Hindawi Publishing Corporation
International Journal of Navigation and Observation
Volume 2012, Article ID 501679, 9 pages
doi:10.1155/2012/501679

Research Article

Effectiveness of GNSS Spoofing Countermeasure Based on Receiver CNR Measurements

J. Nielsen, V. Dehghanian, and G. Lachapelle

Position Location and Navigation Group, University of Calgary, Calgary, AB, Canada T2N 1N4

Correspondence should be addressed to V. Dehghanian, vdehghan@ucalgary.ca

Received 2 January 2012; Revised 4 May 2012; Accepted 30 May 2012

Academic Editor: Dennis M. Akos

Copyright © 2012 J. Nielsen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A perceived emerging threat to GNSS receivers is posed by a spoofing transmitter that emulates authentic signals but with randomized code phase and Doppler 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. In this paper, a simple and readily implementable processing rule based on CNR estimates of the correlation peaks of the despread GNSS signals is developed expressly for reducing the effectiveness of such a spoofer threat. Consequently, a comprehensive statistical analysis is given to evaluate the effectiveness of the proposed technique in various LOS and NLOS environments. It is demonstrated that the proposed receiver processing is highly effective in both line-of-sight and multipath propagation conditions.

1. Introduction

GNSS satellites are approximately 20,000 km away and transmit several watts of signal power such that at the ground level, the power output of a 3-dB gain linearly polarized antenna is nominally −130 dBm [1]. As such, a modest jammer can easily disrupt GNSS signals by increasing the noise floor, making the acquisition of GNSS signals rather difficult. A high processing gain based on a long integration time is one of the possible countermeasures to overcome a noise jammer. Nevertheless, if the GNSS receiver undergoes random motion and is subjected to multipath fading as in a typical urban environment, then the channel decorrelates quickly such that attaining such large processing gains to overcome the jamming is not feasible. However, 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. Also the 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].

A more insidious threat is the standoff spoofer which broadcasts a set of replicas of the authentic SV signals currently visible to the mobile GNSS receiver [2]. The unaware receiver computes the navigation solution based on these counterfeit signals which are passed on to the user as being reliable with potentially damaging consequences. GNSS-based location estimates that are inaccurate but assumed to be accurate are potentially more damaging to the user than in the jamming case where at least the user knows that the service is temporarily unavailable. As the receiver processing gain used for suppressing the jammer is not applicable in the case of the spoofer signal, the spoofer transmit power can be orders of magnitude less than that of the noise jammer. This makes the spoofer signal much more difficult to locate and disable.

There are essentially two categories of spoofer threats envisioned. The first is the self-intentional spoofer that provides the user a means of compromising its GNSS position. An example is a fishing vessel wishing to enter prohibited areas undetected by a GNSS-based monitoring system. A collocated spoofer could provide counterfeit signals to fabricate navigation solution that falls outside the prohibited area [4, 5]. Another example is that of an offender required to wear a mandatory GNSS tracker to ensure compliance with travel restrictions [2].

The second type of spoofers is the standoff spoofer (SS) that could be used in urban areas for malicious purposes ranging from sporadic disruptive hacking to sophisticated

organized terrorist activities. The SS is illustrated in Figure 1 which covers a target area as a sector of an annulus ring. Multiple SS devices could potentially be used to collectively cover a given area such as an urban downtown core. Based on this, the perceived spoofer threat is a network of terrestrial SSs that can cause widespread disruption of GNSS-based location services in dense urban areas.

The SS is of interest in this paper specifically for the scenario of a terrestrial transmitter source that broadcasts replicas of the GNSS signals that are visible in the target area illustrated in Figure 1. Disruption of GNSS services in the target area is achieved by randomly modulating the code phase over a small region of the overall Code-Delay Space (CDS) that is commensurate with the target area. Therefore, at least two correlation peaks will be observed in the CDS. An unsuspecting receiver detects the larger of the correlation peaks which can belong to the spoofer signal. The code phase and the Doppler associated with the spoofer signal are then passed onto the tracking segment and consequently a false navigation solution is generated. Note that, while the target area depicted in Figure 1 has hard boundaries, such boundaries are generally blurry and not well defined. The effectiveness of the SS is considered to drop off outside the depicted annulus sector region with vague boundaries between radii R_1 and R_2. In a typical scenario, R_1 and R_2 are envisioned to be of the order of about 500 m and 2 km such that each SS covers an area of several square kilometres. A modest network of SS devices can then adequately cover a downtown core area. However, for sake of simplicity, only a single isolated SS will be considered in this paper.

The SS is assumed to remain synchronized with currently visible GNSS signals and then synthesize a set of GNSS signals corresponding to the target area. The objective of the SS is not to synthesize a specific counterfeit location for a specific GNSS receiver within the target area. This is not possible as the location of the GNSS receiver is not known to the SS. Furthermore, the objective of the SS is disruption over the general target area rather than affecting specific receivers. As such, the SS transmission signal synthesis does not have to be overly sophisticated. It matches the Doppler offset of the replicated SV signals and adjusts the code phase such that it is commensurate with the intended target region. Note that an urban area is a primarily non-line-of-sight (NLOS) multipath channel. Therefore, the Doppler spectrum as perceived by the GNSS receiver will be spread by an amount commensurating with the magnitude of the receiver velocity but will not be sensitive to direction. Hence, other than the deterministic Doppler offset of the SV to stationary ground-based receiver, no further modulation of the Doppler is required by the SS to ensure a plausible counterfeit signal. The typical handheld consumer GNSS receiver coherently integrates the signal for about 10 to 20 ms. Based on this, the correlation peak in the CDS will have 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 inertial means such that the receiver velocity vector is known, this cannot be used to discriminate the SS signal as multipath Doppler spreading occurs for both the SS and the authentic signals.

