that broadcasts a set of replicas of the authentic satellite vehicle (SV) signals visible to the mobile GNSS receiver [2]. Disruption of GNSS services is achieved by randomly modulating the code phase over a small region of the overall Code Delay Space (CDS) that is commensurate with a target area. The spoofing attack is assumed to happen during the acquisition stage. Therefore, it is not possible to identify the SS signal based on the code phase as corresponding to an outlier navigation solution. The SS is assumed to remain synchronized with currently visible GNSS signals and then transmit a set of signals that would correspond to the typical GNSS signals observable by a receiver in the target area. Note that an effective SS does not necessarily synthesize a specific counterfeit location for a specific GNSS receiver but rather aims to disrupt GNSS services over a general target area by matching the Doppler offset of the replicated SV signals and adjusting the code phase such that it is commensurate with the intended target region. Hence the GNSS receiver cannot easily detect the contribution of these counterfeit signals as obvious outliers. An unaware receiver computes the navigation solution based on the SS generated counterfeit signals which are passed on to the user as being reliable with potentially damaging consequences.

GNSS receivers tethered to a wireless data service provider will typically provide the user with an aided-GNSS (AGNSS) service, significantly reducing the CDS corresponding to a physical area of several square kilometres [4]. Hence there is a diminishing gain for the spoofer attempting to affect a larger target area than this. Hence the counterfeit SS navigation solutions will be construed as plausible. As such, receiver-autonomous integrity monitoring (RAIM) and fault detection and exclusion (FDE) are ineffective in discriminating signals sourced from the envisioned SS [5].

The typical handheld consumer GNSS receiver coherently integrates the signal for about 10 to 20 ms resulting in a correlation peak in the CDS that has a spread in Doppler of about 100 Hz, which is commensurate with the Doppler spread of typical urban traffic (<50 km/hr) [6]. Even if the GNSS receiver is equipped with other ancillary sensors such that the receiver velocity vector is independently known, this cannot be used to discriminate the SS signal as multipath Doppler spreading is approximately equivalent for both the SS and the authentic SV signals.

Note that the receiver processing gain used for suppressing a jamming signal is not effective in the case of the spoofer signal. Consequently, the spoofer transmit power can be orders of magnitude less than that of the noise jammer, which makes the spoofer source much more difficult to locate and disable through radio direction finding and beam forming.

The objective of this paper is to address a computationally efficient processing technique that can be added to relatively unsophisticated consumer grade GNSS receivers to discriminate the spoofer signals transmitted by an SS. The proposed processing is based on estimating and comparing the receiver signal power with a set of thresholds to verify the authenticity of the signal. The detection problem is formulated based on a Rayleigh fading multipath scenario. Nevertheless, it is shown that although suboptimal, the deduced expressions can be utilized for spoofing detection in a generalized Rician multipath channel with minimal performance degradation.

The proposed technique is further extended to include incidental motions of the handheld receiver, instigated through the user interaction with the handset device, in the form of spatial translation and polarization rotation. User interaction with the handheld creates variability in the antenna response, which can be transformed into a diversity gain that adds to the general processing gain of the receiver [7–10]. This processing gain enhances the estimation of the received signal power of the correlation peaks, that, is necessary information in spoofer discrimination. A case study based on GPS L1 C/A signals is developed to demonstrate the effectiveness of the proposed technique. Nevertheless, this technique can be directly extended for other GNSS signal formats such as GPS L2 C/A and GLONASS.

The rest of the paper is organized as follows. In Section 2 the system definition and the assumptions are given. Section 3 formulates a multihypothesis detection problem and focuses on the statistical evaluation of the proposed technique, with the conclusions provided in Section 4.

2. System Definition

This paper considers the analysis of individual GNSS satellite signals, while realizing that simultaneous processing of the available GNSS signals provide extra diversity that can be used to further improve the performance of the proposed spoofer detection technique. The received complex GNSS baseband signal is denoted here by

$$g(t) = A(t)s_o(t) + w(t), \tag{1}$$

where the signal component of $g(t)$ is represented by $s(t) = A(t)s_o(t)$, where "t" is time, $A(t)$ is the channel response to the incident signal at the antenna, and $s_o(t)$ is the complex baseband component of the satellite signal, which can be written as

$$s_o(t;\tau,\Delta f) = d(t-\tau)c(t-\tau)e^{j(2\pi\Delta f t+\psi)}, \tag{2}$$

where $d(t)$ is the navigation data modulation, $c(t)$ is the Pseudo Random Noise (PRN) code, τ is the code phase, Δf represents carrier frequency offset (due to the Doppler of the GNSS signal as well as any frequency offset of the receivers local oscillator), and ψ is the initial phase offset. $s_o(t)$ is known to the receiver except for the navigation data, the code phase, the carrier frequency offset, and the initial phase offset ψ. The received signal, $g(t)$, is corrupted by additive noise (WGN) which has an equivalent complex baseband representation denoted by $w(t)$. It is assumed that $w(t)$ is a complex normal random process, independent of the signal, and has a Power Spectral Density (PSD) that is constant within the bandwidth of the received signal.

The GNSS receiver integrates a temporal snapshot of $g(t)$ over the interval of $t \in [0, T_I]$, where T_I is typically smaller than the duration of one navigation data bit (20 ms). The signal snapshot of $g(t)$ is collected by the receiver and then despread by a locally generated copy of $s_o(t)$ during the initial acquisition. The initial acquisition is typical of a multihypothesis detection in which the receiver searches the Code Doppler Space (CDS) for the frequency offset Δf and the code delay, τ [11, 12]. Note that the initial phase offset ψ is not known to the receiver during the initial acquisition and as such the output of the despreading matched filter is a random complex variable.

