Hindawi Publishing Corporation
International Journal of Navigation and Observation
Volume 2012, Article ID 127072, 16 pages
doi:10.1155/2012/127072

Review Article

GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques

Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle

Position Location and Navigation (PLAN) Group, Schulich School of Engineering, University of Calgary, 2500 University Drive, NW, Calgary, AB, Canada T2N 1N4

Correspondence should be addressed to Ali Jafarnia-Jahromi, ajafarni@ucalgary.ca

Received 24 February 2012; Accepted 29 May 2012

Academic Editor: Elena Lohan

GPS-dependent positioning, navigation, and timing synchronization procedures have a significant impact on everyday life. Therefore, such a widely used system increasingly becomes an attractive target for illicit exploitation by terrorists and hackers for various motives. As such, spoofing and antispoofing algorithms have become an important research topic within the GPS discipline. This paper will provide a review of recent research in the field of GPS spoofing/anti-spoofing. The vulnerability of GPS to a spoofing attack will be investigated and then different spoofing generation techniques will be discussed. After introducing spoofing signal model, a brief review of recently proposed anti-spoofing techniques and their performance in terms of spoofing detection and spoofing mitigation will be provided. Limitations of anti-spoofing algorithms will be discussed and some methods will be introduced to ameliorate these limitations. In addition, testing the spoofing/anti-spoofing methods is a challenging topic that encounters some limitations due to stringent emission regulations. This paper will also provide a review of different test scenarios that have been adopted for testing anti-spoofing techniques.

1. Introduction

GPS-dependent systems are ubiquitous in current positioning and navigation applications. There is an ever-increasing attention to safe and secure GPS applications such as air, marine, and ground transportations, police and rescue services, telecommunication systems, mobile phone location, and tracking the criminal offenders. Nowadays, most mobile phones as well as vehicles are equipped with positioning and navigation systems utilizing GPS. In addition, countless time tagging and synchronization systems in the telecom and electrical power grid industries rely primarily on GPS. As a consequence, such a widely used system is becoming an increasingly attractive target for illicit disruption by terrorists and hackers.

GPS signals are vulnerable to in-band interferences because of being extremely weak broadcasted signals over wireless channels. Therefore, even a low-power interference can easily jam or spoof GPS receivers within a radius˜of several kilometres. In addition, GPS is a backward compatible technology whose signal structure is in the public domain [1]. This makes GPS technology more susceptible to disruptive interfering methods. For example, spoofing attack could effectively mislead an activity monitoring GPS receiver mounted on a cargo transport or fishing vessel. Therefore, the GPS receiver will be logging a counterfeit trajectory with various consequences.

Spoofing and antispoofing mechanisms are emerging issues in modern GPS applications that will increasingly attract research in future [1]. Spoofing is a deliberate interference that aims to coerce GNSS receivers into generating false position/navigation solutions [2]. The spoofer attempts to mimic authentic GPS signals in order to mislead the target receiver. The spoofing attack is potentially significantly more menacing than jamming since the target receiver is not aware of this threat. Recently the implementation of sophisticated spoofers has become more feasible, flexible, and less costly due to rapid advances in software-defined radio (SDR) technology [3].

In recent years, research has been initiated on spoofing discrimination and mitigation [2–9]. This paper first provides a brief review of different spoofing generation

techniques. Subsequently, the vulnerability of civilian GPS receivers to spoofing attacks will be investigated in different operational layers. Then, a brief review of current antispoofing techniques will be provided in terms of spoofing detection and spoofing mitigation. Furthermore, three test scenarios will be investigated that are useful for testing the spoofing/antispoofing algorithms in the real-world scenarios.

This paper is organized as follows: a brief discussion on different spoofing generation techniques is provided in Section 2. GPS vulnerability against spoofing attacks is investigated in Section 3, and then Section 4 demonstrates the received signal model for a GPS receiver under spoofing attack. Antispoofing techniques will be discussed in more detail in Section 5. In Section 6, the test scenarios are investigated in real spoofing environments. Concluding remarks are provided in Section 7.

2. Classification of Spoofing Generation Techniques

Spoofing generation can be divided into three main categories [2, 3, 7].

2.1. GPS Signal Simulator. In this category a GPS signal simulator concatenated with a RF front-end is employed to mimic authentic GPS signals. The signals generated by this kind of spoofer are not essentially synchronized to the real GPS signals. Therefore, the spoofing signals look like noise for a receiver operating in the tracking mode (even if the spoofer power is higher than the authentic signals). However, this type of spoofers can effectively mislead commercial GPS receivers especially if the spoofing signal power is higher than the authentic signals. A GPS signal simulator is the simplest GPS spoofer and it can be detected by different antispoofing techniques such as amplitude monitoring, consistency checks among different measurements, and consistency check with inertial measurement units (IMUs).

2.2. Receiver-Based Spoofers. A more advanced type of spoofer consists of a GPS receiver concatenated with a spoofing transmitter. This system first synchronizes to the current GPS signals and extracts the position, time, and satellite ephemeris, and then it generates the spoofing signal knowing the 3D pointing vector of its transmit antenna toward the target receiver antenna. This kind of spoofer is difficult to discriminate from the authentic signals and is more complicated than the first category. The main challenge toward realization of this kind of spoofer is projecting the spoofing signals to the intended victim receiver with the correct signal delay and strength. Note that the spoofing power should be slightly higher than the authentic signal power in order to successfully mislead the target receiver but it should not be much more than the typical power of GPS signals.

Aligning the carrier frequency and phase to the authentic GPS signals, minimizing the self-jamming effect and suppressing relative data bit latencies are other limitations that a receiver-based spoofer should deal with. Carrier phase alignment to the authentic signals requires centimetre level knowledge of the 3D pointing vector from the spoofer transmit antenna phase centre toward the target receiver antenna phase centre. Therefore, it would be a great advantage for this kind of spoofers if the spoofer antenna were very close to the target receiver antenna. This type of spoofers is relatively hard to detect since they are synchronized to the real GPS satellites and can spoof receivers in tracking mode. Figure 1 shows a repeater-spoofer structure proposed by [3].