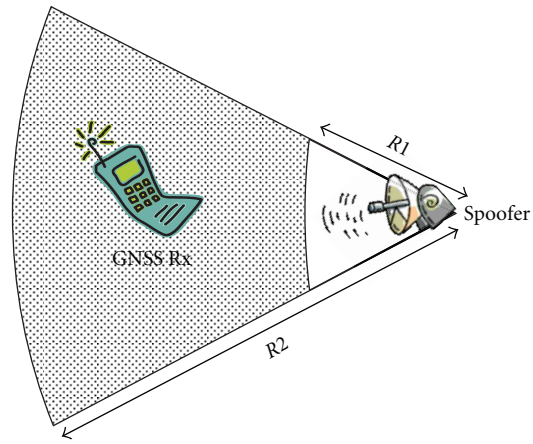


Figure 1: Standoff Spoofer (SS) illuminating a target area which is a sector of an annulus extending from R_1 to R_2.

The code phase of the SS transmissions matches the nominal code phase of the authentic GNSS signals in the target area. Note that the target area is limited to one or two kilometres and hence, the code phase only differs by several chips from one extreme of the target area to the other. For example, in a 90-degree sector with $R_1 = 500$ m and $R_2 = 1500$ m, the average spread is only about four chips. The SS generated code phase will correspond to a random location within the target area generated by slowly and randomly modulating the code phase over a small domain commensurating with the dimensions of the target area. Note that a sophisticated GNSS receiver can potentially discriminate against the SS signal based on the code phase corresponding to an outlier navigation solution. However, as the target region is not very large, the counterfeit SS navigation solutions will be plausible and cannot be easily dismissed as outliers. Furthermore, the typical consumer grade GNSS unit does not possess processing to track multiple candidate navigation solutions let alone discriminate plausible outliers. Also, receiver autonomous integrity monitoring (RAIM) and fault detection and exclusion (FDE) are not effective in detecting such navigationally consistent spoofing signals [4]. Finally, it should also be mentioned that typically 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 [7]. Hence, there is a diminishing gain for the spoofer attempting to affect an area larger than this.

As stated earlier, current consumer-grade receivers are equipped with RAIM and FDE which are not effective in mitigating the navigationally consistent spoofing attacks. A more sophisticated countermeasure to the SS with a random code delay modulation is to carefully tracking all combinations of possible navigation solutions and then dismissing solutions that are less likely based on tracking records spanning several tens of seconds up to the current time. This solution likelihood can be augmented with the use of ancillary sensors and other prior knowledge or belief maps [8]. However, the consumer-grade GNSS receivers considered

herein are assumed not to possess this level of sophistication. Rather, the objective is to address a computationally efficient processing method that can be added to relatively unsophisticated consumer grade GNSS receivers and that will be effective in discriminating against the SS. Such processing is based on the received carrier-to-noise ratio (CNR) measurements of the received GNSS signals. CNR measurement is an integrated part of all GNSS receivers as the navigation algorithm heavily relies on determining the weight of the observables based on measuring the instantaneous CNR. A simple discriminant is that if the CNR is implausibly high then an SS is suspected. Such processing is easily implemented with essentially minor firmware changes to the receiver or an in-line filter component [2]. However, there is the question of how to optimally set the threshold used for CNR comparison. The optimum threshold is easily determined and justified for LOS propagation with a known antenna gain and orientation. However, for a handheld unit operating in an urban canyon with a compromised multiband antenna that is randomly oriented and potentially shadowed, setting the optimum threshold is no longer deterministic nor trivial. Optimization is necessarily based on a statistical analysis, which is the focus of this paper.

The rest of the paper is organized as follows. In Section 2, the system definition and simplifying assumptions are given. A difficulty encountered with the statistical assessment of the SS effectiveness is the plethora of disparate parameters and plausible scenarios encountered. For this paper, a constrained set of idealized parameters and assumptions is necessary to obtain fundamental insights. In Section 3, the effectiveness of the SS and the receiver countermeasures is considered for a variety of LOS and NLOS scenarios. Section 3.5 relates these findings to the plausible physical coverage range of the SS. Finally, Section 4 states the major conclusions.

2. System Description and Assumptions

The performance of spoofer detection based on a threshold applied to the CNR in conjunction with a simple decision rule is analyzed for various propagation conditions. To do this in a comprehensive manner that is not obscured by details, it is necessary to use simplifying assumptions and constraints. While these may erode generality, the benefit is a set of insights gained that are applicable to less idealized and more realistic scenarios.

It is assumed that the GNSS receiver performs a reduced search over the CDS based on traditional despreading correlation processing for each candidate GNSS signal that is potentially visible to the receiver. Assuming that both the authentic and SS signals are present at the receiver for a given despread GNSS signal, the outcome is a set of two correlation peaks corresponding to the spoofer and the authentic signal. The complex amplitude of the authentic and spoofer correlation peaks is represented as

$$\begin{aligned} x^a &= \sqrt{\rho_{a_0}} h_a + w_a, \\ x^s &= \sqrt{\rho_{s_0}} h_s + w_s, \end{aligned} \tag{1}$$

where ρ_{a_0} and ρ_{s_0} are the average CNRs of the authentic and SS signals, respectively. The complex channel gains are denoted by h_a and h_s with $E[|h_a|^2] = E[|h_s|^2] = 1$ where E denotes the expected value operation. Also w_a and w_s represent the normalized white Gaussian noise samples distributed according to $\mathrm{CN}(0, 1)$ with $\mathrm{CN}(\mu, \sigma^2)$ denoting a circularly normal multivariate distribution with a mean of μ and a variance of σ^2. Note that the noise variance is normalized to simplify the expressions to follow.

It is assumed that there are nominally two correlation peaks in the CDS hypothesis space that correspond to the spoofer and the authentic signal for a specific GNSS signal with sample-based CNRs denoted as ρ_s and ρ_a, respectively, namely,

$$\begin{aligned} \rho_a &\equiv |x^a|^2 - 1, \\ \rho_s &\equiv |x^s|^2 - 1. \end{aligned} \tag{2}$$

There are many variations as to how the receiver implements the correlation search over the CDS; however, this assumption of the correlator structure simplifies the system description and subsequent analysis. Furthermore, the possibility of the authentic signal resulting in two distinct correlation peaks due to resolvable multipath or poor receiver design is not considered. The GNSS receiver cannot determine which correlation peak corresponds to the desired authentic signal. However, recognizing that there are two possible choices from which it suspects spoofer activity, it can impose the following simple heuristic rule for selecting the authentic signal:

> Choose the larger of the two peaks as the authentic peak if $(\rho_s < \rho_T) \cap (\rho_a < \rho_T)$, otherwise choose the smaller peak.