The despread baseband signal samples at a correlator output are represented by

$$\begin{aligned} x_{n;\tau,\Delta f} &= \frac{1}{T_I}\int_{(n-1)T_I}^{nT_I} g(t)s_o\left(t;\hat{\tau},\Delta\hat{f}\right)^* dt \\ &= \frac{1}{T_I}\int_{(n-1)T_I}^{nT_I} A(t)dt \\ &\quad + \frac{1}{T_I}\int_{(n-1)T_I}^{nT_I} w(t)s_o\left(t;\hat{\tau},\Delta\hat{f}\right)^* dt \\ &= s_n + w_n, \quad n = 1,\ldots,N, \end{aligned} \tag{3}$$

where "$*$" is a complex conjugate, the subscript "n" denotes the nth signal sampling interval which extends over $t \in [(n-1)T_I, nT_I]$, and s_n, w_n are the postintegration signal and the WGN components, respectively. In addition, $\hat{\tau}$ and $\Delta\hat{f}$ represent the estimated code phase and Doppler based on the initial acquisition which consists of a maximum likelihood search over the CDS of a signal sample, $x_{n;\tau,\Delta f}$, such that

$$\left\{\hat{\tau}, \Delta\hat{f}\right\} = \max_{\arg\{\tau,\Delta f\}} \left(\left|x_{n;\tau,\Delta f}\right|^2\right), \tag{4}$$

where $\{\hat{\tau}, \Delta\hat{f}\}$ are the maximum likelihood (ML) estimates of the true code phase and Doppler frequency, respectively. The estimated code phase and Doppler are then passed on to the tracking loops to facilitate further receiver processing. Consequently, N signal samples, namely, $\mathbf{x} = [x_1, \ldots, x_N]$, can be collected and used for spoofer detection.

3. Theoretical Analysis of Spoofer Detection

A hypothetical scenario is considered based on an SS transmitting spoofing signals in an urban environment as shown in Figure 1. The authentic signal and the spoofer signal are affected by multipath fading and therefore, the received signal power is random in space and polarization. In other words, multipath fading results in signal power fluctuation when the receiver is spatially translated or undergoes polarization changes due to rotation. Unlike the authentic signal power which is insensitive to signal power variations arising from pathloss in the target area (this is due to the fact that the satellite-receiver separation is approximately unchanged over a period of several minutes), the spoofer signal power varies with variation in the spoofer-receiver separation. An empirical model of order n can be utilized to model the spoofer signal power variation due to pathloss as

$$\rho_d^{(\mathrm{sp})} = \rho_{R1}^{(\mathrm{sp})} - 10n\log_{10}\left(\frac{d}{R1}\right), \tag{5}$$

where $R1$ is a reference range, d is the spoofer-receiver range, n is the pathloss exponent, $\rho_d^{(\mathrm{sp})}$ is the average spoofer SNR at d, and $\rho_{R1}^{(\mathrm{sp})}$ is the average received spoofer SNR at $d = R1$ in dBs. Note that, for the spoofer to be effective, the average received spoofer signal power needs to be higher than that of the authentic signal in the target area. Therefore, the received signal power from a standoff spoofer varies significantly with range due to pathloss, meaning that the spoofer signal power is abnormally higher than that of the authentic signal when the receiver is in the proximity of the standoff spoofer. This characteristic of the spoofer signal can be exploited to limit the effectiveness of the SS in its target area based on comparing the measured signal power against a preset threshold.

As stated earlier, a receiver records N signal samples with each of these $n = 1, \ldots, N$ signal samples belonging to one of the three hypotheses, namely, the noise hypothesis H0, the authentic signal hypothesis H1, and the spoofer signal hypothesis H2 as

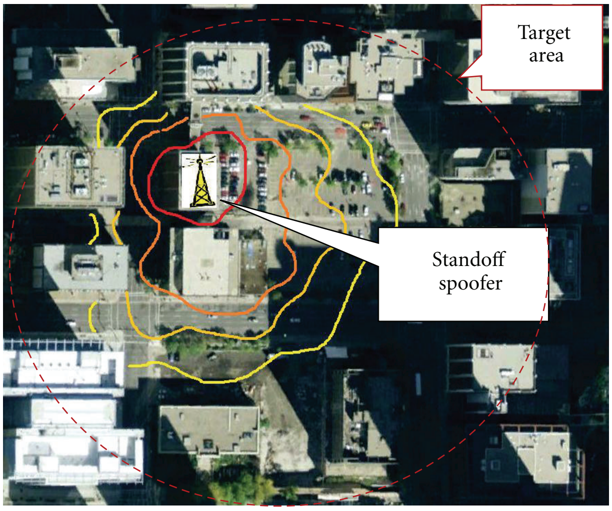


Figure 1: Hypothetical stand-off spoofer scenario in an urban canyon. The contours represent the random average spoofer signal power. The average authentic signal power is approximately constant over the entire area given that the receiver-satellite range is approximately unchanged and hence the pathloss.