2.3. Sophisticated Receiver-Based Spoofers. This category is the most complex and effective type of the spoofing categories. This type is assumed to know the centimetre level position of the target receiver antenna phase centre to perfectly synchronize the spoofing signal code and carrier phase to those of authentic signals at the receiver [7]. This type of spoofer can take advantage of several transmit antennas in order to defeat direction of arrival antispoofing techniques. In this case the spoofer needs to synthesize an array manifold that is consistent with the array manifold of the authentic signal to defeat an angle of arrival (AOA) discriminating GPS receiver.

The complexity of constructing such a spoofer is much higher than the two previous categories discussed above. Compared to the previous spoofing categories, the effectiveness region of this type of spoofer is much more limited. The reason is that carrier phase alignment and array manifold synchronization might be achieved only for a very small region where target receiver antennas are located. In addition, there are some physical limitations regarding the spoofer antenna placement relative to the target receiver antenna(s). As such, the realization of this type of spoofers is very difficult and in many cases impossible due to the geometry and movement of the target receiver antenna(s).

3. GPS Vulnerability against the Spoofing Attack

The vulnerability of GPS to spoofing can be investigated in three operational layers of GPS receivers, namely, the signal processing, data bit, and position/navigation solution levels.

3.1. GPS Vulnerability in Signal Processing Level. The structure of GPS signals, including the modulation type, pseudorandom noise (PRN) signals, transmit frequency, signal bandwidth, Doppler range, and signal strength publicly known. Furthermore, GPS is a backward compatible technology whose L1 signal features do not significantly change through different generations of GPS satellites. Most of the commercial GPS receivers are equipped with automatic gain control (AGC) block that compensates the power variations in the received GPS signal. However, AGC can increase the vulnerability of GPS receivers against higher power spoofing signals since it automatically adjusts the receiver input gain according to the more powerful spoofing signals [8]. Therefore, knowing the general structure and operational basics of a civilian GPS receiver, a spoofing module can generate counterfeit signals that are arbitrarily similar to the

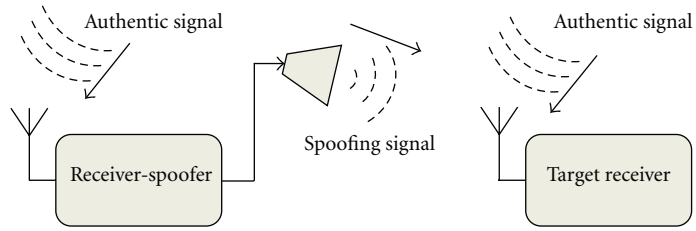

Figure 1: Repeater spoofer block diagram (modified after [3]).

authentic GPS signals such that they can effectively mislead GPS receivers.

3.2. GPS Vulnerability in Data Bit Level. The framing structure of the GPS signals is publicly known. The navigation frame consists of different parts such as almanac, telemetry information, and satellite ephemeris. This information does not change rapidly during short time intervals; for example, the satellite ephemeris information can be acquired in less than 1 minute but it remains unchanged for 12.5 minutes [1]. Therefore, the spoofer can take advantage of this stability in order to regenerate the GPS data frame. In addition, the satellite health status bits can be manipulated by a spoofer in order to mislead the receiver toward rejecting the valid satellite signals [10].

3.3. GPS Vulnerability in Navigation and Position Solution Level. The spoofer can inject counterfeit pseudorange measurements into the receiver, leading to a wrong position, velocity, and time (PVT) solution. The PVT error is proportional to the range residuals multiplied by a geometry related factor. In [11] the authors have developed a vulnerability index against spoofing (VIAS) that indicates the geometric relationship between GPS constellation and the spoofer position that results in receiver position solution deviations. It is assumed that the receiver is already running a receiver autonomous integrity monitoring (RAIM) procedure. Therefore, the VIAS coefficient is proposed for the case where the spoofing signal is not detected by the RAIM technique. It is shown that the VIAS changes over time and position and it has a higher value where the position dilution of precision (PDOP) value is high. The VIAS index can be used in the design and development of antispoofing methods.

In some applications, GPS receivers are strictly used for timing synchronization such as CDMA/GSM cell towers. In this case, the spoofing attack can highly disrupt the accuracy of the estimated timing, and this can seriously disturb the handoff processing between neighboring cells.

4. Received Signal Model

Antispoofing techniques can be generally investigated for two receiver categories, namely, single-antenna and multiple, antenna receivers. This section describes the received signal model for these receivers in the presence of spoofing attack.

4.1. Single Antenna Receiver. Considering the GPS L1 C/A code, the received signal subjected to a spoofing attack can be modeled as

$$r(nT_s) = \sum_{m=1}^{N_{\text{Auth}}} \sqrt{p_m^a} F_m^a(nT_s) + \sum_{q=1}^{N_{\text{Spoof}}} \sqrt{p_q^s} F_q^s(nT_s) + \eta(nT_s), \tag{1}$$

where

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

and N_{Auth} and N_{Spoof} are the number of authentic and spoofing PRN signals, respectively. The superscripts s and a refer to the spoofing and authentic signals, respectively. T_s is the sampling interval, and ϕ, f, p, and τ are the carrier phase, Doppler frequency, signal power and code delay of the received signals, respectively. In this model, $h(nT_s)$ is the transmitted navigation data bit and $c(nT_s)$ is the PRN sequence ant time instant nT_s. The subscripts m and q correspond to the mth authentic signal and qth spoofing signal, respectively. η is the complex additive white Gaussian noise with variance σ^2 and j is the square root of -1.