Here ρ_T is a threshold CNR that ρ_s and ρ_a will be compared to, which is the subject of some adaptive optimization process. Based on this formulation, the probability of a selection error can be evaluated. An error occurs every time the spoofer correlation peak is selected instead of the authentic peak with the Doppler and code delay coordinates passed on to the navigation solution processor. As such there are two types of errors described as

$$\begin{aligned} &\text{type I error: } \{(\rho_s < \rho_T) \cap (\rho_a < \rho_T)\} \cap (\rho_a < \rho_s), \\ &\text{type II error: } \{(\rho_s > \rho_T) \cup (\rho_a > \rho_T)\} \cap (\rho_s < \rho_a). \end{aligned} \tag{3}$$

A graphical aid is introduced in Figure 2 which provides a method of calculating the probability of receiver error as the sum of the probabilities of the two types of errors. This probability will be denoted as P_e and is a measure of the effectiveness of the spoofer; that is, the higher P_e is over a given target area of the spoofer, the more effective it is, and is therefore a suitable metric for quantifying the effectiveness of the SS. P_e depends on the probability density function (PDF) of the CNRs of the authentic and spoofing correlation peaks.

To proceed further, the following definitions are made:

$f_a(\rho_a;\rho_{a_0})$: PDF of ρ_a with the parameter ρ_{a_0};

$f_s(\rho_s;\rho_{s_0})$: PDF of ρ_s with the parameter ρ_{s_0};

$F_a(\rho_a;\rho_{a_0}) = \int_0^{\rho_a} f_a(\lambda;\rho_{a_0})d\lambda$: cumulative distribution of the authentic signal;

$F_s(\rho_s;\rho_{s_0}) = \int_0^{\rho_s} f_s(\lambda;\rho_{s_0})d\lambda$: cumulative distribution of the authentic signal.

Assuming that the authentic and the spoofer CNR samples, $\{\rho_a, \rho_s\}$, are statistically independent random variables, then the joint PDF can be expressed as the product of

$$f_{a,s}(\rho_a,\rho_s;\rho_{a_0},\rho_{s_0}) \approx f_a(\rho_a;\rho_{a_0})\, f_s(\rho_s;\rho_{s_0}). \tag{4}$$

This assumption is based on the authentic SV original signal and the terrestrial source SS signal coming from different bearings and hence, in a dense urban area, the fast fading and nominal path-loss is independent. As the bearings are sufficiently different, the longer-term fading or shadowing is not correlated [6]. Hence, the assumption of independence implied by (4) is made herein. However, there are instances where shadowing does become correlated especially if the bearings of the authentic and SS signals are similar. Based on the graphic shown in Figure 2, P_e is given by

$$\begin{aligned} P_e &= \int_0^{\rho_T} f_s(\rho_s)\left(\int_0^{\rho_s} f_a(\rho_a)d\rho_a\right)d\rho_s \\ &\quad + \int_{\rho_T}^{\infty} f_a(\rho_a)\left(\int_0^{\rho_a} f_s(\rho_s)d\rho_s\right)d\rho_a \\ &= \int_0^{\rho_T} f_s(\rho_s)\left(F_a(\rho_s) - F_a(0)\right)d\rho_s \\ &\quad + \int_{\rho_T}^{\infty} f_a(\rho_a)\left(F_s(\rho_a) - F_s(0)\right)d\rho_a, \end{aligned} \tag{5}$$

where the simplified notation omits the parameters ρ_{s_0} and ρ_{a_0} which are initially assumed to be known parameters. Using $F_a(0) = F_s(0) = 0$, (5) becomes

$$P_e = \int_0^{\rho_T} f_s(\rho_s)F_a(\rho_s)d\rho_s + \int_{\rho_T}^{\infty} f_a(\rho_a)F_s(\rho_a)d\rho_a. \tag{6}$$

The minimum value of P_e can be determined by setting $(\partial/\partial\rho_T)P_e = 0$ such that the condition

$$\frac{\partial}{\partial\rho_T}\int_0^{\rho_T} f_s(\rho_s)F_a(\rho_s)d\rho_s + \frac{\partial}{\partial\rho_T}\int_{\rho_T}^{\infty} f_a(\rho_a)F_s(\rho_a)d\rho_a = 0 \tag{7}$$

emerges and reduces to

$$\frac{f_s(\rho_T)}{F_s(\rho_T)} = \frac{f_a(\rho_T)}{F_a(\rho_T)} \tag{8}$$

which is then solved for the optimum value of ρ_T. Equation (8) is mathematically equivalent to

$$f_s(\rho_T)F_a(\rho_T) - f_a(\rho_T)F_s(\rho_T) \equiv \frac{\partial}{\partial\rho_T}\left(\frac{F_s(\rho_T)}{F_a(\rho_T)}\right) = 0. \tag{9}$$

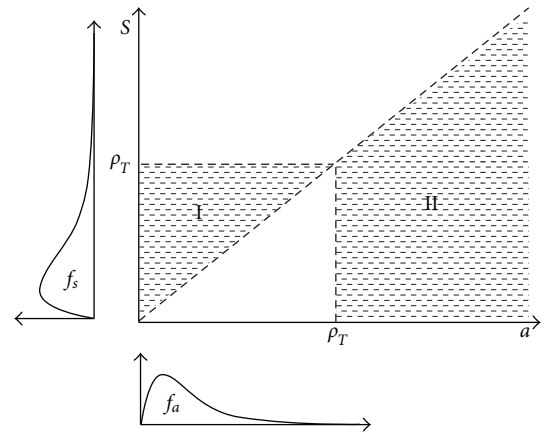


Figure 2: Graphical integration regions for the two error types.