$$\begin{aligned}
\mathrm{H0}: x_n &= \frac{1}{T_I}\int_{(n-1)T_I}^{nT_I} w(t)s_o(t)^* dt \approx w_n \\
\mathrm{H1}: x_n &= \frac{1}{T_I}\int_{(n-1)T_I}^{nT_I} A^{(a)}(t)dt \\
&\quad + \frac{1}{T_I}\int_{(n-1)T_I}^{nT_I} w(t)s_o(t)^* dt \approx s_n^{(a)} + w_n \\
\mathrm{H2}: x_n &= \frac{1}{T_I}\int_{(n-1)T_I}^{nT_I} A^{(\mathrm{sp})}(t)dt \\
&\quad + \frac{1}{T_I}\int_{(n-1)T_I}^{nT_I} w(t)s_o(t)^* dt \approx s_n^{(\mathrm{sp})} + w_n,
\end{aligned} \tag{6}$$

where the normalization $\int_t^{t+T} |s_o(t)|^2 dt = 1$ is assumed and $\hat{\tau}$, $\Delta\hat{f}$ are suppressed for notational convenience. $A^{(a)}(t)$ and $A^{(\mathrm{sp})}(t)$ represent channel gains associated with the authentic and the spoofer signals, respectively. Consequently, a detection variable, $r = h(\mathbf{x})$, can be formulated to decide between the three hypotheses of (6) based on comparing "r" with a set of thresholds, ρ_1, ρ_2, as shown in Figure 2. Note that $h(\mathbf{x})$ is a function that maps the measured signal samples $\mathbf{x}$ to a single variable, r, which is a sufficient statistic with respect to H0, H1, and H2. As will be shown in Section 3.1, r can be found from the probability density functions (PDF) of $\mathbf{x}$ [13] or alternatively from the PDFs of "r" which are denoted here by

$$\begin{aligned}
&\mathrm{H0}: f_{r|\mathrm{H0}}(r) \\
&\mathrm{H1}: f_{r|\mathrm{H1}}(r) \\
&\mathrm{H2}: f_{r|\mathrm{H2}}(r),
\end{aligned} \tag{7}$$

where $f(\cdot)$ denotes a PDF.

One optimization criteria for determining the thresholds (ρ_1, ρ_2) is based on minimizing the probability of error, namely,

$$P_e = 1 - \left[\sum_{i=0}^{2} P(\mathrm{H}i \mid \mathrm{H}i)P(\mathrm{H}i)\right], \tag{8}$$

where $P(\mathrm{H}i)$ for $i = 0, 1, 2$ are the probabilities of H0, H1, and H2 states and $P(\mathrm{H}i|\mathrm{H}i)$ denotes the conditional probability that indicates that of deciding Hi if Hi is correct. Consequently,

$$\begin{aligned} P_e = 1 - [&\mathrm{P(H0)}F_{r|\mathrm{H0}}(\rho_1) + \mathrm{P(H1)}(F_{r|\mathrm{H1}}(\rho_2) - F_{r|H1}(\rho_1)) \\ &+\mathrm{P(H2)}(1 - F_{r|\mathrm{H2}}(\rho_2))], \end{aligned} \tag{9}$$

where $F_{r|\mathrm{H}_i}(\cdot)$ denotes a cumulative distribution function (CDF) of the random variable "r" under H_i. As can be seen from (9), P_e is a function of the authentic signal, the spoofer, and the noise statistics. Therefore, any optimization based on minimizing the probability of error hinges on knowing the spoofer signal statistics, which is not available to an unsuspecting receiver given the capricious nature of a spoofer.

Alternatively, a second optimization can be made based on maximizing the probability of detection for a given probability of false alarm. Assuming $\rho_2 > \rho_1$, the threshold ρ_1 can be determined based on selecting a probability of false alarm P_{FA1} as

$$\begin{aligned} P_{\mathrm{FA1}} &= \Pr\{r > \rho_1 \mid \mathrm{H0}\} \cup \Pr\{r > \rho_2 \mid \mathrm{H0}\} \\ &= \Pr\{r > \rho_1 \mid \mathrm{H0}\}. \end{aligned} \tag{10}$$

Therefore,

$$\rho_1 = 1 - F_{r|\mathrm{H0}}(P_{\mathrm{FA1}}). \tag{11}$$

As is evident from (11), ρ_1 depends on P_{FA1} and on the noise statistic, which is approximately known to the receiver.

As stated earlier, the average spoofer SNR is not known and varies with varying spoofer-receiver separation due to pathloss, spoofer transmit power variations, and so forth. However, the average authentic line of sight (LOS) SNR is approximately known, given that the average LOS CNR of GNSS signals at the ground level is typically within [40–50] (dB-Hz), which maps into a postprocessing SNR of approximately [10–20] dB based on 1 ms of coherent integration. This a priori information can be used to determine a second threshold, ρ_2, based on selecting a probability of false alarm associated with H2 as

$$P_{\mathrm{FA2}} = \int_{\rho_2}^{\infty} f_{r|\mathrm{H1}}(r)dr. \tag{12}$$

Given that the satellite geometry is not known to an acquiring receiver, it is reasonable to assume that SVs are approximately uniformly distributed in the sky. Consequently, the PDF of the average post processing SNR of the authentic GNSS signals, $\rho^{(a)}$, can be approximated as

$$\rho^{(a)} \sim U(\rho_L, \rho_H), \tag{13}$$

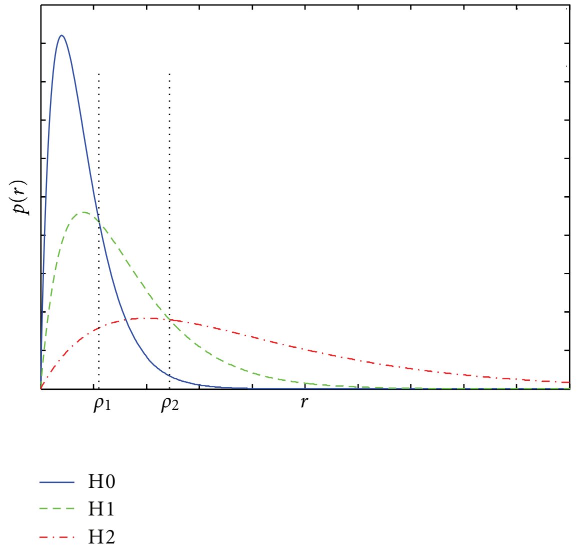


FIGURE 2: A diagram of the PDFs of the detection variable "r" under H0, H1, and H2 hypotheses.