4.2. Multiple-Antenna Receiver. Assume an arbitrary N-element antenna array configuration. In this configuration, one antenna is chosen as the reference antenna. Without loss of generality assume that the reference coordinate system is located at the reference antenna (r_1) as shown in Figure 2. Here, it is assumed that the spoofer is a single-antenna transmitter that is transmitting several PRN signals from the same direction. Therefore, the complex baseband representation of N received spatial samples of authentic and spoofing signals impinging on the antenna array before de-spreading can be written in vector form as

$$\begin{aligned} \mathbf{r}(nT_s) = \begin{bmatrix} r_1(nT_s) \\ \vdots \\ r_N(nT_s) \end{bmatrix} &= \sum_{m=1}^{N_{\text{Auth}}} \mathbf{a}_m \sqrt{p_m^a} F_m^a(nT_s) \\ &+ \mathbf{b} \sum_{q=1}^{N_{\text{Spoof}}} \sqrt{p_q^s} F_q^s(nT_s) + \boldsymbol{\eta}(nT_s), \end{aligned} \tag{3}$$

where $\boldsymbol{\eta}$ is the $N \times 1$ complex additive white Gaussian noise vector with covariance matrix $\sigma^2\mathbf{I}$ and $\mathbf{I}$ represents a N by N

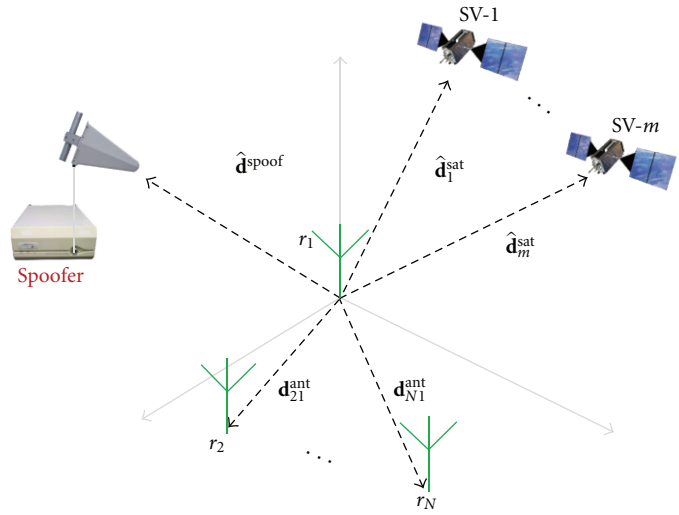

Figure 2: Multiple-antenna configuration.

identity matrix. $\mathbf{a}_m$ and $\mathbf{b}$ are steering vectors incorporating all spatial characteristics of the antenna array for authentic and spoofing signals, which can be written as

$$\mathbf{b} = \begin{bmatrix} 1 \\ b_2 \\ \vdots \\ b_N \end{bmatrix} = \begin{bmatrix} e^{-j((2\pi \mathbf{d}_{11}^{\text{ant}} \cdot \hat{\mathbf{d}}^{\text{spoof}})/\lambda)} \\ e^{-j((2\pi \mathbf{d}_{21}^{\text{ant}} \cdot \hat{\mathbf{d}}^{\text{spoof}})/\lambda)} \\ \vdots \\ e^{-j((2\pi \mathbf{d}_{N1}^{\text{ant}} \cdot \hat{\mathbf{d}}^{\text{spoof}})/\lambda)} \end{bmatrix},$$
$$\mathbf{a}_m = \begin{bmatrix} 1 \\ (a_m)_2 \\ \vdots \\ (a_m)_N \end{bmatrix} = \begin{bmatrix} e^{-j((2\pi \mathbf{d}_{11}^{\text{ant}} \cdot \hat{\mathbf{d}}_m^{\text{sat}})/\lambda)} \\ e^{-j((2\pi \mathbf{d}_{21}^{\text{ant}} \cdot \hat{\mathbf{d}}_m^{\text{sat}})/\lambda)} \\ \vdots \\ e^{-j((2\pi \mathbf{d}_{N1}^{\text{ant}} \cdot \hat{\mathbf{d}}_m^{\text{sat}})/\lambda)} \end{bmatrix}, \tag{4}$$

where $\mathbf{d}_{i1}^{\text{ant}}$ represents a vector pointing from the origin (reference antenna phase centre) to the ith antenna phase centre. $\hat{\mathbf{d}}_m^{\text{sat}}$ and $\hat{\mathbf{d}}^{\text{spoof}}$ represent the pointing unit vectors from the origin to the mth authentic satellite and spoofing source respectively. λ represents the GPS carrier wavelength at L1 frequency.

5. Classification of Antispoofing Techniques

Several antispoofing techniques have been proposed in the open literature and can generally be classified into two main categories, namely *spoofing detection* and *spoofing mitigation*. Spoofing detection algorithms concentrate on discriminating the spoofing signals but they do not necessarily perform countermeasures against the spoofing attack, while spoofing mitigation techniques mainly concentrate on neutralizing the detected spoofing signals and help the victim receiver to retrieve its positioning and navigation abilities. In the following subsections a brief introduction is provided on different techniques proposed for each category.

5.1. Spoofing Detection

5.1.1. Methods Based on the Signal Power Monitoring

(a) C/N_0 Monitoring. Most GPS receivers employ C/N_0 measurements as a parameter that characterizes the received signal quality. In open sky conditions, only satellite movement and ionosphere variations can cause gradual smooth changes in the received signal power. However, when a higher power spoofer misleads a GPS receiver, the received C/N_0 may experience a sudden change that can indicate the presence of the spoofing signal. The antispoofing receiver can continuously monitor the C/N_0 and look for any unusual variation that can be a sign of spoofing attack. It is easy for a GPS receiver to store a time history of the signal received from each satellite.