A useful observation is that if the PDFs of the authentic and the spoofer signals are scaled versions of each other, that is, $F_a(\rho_T) = F_s(\rho_T/c)$; then (9) holds only if $\rho_T = 0$ and $\rho_T = \infty$, since a cumulative distribution function (CDF) is a monotonically increasing function. This means that a finite threshold other than $\rho_T = 0$ and $\rho_T = \infty$ does not exist. In other words, for the common case when $f_a(\rho_a)$ is a monomodal function then it is easily shown that $f_a(\rho_a)/F_a(\rho_a)$ is a monotonically decreasing function. Hence, if $f_a(\rho)$ is approximately a translation of the function $f_s(\rho)$, then the intersection points of $f_s(\rho_T)/F_s(\rho_T)$ and $f_a(\rho_T)/F_a(\rho_T)$ can only be at $\rho_T = 0$ and $\rho_T = \infty$. This observation will be used in the next section. Note that a threshold of $\rho_T = \infty$ is equivalent to having no threshold rather than applying a nonrealistically large threshold.

3. Performance of Antispoofing for LOS and NLOS Conditions

In this section, P_e is determined for LOS and NLOS scenarios. This is generally done by first solving for the optimum threshold ρ_T and then determining P_e.

3.1. LOS with Additive Noise. As defined in (1), the in-phase and quadrature components of the demodulated signal are normalized such that the additive noise is of unit variance for the in-phase and quadrature Gaussian components. With this, the LOS signal from the authentic signal will have a mean square magnitude of $2\rho_{a_0}$. Likewise the LOS from the SS will have a mean square magnitude of $2\rho_{s_0}$. Hence, the PDF of the square magnitudes of the correlation peaks corresponding to the authentic and spoofer signals will then be given as

$$\begin{aligned} f_a(\rho_a;\rho_{a_0}) &= \chi_2'^2(\rho_a; 2\rho_{a_0}, 1), \\ f_s(\rho_s;\rho_{s_0}) &= \chi_2'^2(\rho_s; 2\rho_{s_0}, 1), \end{aligned} \tag{10}$$

where $\chi_N'^2(x;\mu,\sigma^2)$ is the noncentral chi-square PDF of variable x with N degrees of freedom (DOF), the noncentrality parameter μ, and the corresponding variance of the Gaussian

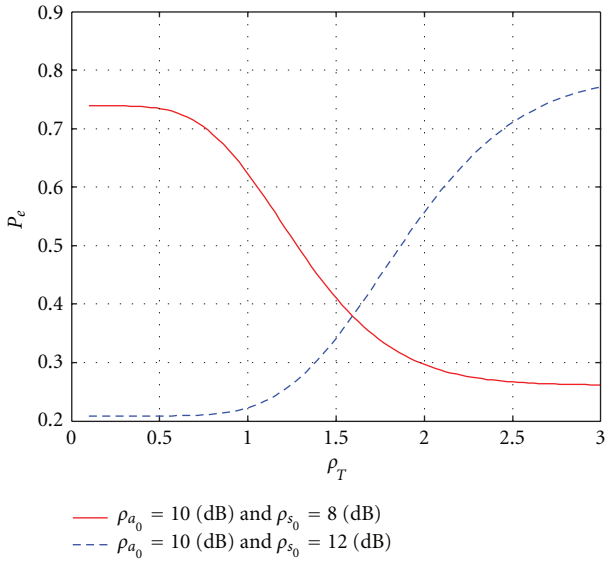


Figure 3: P_e as a function of ρ_T.

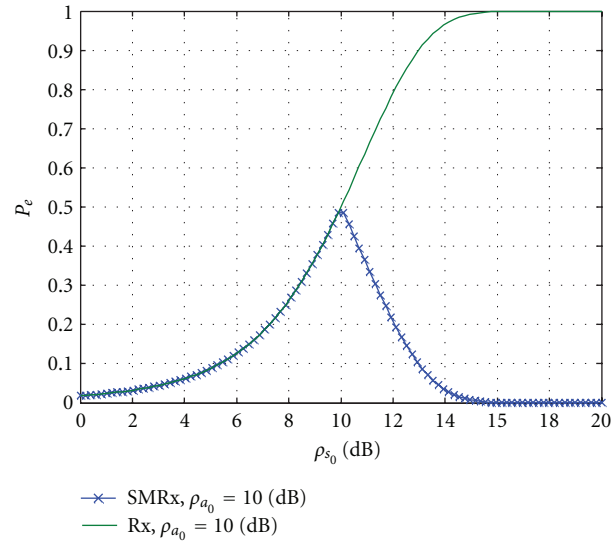


Figure 4: P_e as a function of ρ_{s_0} for a conventional receiver (Rx) and a spoofer mitigated receiver (SMRx).

parameter σ^2 [9]. P_e is plotted in Figure 3 as a function of ρ_T for specific cases where $\rho_{a_0} > \rho_{s_0}$ and $\rho_{a_0} < \rho_{s_0}$. As stated earlier, when $\rho_{a_0} > \rho_{s_0}$ the optimum threshold is $\rho_T = \infty$, while for $\rho_{a_0} < \rho_{s_0}$ the optimum threshold is $\rho_T = 0$. This is tantamount to selecting the larger of the two peaks if the average power of the authentic signal is larger than the average power of the spoofer. Otherwise, choose the smaller of the two peaks if the average power of the spoofer is larger than the average power of the authentic signal. This trivial conclusion is a manifestation of the assumption that ρ_{a_0} and ρ_{s_0} are known, which is not generally the case.

Note that as $f_a(\rho)$ is approximately a translation of the function $f_s(\rho)$ then the intersection points of $f_s(\rho_T)/F_s(\rho_T)$ and $f_a(\rho_T)/F_a(\rho_T)$ can only be at $\rho_T = 0$ and $\rho_T = \infty$ as observed before.

Figure 4 shows a plot of P_e for a receiver with no spoofer mitigation, herein denoted by Rx, compared to the P_e for a receiver with spoofer mitigation, herein denoted by SMRx, with $\rho_T = \infty$ for $\rho_{a_0} > \rho_{s_0}$ and $\rho_T = 0$ for $\rho_{a_0} < \rho_{s_0}$. The GNSS receiver with no spoofer mitigation is equivalent to setting $\rho_T = \infty$. As such there is no difference in the performance of the GNSS receivers with and without spoofer mitigation when $\rho_{a_0} > \rho_{s_0}$. However, for the case of $\rho_{a_0} < \rho_{s_0}$, the effectiveness of the spoofer mitigation is clearly evident in the reduction of P_e.