where $U(\rho_L, \rho_H)$ denotes a uniform PDF and $\rho_L \approx 10, \rho_H \approx 20$ dB denotes the lower and the upper bounds of the uniform distribution. Consequently,

$$\begin{aligned} f_{r|\mathrm{H1}}(r) &= \int f_{r|\mathrm{H1}}\left(r \mid \rho^{(a)}\right) f_{\rho^{(a)}}\left(\rho^{(a)}\right) d\rho^{(a)} \\ &= \frac{1}{\rho_H - \rho_L} \int_{\rho_L}^{\rho_H} f_{r|\mathrm{H1}}\left(r \mid \rho^{(a)}\right) d\rho^{(a)}. \end{aligned} \tag{14}$$

ρ_2 can be numerically computed by inserting (14) into (12). Finally, the probability of detection associated with H2 can be computed as

$$P_{\mathrm{D2}}(\rho_2) = P_{22} = \int_{\rho_2}^{\infty} f_{r|\mathrm{H2}}(r)dr. \tag{15}$$

3.1. Spoofer Detection Based on a Moving Antenna. As stated earlier, the typical usage mode of a handheld receiver includes incidental motion in the form of spatial translation, polarization rotation, and blocking of the receiver antenna. It is known that any temporal variation in the antenna response results in a temporal signal decorrelation in a multipath environment such that extra diversity branches can be made available for receiver processing [7–10].

To exploit the extra processing gain arising from antenna motion, the statistical properties of $\mathbf{x}$ need to be considered. Distribution of scatterers in many multipath environments such as indoors or urban areas approximately resembles a uniform sphere of scatterers [9, 14]. The correlation coefficient between signal samples, $\mathbf{s} = [s_1, \ldots, s_n]$, collected through spatially translating an antenna over an arbitrary trajectory in a Rayleigh fading environment that resembles a sphere of scatterers can be shown to be [7]

$$[\mathbf{C_s}]_{mn} = \eta \operatorname{sinc}(k_0 p_{mn}), \tag{16}$$

where $k_0 = 2\pi/\lambda$ is the propagation constant, $p_{mn} = |\mathbf{p}_m - \mathbf{p}_n|$ is the spatial separation between the antenna positions at

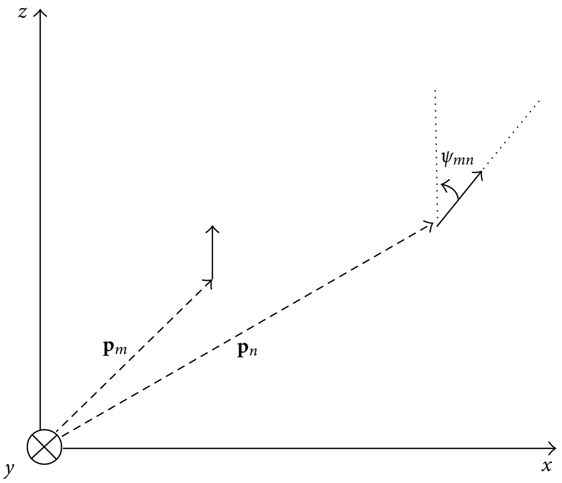


Figure 3: Spatial translation and polarization rotation of a GNSS handheld antenna.

which signal samples x_m and x_n are collected (see Figure 3), and η is the variance of $\mathbf{s}$. Consequently, x_m are statistically uncorrelated if the spatial separation between the antenna positions at which the samples are measured are greater than half a carrier wavelength (in GPS L1 frequency this maps into a spatial separation of 10 cm), resulting in the approximation of $\mathbf{C_s} \approx \eta \mathbf{I}_N$, where $\mathbf{I}_N$ is an $N \times N$ identity matrix.

Rotation is another form of user interaction with a handheld receiver that results in variation in antenna's polarization. Variation in antenna's polarization is known to result in signal decorrelation. It can be shown that the covariance of signal samples measured through polarization rotation of a handheld antenna follows from [15] as

$$[\mathbf{C_s}]_{mn} = \eta \cos \psi_{mn}, \tag{17}$$

where ψ_{mn} is the angular separation of the polarization vectors at which signal samples x_m and x_n are collected (see Figure 3). Note that only three degrees of freedom are realizable based on a polarization rotation of a linearly polarized antenna [16]. Therefore, $N \leq 3$ uncorrelated signal samples are realizable based on a polarization rotation.

A combination of polarization rotation and spatial translation can be utilized to further increase the number of diversity branches [9]. The cross-covariance arising from a combined spatial-polarization translation of a GNSS handheld antenna can be shown to be [9]

$$[\mathbf{C_s}]_{mn} = \eta \operatorname{sinc}(k_0 p_{mn}) \cos \psi_{mn}. \tag{18}$$

As can be seen from (18), the receiver motion in the form of a combined translation in space and rotation of polarization decorrelates the received signal and therefore can be utilized to synthesize several diversity branches useful for receiver processing.