Consider the correlator output for the lth authentic signal as the following equation:

$$y_l^a(kNT_s) = \underbrace{\sqrt{p_l^a} e^{j\varphi_l^a}}_{S\text{: Desired Signal}} + \underbrace{\sum_{\substack{m=1 \\ m \neq l}}^{N_{\text{Auth}}} \sqrt{p_m^a} C_{ml}^a(kNT_s)}_{I_{\text{Auth}}\text{: Interference caused by other authentic PRNs}} + \underbrace{\sum_{q=1}^{N_{\text{Spoof}}} \sqrt{p_q^s} C_{ql}^s(kNT_s)}_{I_{\text{Spoof}}\text{: Interference caused by spoofer generated PRNs}} + \underbrace{\overline{\eta}(kNT_s)}_{\text{Gaussian Noise}}, \tag{5}$$

where

$$C_{ml}^a(kNT_s) = \frac{1}{N} \sum_{n=(k-1)N+1}^{kN} F_m^a(nT_s) \hat{F}_l(nT_s),$$
$$C_{ql}^s(kNT_s) = \frac{1}{N} \sum_{n=(k-1)N+1}^{kN} F_q^s(nT_s)\, \hat{F}_l(nT_s), \tag{6}$$
$$\hat{F}_l(nT_s) = c_l(nT_s - \hat{\tau}_l)\, e^{-j2\pi \hat{f}_l nT_s},$$

where N determines the coherent integration interval and kNT_s is the time instant at which the correlator output is updated. $C^a_{ml}(kNT_s)$ is the cross-correlation between $F^a_m(nT_s)$ and the lth locally generated PRN signal replica, $\widehat{F}_l(nT_s)$, whose Doppler and code delay are $\hat{\tau}_l$ and $\widehat{f}_l$, respectively. Herein, the effect of data bits has been neglected to simplify the notations. In (5) the second and third additive terms (I_{Auth} and I_{Spoof}) are interference terms caused by cross-correlation effect of other authentic and spoofing signals. $\overline{\eta}[kNT_s]$ is the filtered noise component with variance σ^2/N. The C/N_0 measurement for each GPS signal is proportional to the ratio between the despread signal power at the correlator output to the noise power plus other signal interferences. The postprocessing signal-to-noise ratio (SNR), which is linked to the C/N_0 value, can be shown as

$$\text{SNR}^a_l = \frac{p^a_l}{|I_{\text{Auth}}|^2 + \left|I_{\text{Spoof}}\right|^2 + (\sigma^2/N)}. \tag{7}$$

GPS signals are designed such that $|I_{\text{Auth}}|^2$ is negligible compared to the filtered Gaussian noise variance. However, $|I_{\text{Spoof}}|^2$ increases as the total spoofing power (TSP) increases. TSP is the sum of signal powers for different spoofing PRNs (i.e., TSP $= \sum_{q=1}^{N_{\text{Spoof}}} \sqrt{p^s_q}$). Therefore, an asynchronous spoofing source that is transmitting several PRNs with considerable power can effectively reduce the C/N_0 of the authentic signals. However, if a spoofing signal is despread, its corresponding C/N_0 measurement would be in the normal authentic C/N_0 range. In this case, the spoofer has generated higher power correlation peaks over an elevated noise floor. This procedure can effectively mislead those spoofing detection techniques that are based on C/N_0 monitoring. As a consequence, the receiver might be tracking the higher power spoofing correlation peaks while its C/N_0 measurement does not show any abnormalities [12].

Figure 3 illustrates the authentic and spoofing SNR values versus the TSP for the case of 10 equal power authentic signals and 10, 20, and 30 equal power spoofing signals. The power of each authentic signal is -158 dBW and the coherent integration time is $T_c = NT_s = 1$ ms. A typical detection SNR threshold has been depicted in this figure. It is observed that the SNR of the authentic signals decreases as the TSP increases, while, on the contrary, the SNR of the spoofing signals increases up to a certain level as the TSP increases. The maximum spoofing SNR level depends on the number of transmitted spoofing PRN signals and the distribution of TSP among them. The receiver noise floor estimate at the 1 ms integration time is also depicted on the right-hand side of the y-axis of Figure 3. This curve is useful for analyzing the noise floor increase at a certain TSP level.

(b) Absolute Power Monitoring. As the path loss between the spoofer and target receiver is highly variable, it is difficult for a spoofer to estimate the transmit power required to impose sufficient signal strength at the target receiver while not excessively exceeding the typical power level of the authentic GPS signals [8]. The maximum received power of the GPS signals at earth terminals is around -153 dBW at the L1 frequency [13]. Therefore, reception of a spoofing signal whose absolute power is considerably higher than the expected authentic GPS signal power is a simple direct means of detecting a spoofing attack.

Figure 4 provides a comparison between the spoofing vulnerability regions for a C/N_0 monitoring receiver and an absolute power monitoring receiver. It has been assumed that the absolute power monitoring receiver is able to discriminate the elevated noise floor as well as higher power PRN signals within a 2 dB accuracy range. In other words, this receiver discriminates those PRNs whose absolute power is 2 dB or higher than the maximum possible received power of GPS L1 C/A signal. Furthermore, this receiver is capable of detecting a 2 dB increase in noise floor from its desired value. On the other hand, the C/N_0 monitoring receiver is only able to discriminate the signals whose SNR is higher than the maximum possible SNR of the GPS L1 C/A signal (this value is assumed to be 21.8 dB for $T_c = 1$ ms and temperature = 300°K).

Hence, as it is shown in Figure 4, the vulnerability region of the absolute power monitoring receiver is much smaller than the vulnerability region of the C/N_0 monitoring receiver. Furthermore, if the receiver is able to detect the absolute receiver power more accurately, it can considerably reduce the size of its vulnerability window in the presence of a spoofing attack [12].

Implementation of this power monitoring technique requires the receiver ability to measure the absolute amplitude of the received signal within a certain accuracy level. Hence, the hardware complexity slightly increases. In addition, the relatively high dynamic range of the GPS signal strength imposes another limitation to the performance of the amplitude discrimination techniques.