3.2. NLOS with Additive Noise. In this section, it is assumed that ρ_{a_0} and ρ_{s_0} are again deterministic and known to the receiver. The PDFs of the magnitude of the correlation peaks corresponding to the authentic and spoofer signals are then be given as

$$f_a(\rho_a;\rho_{a_0}) = \chi_2^2(\rho_a;\rho_{a_0}),$$
$$f_s(\rho_s;\rho_{s_0}) = \chi_2^2(\rho_s;\rho_{s_0}), \quad (11)$$

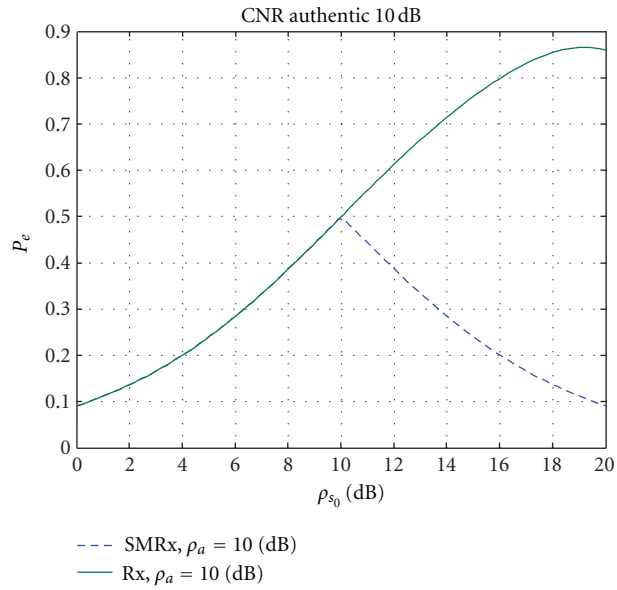


Figure 5: Comparison of the conventional and the spoofer mitigation receiver based on 2 DOF in a NLOS Rayleigh fading channel.

where $\chi_2^2(x;\sigma^2)$ is the central chi-square PDF of variable x with 2 DOF, with a variance of each DOF of $\rho_{a_0} + 1$ for the authentic signal and $\rho_{s_0} + 1$ for the spoofing signal.

Figure 5 shows a plot of P_e for a receiver with no spoofer mitigation (Rx) compared to the P_e for a receiver with spoofer mitigation (SMRx) with $\rho_T = \infty$ for $\rho_{a_0} > \rho_{s_0}$ and $\rho_T = 0$ for $\rho_{a_0} < \rho_{s_0}$. Comparing Figure 5 with Figure 4, it is evident that the spoofer mitigation is more effective when a LOS rather than a NLOS scenario is encountered. Hence, when the spoofer and authentic signals are more random as in the NLOS case, distinguishing them based on the sample CNR is more difficult and hence, subject to higher P_e.

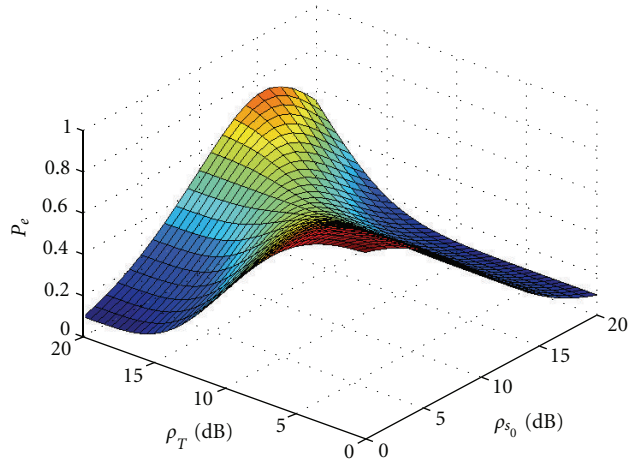


FIGURE 6: P_e as a function of ρ_T and ρ_{s_0}, for $\rho_{a_0} = 10$ and NLOS Rayleigh conditions based on 2DOF.

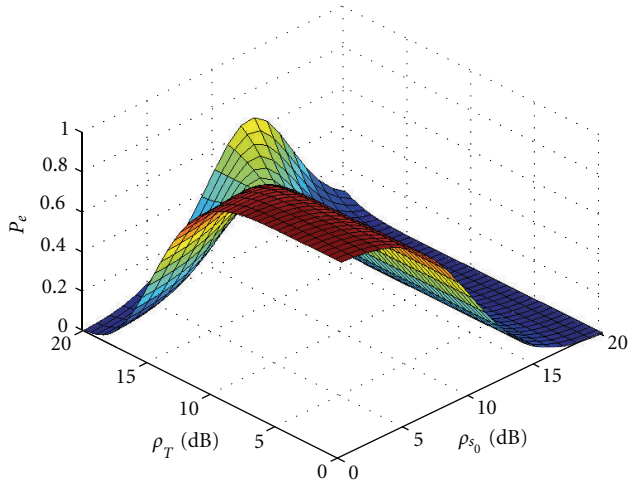


FIGURE 7: P_e as a function of ρ_T and ρ_{s_0}, for $\rho_{a_0} = 10$ and NLOS conditions based on $M = 3$ (6DOF).

Figure 6 shows P_e as a function of ρ_T and for various ρ_{s_0}. The effectiveness of the spoofer countermeasure is again evident in the region where $\rho_{a_0} < \rho_{s_0}$. The same behavior as before occurs, namely, that the optimum ρ_T for spoofer power less than authentic power is $\rho_T = \infty$ while for spoofer power greater than authentic power is $\rho_T = 0$, which is again a manifestation of the assumed known average powers.

3.3. Diversity NLOS with Additive Noise. Assuming a ring or a sphere of scatterers to model a typical urban environment, the signals arriving at antennas with an approximate separation of half a carrier wavelength, are statistically uncorrelated. Consequently, M statistically independent samples of the receiver correlator output can be made available through accumulating M successive samples of the correlator outputs as the receiver is moving. The CNR of each correlation sample is ρ_{a_0} and ρ_{s_0} for the authentic and spoofing signals, respectively, which are again assumed to be deterministic and known to the receiver.