3.1.1. Uncorrelated Rayleigh Fading Channels. Assume that N uncorrelated signal samples are obtained based on a combined spatial and polarization translation of a GNSS handheld receiver in an uncorrelated Rayleigh fading channel such that $\mathbf{C_s} = \eta \mathbf{I}_N$. Consequently, $\mathbf{x} = \{x_1, \ldots x_N\}$ are jointly CN zero-mean RVs with $\mathbf{x} = \mathbf{s} + \mathbf{w} \sim \mathrm{CN}(0, \mathbf{C_x})$. $\mathbf{C_x} = \mathbf{C_s} + \mathbf{C_w}$ denotes a covariance matrix of $\mathbf{x}$ with $\mathbf{C_w}$ as the noise covariance matrix. To simplify the expressions to follow and without any loss of generality, the noise covariance is normalized such that $\mathbf{C_w} = \mathbf{I}_N$. Therefore, the SNR can be written as

$$\rho = \eta. \tag{19}$$

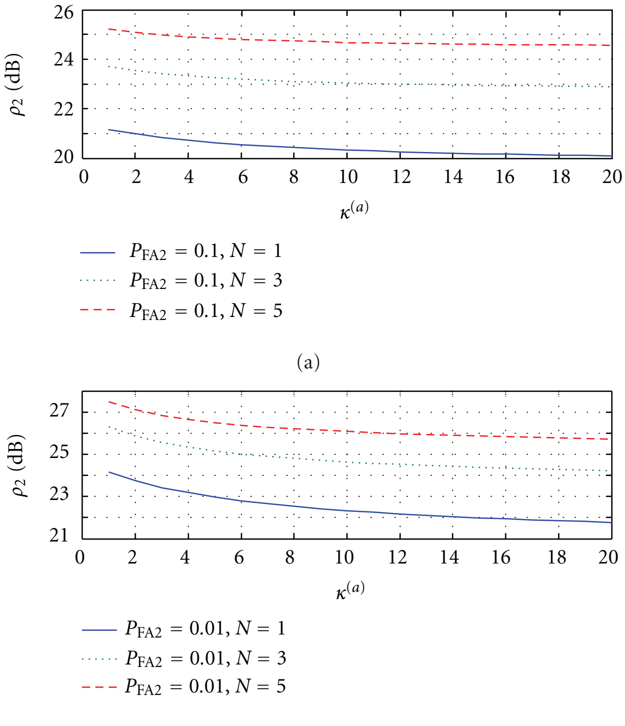
Consequently, the signal samples collected by a moving antenna in an uncorrelated Rayleigh fading channel are distributed according to $\mathbf{x} \sim \mathrm{CN}(0, (\eta + 1)\mathbf{I})$. It can be shown that

$$r = \mathbf{x}^H \mathbf{x} \tag{20}$$

is a sufficient statistics with respect to the hypotheses H0, H1, and H2 and as such is the detection variable [13]. The thresholds (ρ_1, ρ_2) can be found by determining the PDF of r and substituting in (10)–(15) for any given $P_{\mathrm{FA1}}, P_{\mathrm{FA2}}$.

Note that r is a measure of the received signal power. Therefore, the detection problem is based on comparing the received signal power, r, with a set of thresholds, (ρ_1, ρ_2), to determine the authenticity of the received signal. For the spoofer to be effective, the spoofer signal power must be higher than that of the authentic signal in the target area such that the ML search in the CDS results in selecting the spoofer signal which has the largest correlation peaks. Therefore, r, which is a measure of the received signal power, can be utilized to discriminate the spoofer from the authentic signals.

3.1.2. Generalized Rician Channels. In a generalized Rician channel, the channel gain, $A(t)$, is a random variable distributed according to $\mathrm{CN}(\mu, \eta/2)$ where $\mu = |\mu|\sqrt{2}\exp(j\alpha(t))$ is the complex mean with $\alpha(t)$ denoting the phase of the complex mean and $\eta/2$ is the variance of the in-phase and the quadrature-phase Gaussian components of the channel gain. Consequently, $\mathbf{x}$ are jointly CN RVs and are distributed according to $\mathbf{x} = \mathbf{s} + \mathbf{w} \sim \mathrm{CN}(\overline{\mathbf{m}}, \mathbf{C_x})$, where $\overline{\mathbf{m}} = \mu[e^{j\alpha_1}, \ldots, e^{j\alpha_N}]^T$ is an $N \times 1$ vector with α_i denoting the phase, $\mathbf{C_x} = \mathbf{C_s} + \mathbf{C_w}$ is a covariance matrix of $\mathbf{x}$, and $\mathbf{C_w} = \mathbf{I}_N$ is the normalized noise covariance. In a Rician channel, the average SNR, ρ, can be defined as $\rho = 2|\mu|^2 + \eta$, and the magnitude of the mean, $|\mu|$, and the variance, η, are related through the Rician K-factor, κ, such that $\kappa = |\mu|^2/\eta$. Since the angle of arrival (AoA) of the dominant signal component is not known to the receiver, μ cannot be estimated and therefore $\overline{\mathbf{m}}$ and subsequently κ are unknown which makes it impossible to formulate a sufficient statistics based on a likelihood ratio test [13]. Nevertheless, as will be shown here, the performance of the spoofer detection is approximately insensitive to the variation in the K-factor, κ, and to the cross-correlation of signal samples $\mathbf{s}$ as long as the cross-correlation remains moderately low, for example, <0.7. This is reasonable since diversity gain arising from combining equal-power diversity branches remains mostly



(a)

(b)

Figure 4: Threshold ρ_2 computed for various values of K-factor and different P_{FA2} and N at $\rho^{(a)} = 15$ (dB).