(c) Received Power Variations versus Receiver Movement. Based on the free space square law of propagation, the received power of a free space propagating signal is proportional to the inverse of the squared propagation distance. GPS satellites are around 20,000 kilometres away from the earth surface; therefore, if the receiver moves on the earth surface in low multipath open sky environments, no considerable change in the received power from authentic satellites should be observed other than the deterministic losses occurring at lower elevations. However, as discussed before, the spoofing signal is usually transmitted from a single directional antenna located much closer to the receiver compared to the GPS satellites. Therefore, the movement of the receiver relative to the spoofer antenna can considerably change the C/N_0 received from spoofing signals. Figure 5 illustrates the variations of spoofing and authentic received C/N_0 values versus the receiver distance from a spoofer antenna. It is observed that when the spoofer is very close to its target receiver, even a slight movement between spoofer and the target receiver can considerably affect the received spoofing signal C/N_0. It should be considered that all the spoofing signals are usually transmitted from the same antenna and therefore all experience the same propagation medium. As such, variations of all spoofing signals will be

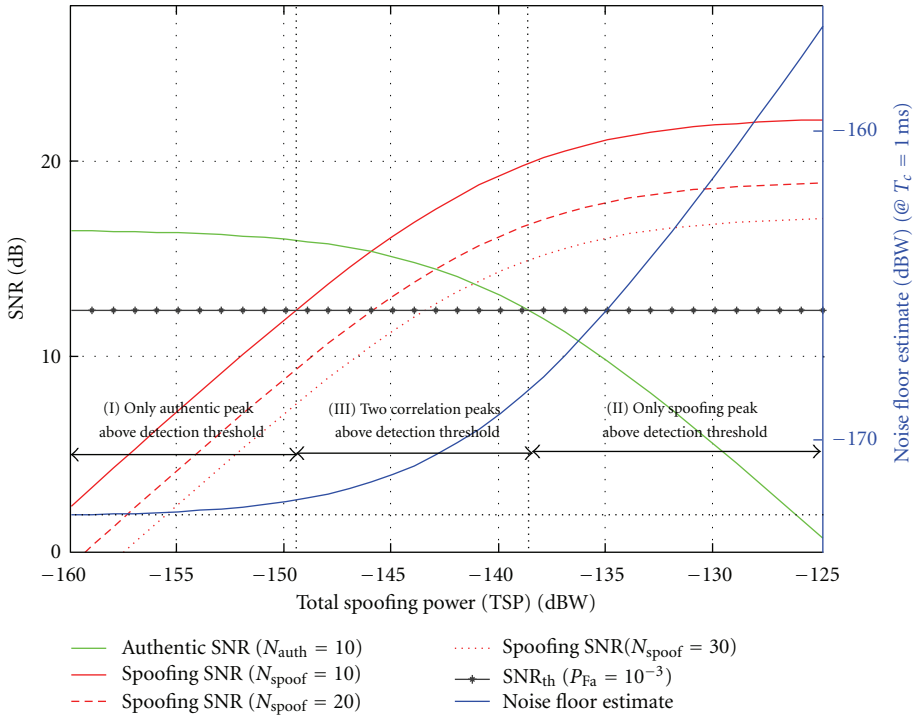

Figure 3: Received SNR versus TSP for authentic and spoofing correlation peaks [12].

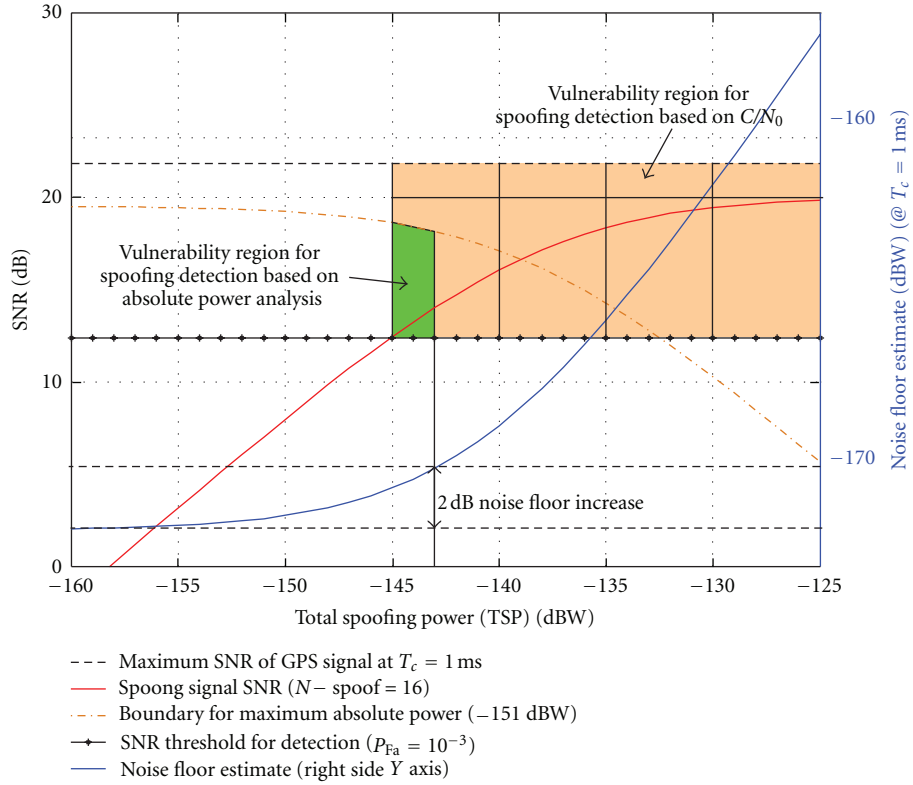

Figure 4: Vulnerability region comparison of C/N_0 versus absolute power monitoring techniques [12].