A plot of P_e based on $M = 3$ independent samples is shown in Figure 7. Similar to the no diversity case with $M = 1$, the optimum ρ_T for spoofer power less than the authentic power is $\rho_T = \infty$, while for spoofer power greater than the authentic power, the maximum is $\rho_T = 0$. Again, this is reasonable as the spoofer and authentic signal is identically distributed except for the deterministic and known average powers. Clearly, if it is known that $\rho_{a_0} > \rho_{s_0}$ then the larger peak would correspond to the authentic signal more often than the lower peak.

3.4. Measurement Uncertainty and Unknown Spoofer Average Power. In the previous sections, the outcome was a trivial optimization of ρ_T as $\rho_T = 0$ if $\rho_{a_0} < \rho_{s_0}$ and $\rho_T = \infty$ if $\rho_{a_0} > \rho_{s_0}$, which resulted from the assumption that $\{\rho_{s_o}, \rho_{a_o}\}$ was known to the receiver. In this section, the more realistic multipath propagation case is considered where the average spoofer CNR is completely unknown. This is reasonable as the spoofer could be of arbitrary transmit power and range from the receiver. However, it will be assumed that ρ_{a_0} is known approximately to the receiver. This is reasonable as the average power of a GNSS SV signal is approximately known in a multipath environment with the exception of factors such as shadowing and building penetration losses. Antenna orientation is typically not a factor as the multipath is distributed across a large angular sector.

As ρ_{s_0} is unknown, it is reasonable to assume a uniform PDF for ρ_s such that $f_s(\rho_s) = c_s$ where c_s is a constant. Consequently, P_e can be found from (6) as

$$P_e = c_s \int_0^{\rho_T} F_a(\rho_a)\, d\rho_a + c_s \int_{\rho_T}^{1/c_s} a f_a(\rho_a)\, d\rho_a. \tag{12}$$

Now the optimum ρ_T can be found from $\partial P_e(\rho_T)/\partial \rho_T = 0$ which simplifies to

$$F_a(\rho_T) - \rho_T f_a(\rho_T) = 0. \tag{13}$$

Equation (13) can be solved to find the optimum ρ_T. Figure 8 shows $F_a(\rho_T) - \rho_T f_a(\rho_T)$ for $M = 1, \ldots, 4$ based on a Rayleigh fading channel and $\rho_{a_0} = 10$ (dB). As can be seen from this figure, $\rho_T = \infty$ is optimum for $M = 1$. This means that a finite threshold does not exist for $M = 1$ and as such the proposed spoofing countermeasure does not reduce the spoofer effectiveness as $\rho_T = \infty$ is equivalent to a receiver with no spoofing countermeasure. However, as the diversity order increases, an optimum ρ_T other than 0 or ∞ can be found from (13). As will be shown in the next section, the optimum value of ρ_T reduces P_e and as such reduces the spoofer effective range.

3.5. Relating Observations of Spoofer Effectiveness to Physical Range. Having evaluated P_e for various scenarios, it is of interest to determine the spoofer effectiveness as a function of the physical range. The potential target area of the spoofer as illustrated in Figure 1 is conceptually the physical region in which P_e is large enough to impact the navigation solution. In this section, an approximation of the physical range of

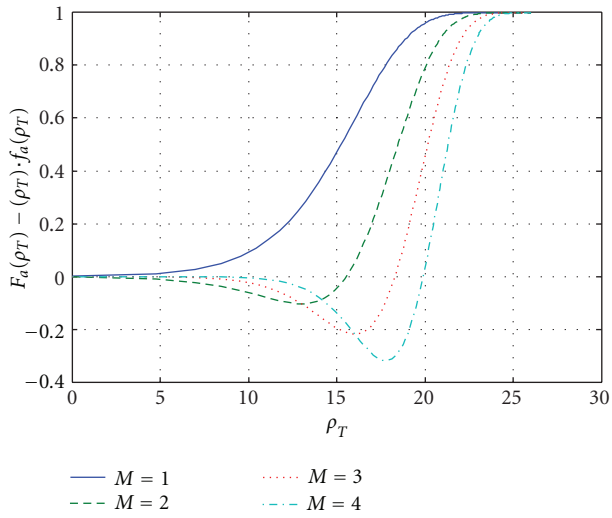


FIGURE 8: $F_a(\rho_T) - \rho_T f_a(\rho_T)$ as a function of ρ_T for various number of diversity branches based on a NLOS Rayleigh fading channel and $\rho_{a_0} = 10$ (dB).

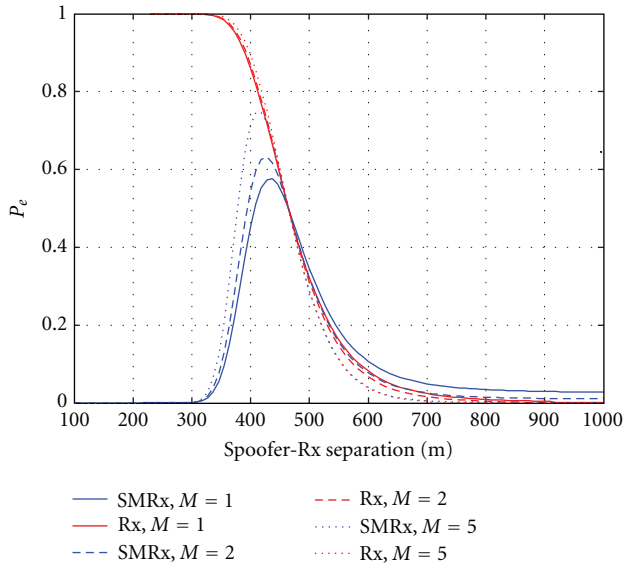


FIGURE 9: P_e as a function of spoofer-Rx separation in a LOS channel with measurement errors and based on $\rho_{a_0} = 10$ (dB), $\rho_{s_0}(R_1) = 30$ dB, and a path-loss exponent of $n = 3$.

spoofer effectiveness is determined based on the empirical path-loss model of order n as

$$\rho_{s_0} = \rho_{s_0}^{(R_1)} - 10n \log_{10}\left(\frac{d}{R_1}\right), \tag{14}$$

where R_1 is a reference range, d is the spoofer-receiver range, n is the path-loss exponent, and $\rho_{s_0}^{(R_1)}$ is the average received spoofer CNR at $d = R_1$.