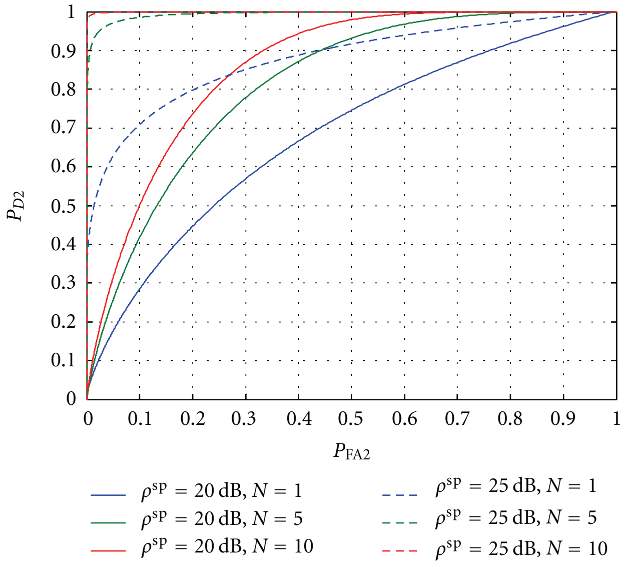


Figure 5: ROC curves based on $\rho^{(a)} = 15$ and $\kappa^{(a)} = \kappa^{(sp)} = 1$.

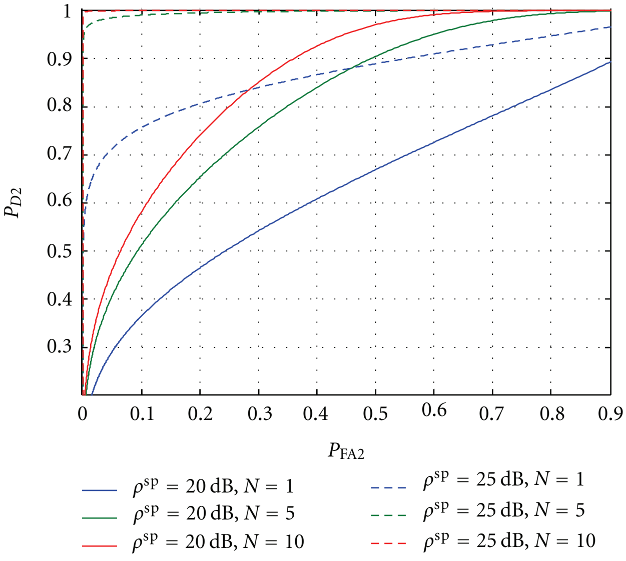


Figure 6: ROC curves based on $\rho^{(a)} = 15$ and $\kappa^{(a)} = 10,\ \kappa^{(sp)} = 1$.

unchanged for branch cross-correlations <0.7. Therefore, the suboptimal detection variable of (20) can be applied for spoofing detection in a generalized Rician channel with small performance degradation. Figure 4 shows ρ_2 being computed from (14) for various authentic and spoofer channel K-factors ($\kappa^{(a)}$and $\kappa^{(sp)}$) and based on $\rho^{(a)} = 15$ (dB) and $\rho^{(sp)} = 20$ (dB), two typical $P_{FA2} = 0.01, 0.1$, and for $N = 1,3,5$. As can be seen from Figure 4, smaller K-factors result in larger ρ_2 values. This is due to the increased uncertainty in the received signal power as the K-factor decreases. Nevertheless, the variation in ρ_2 is limited to a few dB and as such the K-factor does not play a major role in the optimization problem and may be ignored in the expense of slightly lower performance. Therefore, (20) can be applied to a generalized Rician channel as a suboptimal detector. In addition, as can be seen from this figure, a larger N results in a smaller ρ_2 for the same performance requirement of P_{FA2}. This is due to the diversity gain made available through the extra diversity branches for $N > 1$.

Figures 5 and 6 show the receiver operating characteristics (ROC) based on the detection variable of (20) and for $\rho^{(a)} = 15$ dB, various N and $\rho^{(sp)}$, and based on $\kappa^{(a)} = \kappa^{(sp)} = 1$ and $\kappa^{(a)} = 10$, $\kappa^{(sp)} = 1$. As can be seen in these figures, the detection performance improves with increasing the number of diversity branches, N. Also, larger $\rho^{(sp)}$ result in a better detection due to the further separation between the PDFs of the authentic and spoofing signals. When a stronger LOS signal component is present ($\kappa^{(a)} = 10$ in Figure 6), a better detection performance is realized due to the reduced uncertainty in the authentic signal power. Note that setting $P_{FA2} = 0$ in (12) results in $\rho_2 = \infty$ and therefore $P_{D2} = 0$. This corresponds to a receiver not equipped with any spoofer detection.

To provide an alternative measure of performance improvement, the probability of error P_e of (9) can be used. Figure 7 shows P_e for various N, $\kappa^{(a)}$, and $\rho^{(a)} = 15$ and based on $\kappa^{(sp)} = 1$ and $\rho^{(sp)} = 25$ (dB). As can be seen from this figure, P_e is approximately independent of the exact value of K-factor, which emphasizes the previous observations of Figure 4 where it was shown that the threshold ρ_2 is not very sensitive to the variations of the K-factor. P_e decreases rapidly with increasing the number of diversity branches. The latter demonstrates the performance enhancement arising from