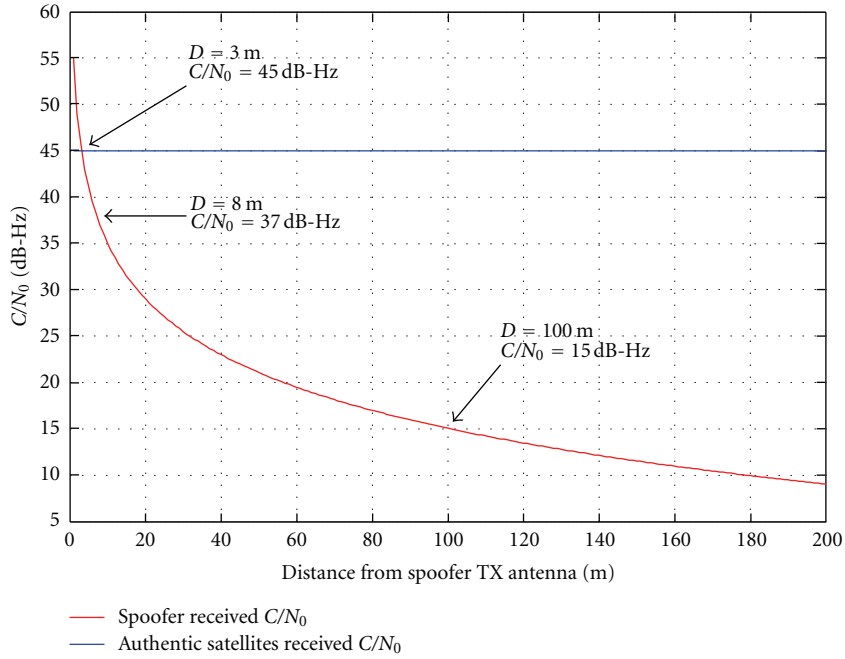

Figure 5: Variations of spoofing and authentic received C/N_0 versus receiver distance from spoofer transmitting antenna.

the same regardless of the receiver movement and multipath effects [11]. Here it is assumed that the spoofer does not differentially modulate the C/N_0 of the different PRN signals.

This method is a low-complexity spoofing discrimination technique that does not impose extensive hardware/software modifications to the GPS receiver. However, since the receiver does not necessarily know the position of the spoofer antenna and the distance variations with respect to the receiver antenna, there is no guarantee that the receiver movement considerably changes the received C/N_0 of the spoofer generated signals. For example, when both spoofing transmitter and GPS receiver are located in the same vehicle, the movement of vehicle does not cause variation in measure of spoofing signals C/N_0. Another disadvantage of this technique is that it cannot be employed for the case of static GPS receivers. Therefore, the effectiveness of this spoofing discrimination technique is limited to a few spoofing scenarios.

(d) L1/L2 Power Level Comparison. There is a predefined power level difference between GPS signals in different frequency bands [8] and many GPS receivers are able to monitor both L1 and L2 signals. However, a low-complexity spoofer may only generate L1 signal. Therefore, a large difference between L1 and L2 power levels or the absence of L2 signals can reveal the presence of a spoofing signal.

This method can successfully detect the single-band spoofers. However, most of the civil GPS receivers do not have the ability to monitor both L1 and L2 frequency bands and this discrimination technique imposes additional hardware complexity to the GPS receiver.

5.1.2. Spoofing Discrimination Using Spatial Processing. Due to logistical limitations, spoofing transmitters usually transmit several counterfeit signals from the same antenna while the authentic signals are transmitted from different satellites with different directions. Therefore, a spatial processing technique can be employed to estimate the spatial signature of received signals and discriminate those signals that are spatially correlated.

(a) Multiantenna Spoofing Discrimination. In [2] a spoofing detection technique is proposed which observes the phase difference between two fixed antennas for around one hour. Knowing the bearing of the antenna array and the satellites movement trajectory, the theoretical phase differences can be calculated and compared to the practical phase difference observed by the antenna array to discriminate the spoofing threat. The main drawback of the algorithm is that it takes a long time (about 1 hour) to discriminate the spoofing signals. In addition, this technique requires a calibrated antenna array with known array orientation in order to operate properly.

In [14] an antenna array structure is used to detect and mitigate spoofing signals based on their spatial correlation. The correlator output phase measurements for different PRN signals are mutually compared to discriminate the ones received from the same spatial sector. This technique can successfully detect spoofing signals and it does not need any array calibration or information regarding array orientation. This technique can effectively discriminate the spoofing scenarios that employ a single transmit antenna. In addition, the multipath propagation does not degrade the performance of this method since all the spoofing signals experience the same propagation channel characteristics.

However, this technique increases the hardware complexity of the GPS receiver as it necessitates the use of several antenna branches. Furthermore, applying this method increases the computational complexity of GPS receiver since the receiver needs to acquire and track both spoofing and authentic signals in order to be able to discriminate spoofing PRNs.

A multipleantenna spoofer might be able to defeat the multiple-antenna spoofing discrimination techniques depending on the number of transmit antennas, the number of receiver antennas, and the geometry of spoofer antennas with respect to the target receiver antennas. However, there are many practical limitations to realizing such a sophisticated spoofing scenario.

(b) Synthetic Array Spoofing Discrimination. In [6] a spoofing detection technique that employs a synthetic antenna array has been proposed. In this scenario a single-antenna handheld GPS receiver is moved along a random trajectory and forms a synthetic antenna array structure. This scenario is shown in Figure 6. The received signals amplitude and phase corresponding to different PRN signals are continually compared to each other using a correlation coefficient metric (ρ_{ij}). Therefore, after acquiring different PRN signals in the received signal set (both authentic and spoofing signals), spoofing signals are discriminated using the following normalized correlation coefficient:

$$\rho_{ij} = \left| \frac{E\left[(\mathbf{y})_i^H (\mathbf{y})_j\right]}{\sqrt{E\left[(\mathbf{y})_i^H (\mathbf{y})_j\right]}\ \sqrt{E\left[(\mathbf{y})_j^H (\mathbf{y})_j\right]}} \right|, \tag{8}$$

where $E[]$ represents the statistical expectation and the superscript H denotes the conjugate transpose. $(\mathbf{y})_i$ and $(\mathbf{y})_j$ represent the ith and jth columns of matrix $\mathbf{y}$, which is defined as follows:

$$\mathbf{y} = \begin{bmatrix} [\mathbf{y}^a[1], \mathbf{y}^s[1]] \\ [\mathbf{y}^a[2], \mathbf{y}^s[2]] \\ \vdots \\ [\mathbf{y}^a[M], \mathbf{y}^s[M]] \end{bmatrix}_{M \times L}, \tag{9}$$

$$\mathbf{y}^a[k] = \left[y_1^a(kNT_s), \ldots, y_{N_{\text{Auth}}}^a(kNT_s) \right],$$

$$\mathbf{y}^s[k] = \left[y_1^s(kNT_s), \ldots, y_{N_{\text{Spoof}}}^s(kNT_s) \right].$$

In (9), it is assumed that correlator outputs are monitored during M time instances and $\mathbf{y}$ is an $M \times L$ matrix where L is the number of acquired PRN signals ($L \leq N_{\text{Auth}} + N_{\text{Spoof}}$). $\mathbf{y}^a[k]$ is the set of correlator outputs for all acquired authentic signals at time instant kNT_s, whereas $\mathbf{y}^s[k]$ consists of all acquired spoofing peaks for that time instant. M is the number of equivalent spatial samples.