For a LOS scenario with measurement errors, the PDFs of the SS CNR and SV CNR estimates are noncentral chi-square with $2M$ DOF with M denoting the number independent

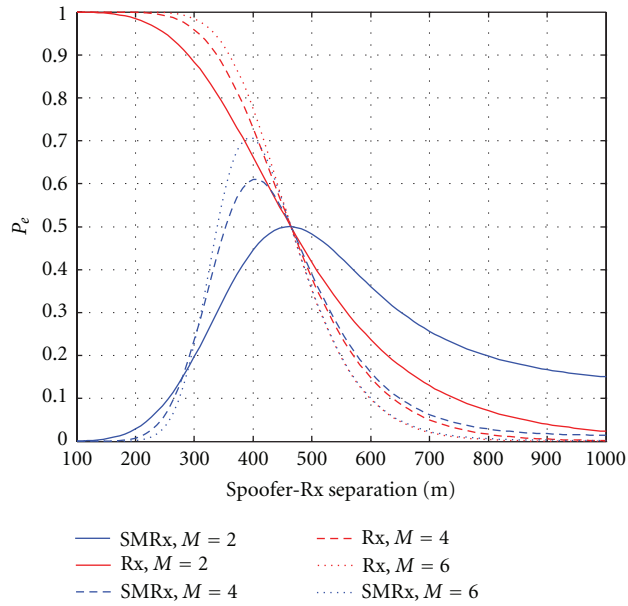


FIGURE 10: P_e as a function of spoofer-Rx separation in a Rayleigh channel and based on $\rho_{a_0} = 10$ (dB), $\rho_{s_0}(R_1) = 30$ dB, and a path-loss exponent of $n = 3$.

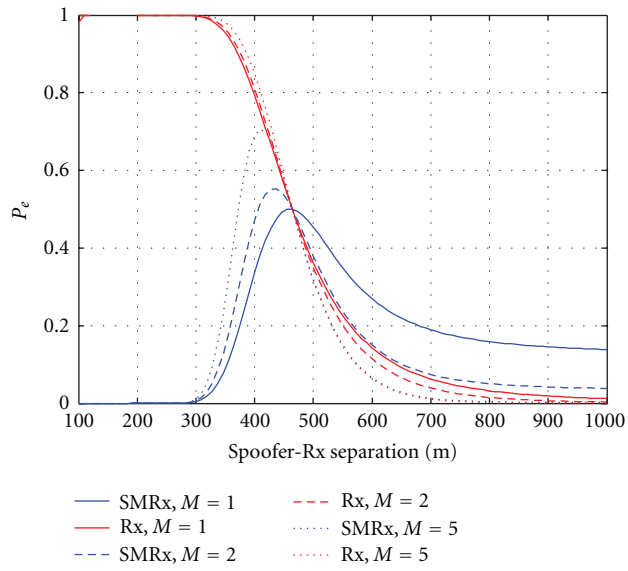


FIGURE 11: P_e as a function of spoofer-Rx separation in a Rician channel with $K_a = K_s = 1$ and based on $\rho_{a_0} = 10$ (dB), $\rho_{s_0}(R_1) = 30$ dB, and a path-loss exponent of $n = 3$.

diversity branches used to estimate the CNR. P_e can therefore be found by computing ρ_T using (13) and substituting it in (6). Figure 9 shows P_e for the spoofer mitigated receiver (SMRx) as well as a conventional Rx for various spoofer-receiver separations and M. As can be seen from this figure, aSMRx significantly reduces the effectiveness of the spoofer through reducing P_e. Also observed is that the higher the diversity order M is, the more effective the spoofer mitigation

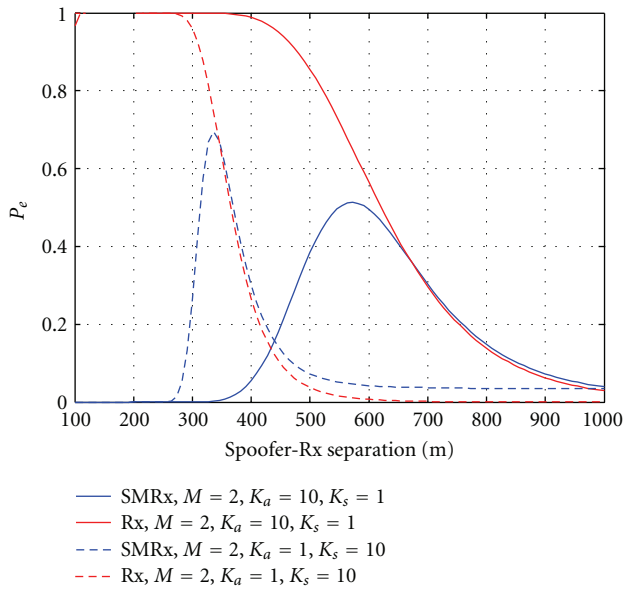


Figure 12: P_e as a function of spoofer-Rx separation in a Rician channel based on $\rho_{a_0} = 10\,(\text{dB})$, $\rho_{s_0}(R_1) = 30\,\text{dB}$, and a path-loss exponent of $n = 3$.

is. For a Rayleigh fading channel, the PDFs of the spoofer and the authentic CNRs are central chi-square with $2M$ DOF. P_e can be found by numerically computing ρ_T from (13) and setting it in (6). Figure 10 shows P_e for an SMRx as well as a conventional Rx with no spoofing countermeasures. Note that the performance of the SMRx is significantly better than that of a conventional Rx with higher diversity branches resulting in better performance. In addition, Figures 11 and 12 compare the P_e of SMRx and Rx under a generalized Rician channel with various K-factors such that [10]

$$f_a(\rho_a;\rho_{a_0}) = \chi'^2_{2M}\left(\frac{K_a}{K_a+1}\rho^2_{a_0}, \frac{1}{K_a+1}\rho_{a_0}+1\right),$$
$$f_s(\rho_s;\rho_{s_0}) = \chi'^2_{2M}\left(\frac{K_s}{K_s+1}\rho^2_{s_0}, \frac{1}{K_s+1}\rho_{s_0}+1\right), \quad (15)$$

where K_a and K_s are the Rician K-factors associated with the SV and the SS channels, respectively. Similar to the LOS and the Rayleigh channels, a noticable improvement spoofer mitigation is realizable. In order to quantify the reduction in spoofer effective range, a heuristic metric is introduced here as

$$\text{SRRF} = \left(\frac{\int_{R_1}^{R_2} P_e^{\text{Rx}}\,dR - \int_{R_1}^{R_2} P_e^{\text{SMRx}}\,dR}{\int_{R_1}^{R_2} P_e^{\text{Rx}}\,dR}\right) \times 100, \quad (16)$$

where SRRF denotes the spoofer range reduction factor. The SRRF is computed for various channel scenarios and diversity branches and the results are summarized in Table 1.