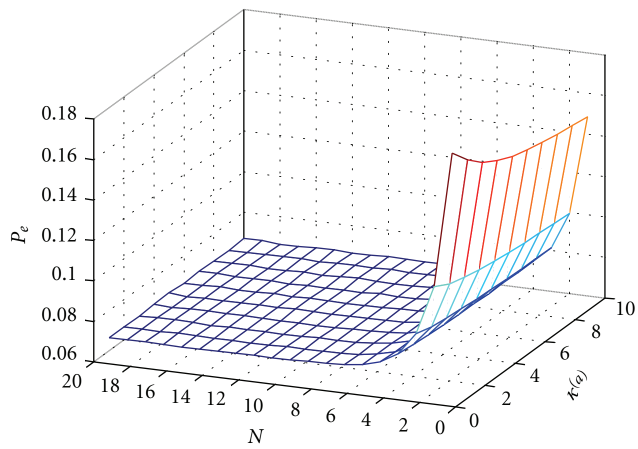


Figure 7: P_e for various N and $\kappa^{(a)}$, $\rho^{(a)} = 15$, and based on $P_{\mathrm{FA1}} = P_{\mathrm{FA2}} = 0.1$, $\kappa^{(\mathrm{sp})} = 1$ and $\rho^{(\mathrm{sp})} = 25$ (dB).

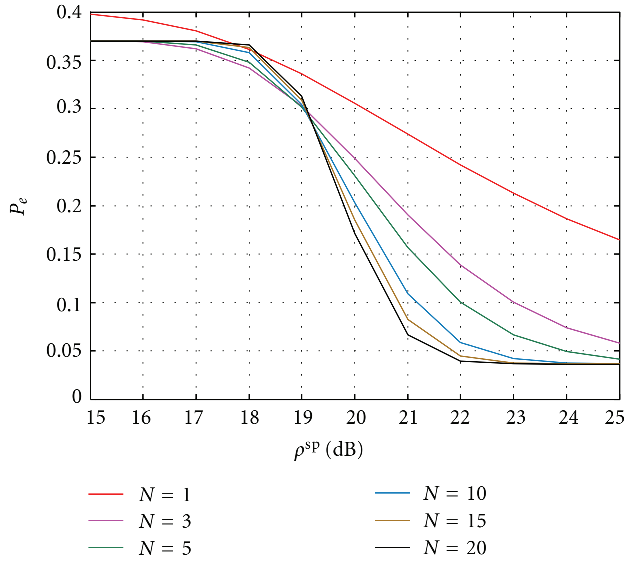


Figure 8: P_e versus $\rho^{(\mathrm{sp})}$ and for $\rho^{(a)} = 15$ (dB) and $P_{\mathrm{FA1}} = 0.01$ and $P_{\mathrm{FA2}} = 0.1$, $\kappa^{(a)} = \kappa^{(\mathrm{sp})} = 1$, and for $N = 1, 3, 5, 10, 15, 20$.

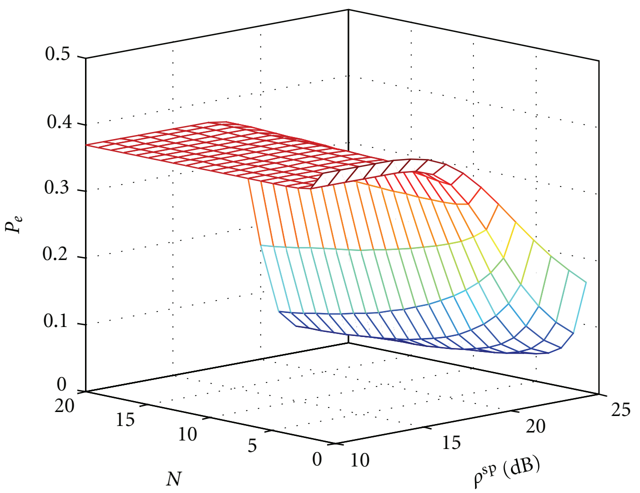


Figure 9: P_e for N = 1–20, $P_{\mathrm{FA1}} = 0.01$ and $P_{\mathrm{FA2}} = 0.1$, $\kappa^{(a)} = \kappa^{(\mathrm{sp})} = 1$, $\rho^{(a)} = 15$, and $\rho^{(\mathrm{sp})}$ = 10–25 (dB).

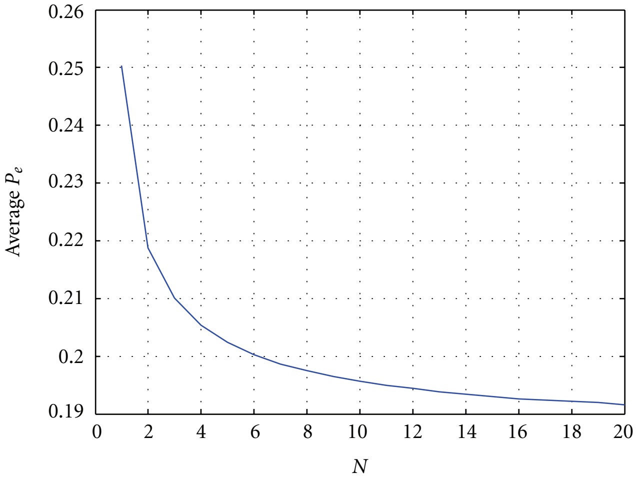


Figure 10: $\overline{P}_e$ for various N based on $P_{\mathrm{FA1}} = 0.01$ and P_{FA2}= 0.1, $\kappa^{(a)} = \kappa^{(\mathrm{sp})} = 1$ and $\rho^{(a)} = 15$ (dB), and for $\rho^{(\mathrm{sp})}$ averages over $\rho_{\min} = 15$, $\rho_{\max} = 25$ (dB).

the extra diversity branches made available through utilising a moving antenna.