Figure 7 illustrates the normalized signal amplitude for acquired spoofing and authentic signals. During the data collection, the antenna was randomly moved. It is observed that the amplitude variations for spoofing signals are highly correlated (i.e., the plots representing the amplitudes of PRN-16, PRN-18, PRN-21, and PRN-29 are totally overlaid) while this correlation does not exist for the authentic signals (i.e., the amplitudes of PRN-22 and PRN-24 do not overlay). This technique works effectively even in multipath environments because all the spoofing signals experience the same fading path. Furthermore, since this method does not employ several receive antennas, its hardware complexity is much lower as compared to the techniques proposed in [2, 14]. However, in the case that spoofer differentially modulates the amplitude and/or phase of different PRN signals, some modifications should be applied to this method in order to successfully discriminate the counterfeit signals.

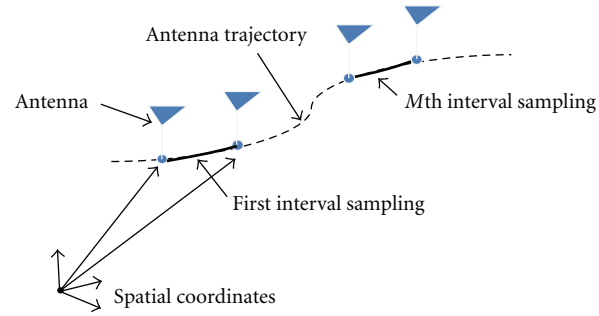

Figure 6: Spatial Sampling for a Moving Handheld GPS Receiver (modified after [6]).

5.1.3. Time of Arrival (TOA) Discrimination

(a) PRN Code and Data Bit Latency. In the case that the receiver-based spoofer does not have any prior information regarding the navigation data bits, it should first decode the received GPS signals and then generate a processed replica as the spoofing signal. Hence, an unavoidable delay exists between the spoofing data bit boundaries with respect to the authentic ones [3, 15, 16]. Therefore, if the data bit transition happens at time instants with a spacing other than 20 ms, then a spoofing attack might be present.

This technique encounters some limitations because the GPS data frame structure is already known and it consists of different parts with different update frequencies. The update frequency of most parts of the GPS frame is very low. Therefore, the majority of the GPS data bits can be predicted by the spoofer if it has already acquired the GPS information before starting to transmit the fake spoofing signals.

(b) L1/L2 Signals Relative Delay. GPS satellites transmit encrypted P(Y) codes on both L1 and L2 frequencies. The signals received on these two frequencies have a relative delay/attenuation that is caused by the different frequency response of the ionosphere. Therefore, if a dual frequency GPS receiver correlates the L1 and L2 signals, it should observe only one correlation peak [8]. The propagation delay in L2 is larger than the L1 frequency; therefore the approximate relative delay of correlation peaks is already known to the GPS receiver. The spoofer should be able to generate signals on both frequencies in order to defeat this countermeasure.

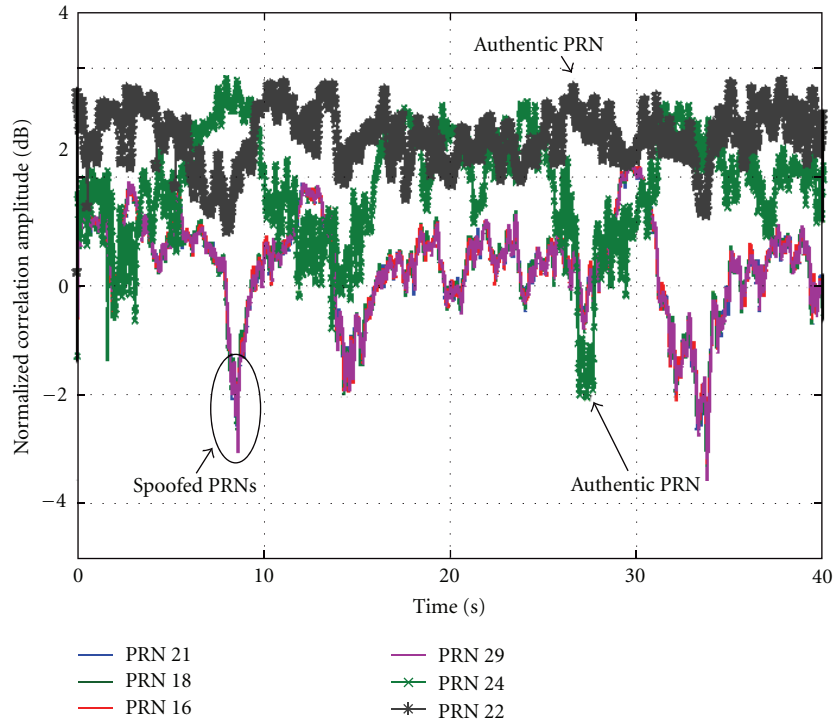

Figure 7: Correlation amplitude for spoofing and authentic PRN signals.

5.1.4. Signal Quality Monitoring (SQM). SQM techniques have been previously employed to monitor the GPS correlation peak quality in multipath fading environments [17]. Spoofing attacks on a tracking receiver can affect the correlator output in a way similar to that of multipath components [18]. Therefore, authors of [4, 5, 7] have extended the SQM techniques to detect the spoofing attack on tracking receivers that are working in line-of-sight condition. They have employed the *ratio* and *delta* SQM tests in order to detect any abnormal asymmetry and/or flatness of GPS correlation peaks that is imposed by the spoofing attack. It is assumed that the receiver has initially locked onto the authentic correlation peaks and a spoofing attack tries to deceive the receiver toward tracking its fake correlation peaks.