4. Conclusions

It was shown that a relatively unsophisticated standoff spoofer can effectively disrupt a large physical area. However, processing based on estimating the CNR of the spoofer and the authentic received signals and applying a straightforward threshold rule can significantly reduce the effectiveness of the standoff spoofer. This was shown for LOS, NLOS, and Ricean multipath conditions. If the average spoofer and authentic signal power is known then the setting of ρ_T is trivial. However, if ρ_s is completely unknown then it has a finite optimum, that is, a function of ρ_a and the type of propagation environment detected by the receiver. An expression for computing the optimum ρ_T was deduced and applied to various channels. The results demonstrated the effectiveness of the proposed spoofer mitigation technique. A heuristic metric of spoofer effectiveness (SRRF) was proposed. It was shown that SRRF is reduced by up to 75% for LOS, 45% for NLOS Rayleigh $M = 2$, and 60% for NLOS Rayleigh $M = 5$ and 70% based on a Rician channel with $K_a = K_s = 1$ for $M = 2$, hence aptly demonstrating the effectiveness of the proposed countermeasure approach.

Table 1: Spoofer range reduction factor (SRRF) computed for various channel scenarios based on $\rho_{a_0} = 10\,\text{dB}$, $\rho_{s_0}(R_1) = 30\,\text{dB}$.

	No. of diversity branches	Path-loss exponent (n)	K_a	K_s	SRRF (%)
Rician Ch.	$M = 1$	3	1	1	**60**
	$M = 2$	3	1	1	**70**
	$M = 5$	3	1	10	**75**
	$M = 5$	3	10	1	**70**
Rayleigh Ch.	$M = 2$	3	0	0	**45**
	$M = 5$	3	0	0	**60**
LOS	$M = 1$	3	NA	NA	**74**
	$M = 5$	3	NA	NA	**75**

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 *Institute of Navigation—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] L. Scott, "Location assurance," *GPS World*, vol. 18, no. 7, pp. 14–18, 2007.

[5] L. Scott, "Anti-spoofing and authenticated signal architetures for civil navigation systems," in *Proceedings of the ION GPS/GNSS*, Portland, Ore, USA, September 2003.

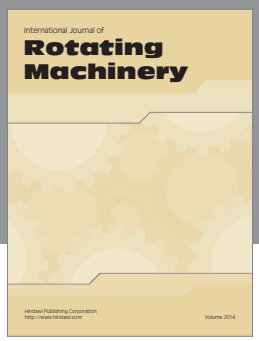
[6] W. C. Jakes, *Microwave Mobile Communications*, IEEE Press, New York, NY, USA, 1974.

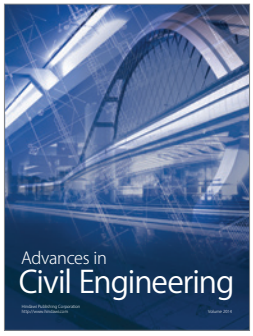
[7] F. S. T. V. Diggele, *A-GPS: Assisted GPS, GNSS, and SBAS*, Artech House, 2009.

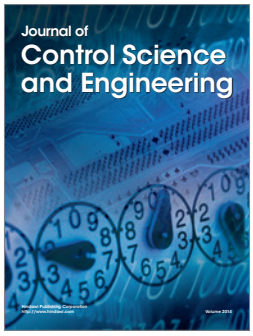
[8] S. Thurun, W. Burgard, and D. Fox, *Probabilistic Robotics*, MIT Press, 2006.

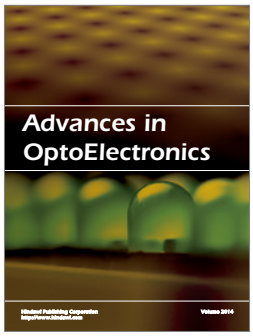
[9] S. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, vol. 2, Printice-Hall, Upper Saddle River, NJ, USA, 1998.

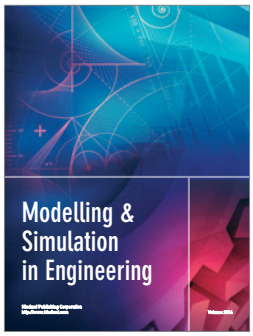
[10] J. G. Proakis, *Digital Communications*, McGraw-Hill, New York, NY, USA, 2001.

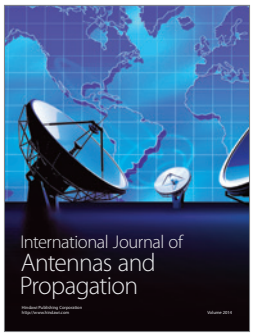


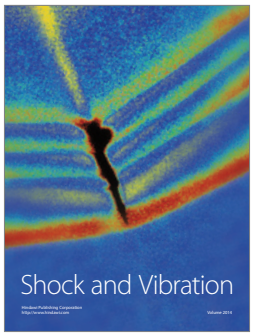


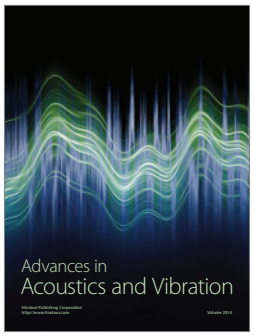












Hindawi

Submit your manuscripts at
http://www.hindawi.com