Figure 8 shows P_e for $\rho^{(a)} = 15$ (dB) and various $\rho^{(\mathrm{sp})}$, $\kappa^{(a)} = \kappa^{(\mathrm{sp})} = 1$, and for $N = 1, 3, 5, 10, 15, 20$. Similarly, larger N and larger $\rho^{(\mathrm{sp})}$, which provide a better separation between the authentic and the spoofing signal PDFs, result in a smaller P_e. This is further demonstrated in Figure 9 where P_e is plotted for N = 1–20, $\kappa^{(a)} = \kappa^{(\mathrm{sp})} = 1$, and $\rho^{(\mathrm{sp})}$ = 10–25 (dB). Note that, as the PDFs of the authentic and the spoofer signals become more alike, for example, $\rho^{(a)} = \rho^{(\mathrm{sp})}$, P_e becomes larger.

As stated earlier, the spoofer signal power is affected by pathloss quantifiable by (5). As a result, the received spoofer SNR varies with the proximity to the spoofer transmitter. To provide an average measure of performance enhancement arising from utilizing the proposed technique, the average probability of error, $\overline{P}_e$, can be defined as

$$\overline{P}_e = \int_{\rho_{\min}}^{\rho_{\max}} P_e\left(\rho^{(\mathrm{sp})}\right) d\rho^{(\mathrm{sp})}. \qquad (21)$$

Figure 10 shows $\overline{P}_e$ for various N based on $\kappa^{(a)} = \kappa^{(\mathrm{sp})} = 1$ and $\rho^{(a)} = 15$ (dB), and for $\rho_{\min} = 15$, $\rho_{\max} = 25$ (dB). The effect of diversity is further emphasized in this figure where the average probability of error decreases by increasing N such that $\overline{P}_e \simeq 0.19$ for $N = 20$, implying that the proposed technique is very effective in reducing the spoofer effectiveness in the target area.

4. Conclusions

A multi-hypothesis detection problem was formulated based on a likelihood ratio test applicable to GNSS spoofing detection. A straight forward spoofing detection technique based on signal power measurements was proposed and was shown to be effective for verifying the authenticity of the received GNSS signals in urban multipath environments, meaning that the spoofer signal power is abnormally higher than that of the authentic signal when the receiver is in the proximity of the standoff spoofer.

The proposed processing was further extended to exploit extra diversity branches made available based on a moving handheld receiver and was shown to further improve the spoofer detection performance. Unlike the previously proposed antispoofing techniques, the proposed technique does not require any hardware modification and can be readily applied to any handheld GNSS receiver with minimal firmware changes. It was shown that the proposed technique is largely insensitive to uncertainties in the statistical properties of the multipath channel as long as the collected signal samples are not strongly correlated. A suboptimal detector was proposed and effectively applied to a generalized Rician channel in which the channel parameters are not available to the receiver. An extensive statistical analysis was performed to assess the performance of the proposed technique. It was shown that the average probability of error can be reduced to less than 20% in a typical urban environment.

References

[1] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications*, Artech House, Norwood, Mass, USA, 2006.

[2] 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 the International Technical Meeting (ITM '10)*, pp. 868–882, San Diego, Calif, USA, January 2010.

[3] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: development of a portable gps civilian spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '08)*, pp. 1198–1209, Savanna, Calif, USA, September 2008.

[4] F. S. T. V. Diggele, *A-GPS: Assisted GPS, GNSS, and SBAS*, Artech House, 2009.

[5] L. Scott, "Location assurance," *GPS World*, vol. 18, no. 7, pp. 14–18, 2007.

[6] W. C. Jakes, *Microwave Mobile Communications*, IEEE Press, New York, NY, USA, 1974.

[7] A. Broumandan, J. Nielsen, and G. Lachapelle, "Indoor GNSS signal acquisition performance using a synthetic antenna array," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 2, pp. 1337–1350, 2011.

[8] V. Dehghanian, *Generalized diversity gain of a mobile antenna [Ph.D. thesis]*, Electrical and Computer Engineering, University of Calgary, Calgary, Canada, 2011.

[9] V. Dehghanian, J. Nielsen, and G. Lachapelle, "Combined spatial-polarization correlation function for indoor multipath environments," *IEEE Antennas and Wireless Propagation Letters*, vol. 9, pp. 950–953, 2010.

[10] V. Dehghanian, J. Nielsen, and G. Lachapelle, "Diversity gain through antenna blocking," *International Journal of Antennas and Propagation*, vol. 2012, Article ID 735080, 6 pages, 2012.

[11] G. E. Corazza, C. Caini, A. Vanelli-Coralli, and A. Polydoros, "DS-CDMA code acquisition in the presence of correlated fading—part I: theoretical aspects," *IEEE Transactions on Communications*, vol. 52, no. 7, pp. 1160–1168, 2004.

[12] C. Caini, G. E. Corazza, and A. Vanelli-Coralli, "DS-CDMA code acquisition in the presence of correlated fading—part II: Application to cellular networks," *IEEE Transactions on Communications*, vol. 52, no. 8, pp. 1397–1407, 2004.

[13] S. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, vol. 2, Prentice-Hall, Upper Saddle River, NJ, USA, 1998.

[14] H. L. VanTrees, *Detection Estimation and Modulation Theory: Part IV*, John Wiley & Sons, NewYork, NY, USA, 2002.

[15] V. Dehghanian, J. Nielsen, and G. Lachapelle, "Combined spatial-polarization correlation function for indoor multipath environments," in *Proceedings of the 7th International Symposium on Wireless Communication Systems (ISWCS '10)*, pp. 874–876, September 2010.

[16] A. S. Y. Poon and D. N. C. Tse, "Degree-of-freedom gain from using polarimetric antenna elements," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 5695–5709, 2011.