The SQM antispoofing techniques are powerful methods toward detecting the spoofing attack especially in the line-of-sight propagation environments. However, in the presence of multipath propagation, the SQM method might not be able to discriminate between spoofing signals and multipath reflections.

5.1.5. Distribution Analysis of the Correlator Output. In line-of-sight (LOS) conditions, the correlator output power for a tracking receiver approximately follows a Chi-squared (χ^2) distribution. For the case of a spoofing attack on a tracking receiver, the spoofing signal correlation peak should be located as close as possible to that of the authentic signal; therefore, the correlator output power is affected by the spoofing signals. As such, assuming that the receiver is initially locked into tracking the authentic peak, the correlator output amplitude can be written as follows [19]:

$$y_l\left[\Delta f_l^{a,s}, \Delta\tau_l^{a,s}, kNT_s\right] = \sqrt{p_l^a}\, e^{j\varphi_l^a} + \sqrt{p_l^s} R\left(\Delta\tau_l^{a,s}\right) \frac{\sin\left(\pi\Delta f_l^{a,s} NT_s\right)}{N\sin\left(\pi\Delta f_l^{a,s} T_s\right)} \times e^{j\pi\Delta f_l^{a,s}(N-1)T_s + j\varphi_l^s} + \tilde{\eta}_l[kNT_s], \tag{10}$$

where $\Delta\tau_l^{a,s}$ and $\Delta f_l^{a,s}$ are delay and frequency differences between the authentic and spoofing signals, respectively, and these parameters are generally functions of time. $R(\cdot)$ is the correlation function that is closely related to the choice of GPS signal subcarrier. This function is a triangle with a normalized height and two-chip base width for the GPS subcarrier. It is assumed that the spoofer smoothly changes the code delay and the Doppler frequency of its signal in order to lift off the tracking point of the target receiver. Therefore, the interaction between the authentic and spoofing signals leads to some fluctuations in the correlator output amplitude. These fluctuations cause the correlator output distribution to deviate from the expected χ^2 distribution. This feature can be used for detecting the presence of spoofing signals [19]. Figure 8 shows the correlator output distributions for different relative powers for authentic and spoofing signals. It is observed that the correlator output distributions are completely different in the presence and absence of spoofing attacks.

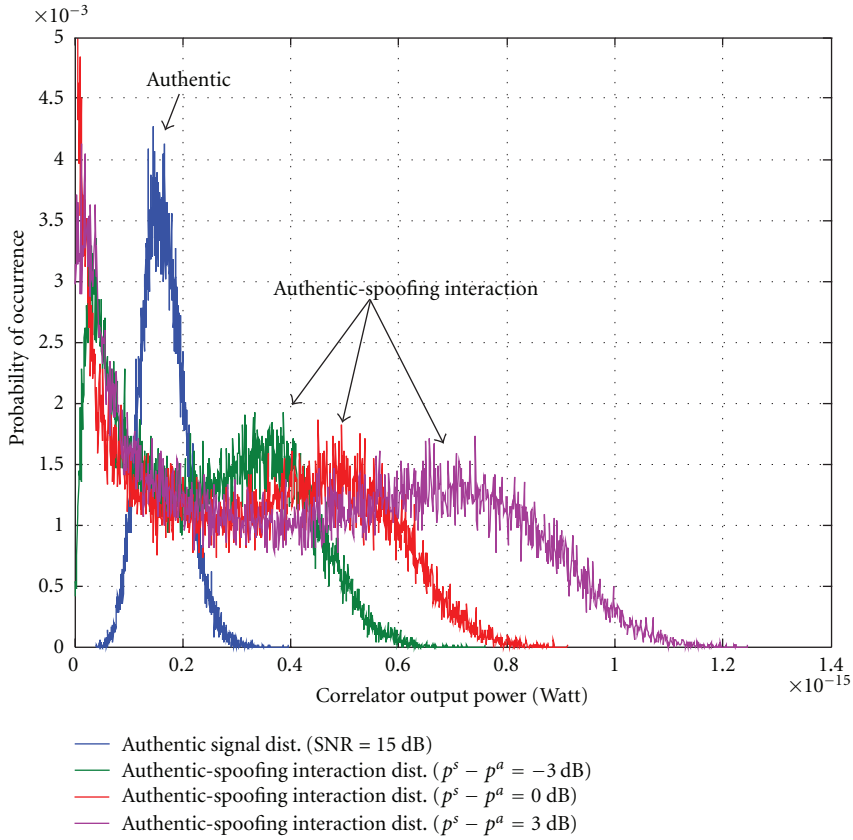

Figure 8: Distribution of prompt correlator output power for authentic signals and authentic-spoofing interaction for different spoofing powers [19].

This technique can successfully discriminate spoofing signals in the line-of-sight propagation environments. However, in presence of multipath propagation, the χ^2 distribution is not a valid assumption for the distribution of correlator output amplitude. Therefore, this method is of limited applicability in non-line of sight propagation environments.

5.1.6. Consistency Check with Other Navigation and Positioning Technologies. The augmenting data from auxiliary devices such as inertial measurement unit (IMU) can help the target receiver to discriminate the spoofing threat [2, 20]. In addition, the GPS receiver can compare the solution extracted by received GPS signals to the other position and navigation solutions obtained by mobile networks or WiFi stations. Therefore, if the confidence region of different solutions does not have intersection, there is a high likelihood of a spoofing condition.

Employing this spoofing detection technique increases the hardware and software complexity of GPS receiver. The IMU sensors require calibration before being employed for the positioning purposes [21]. In addition, alternative wireless location technologies such as cellular networks do not usually provide position solutions as accurate as GPS signals; therefore, they might not be very helpful if there is a small mismatch between spoofing solution and authentic position. Furthermore, there is a limited coverage of cellular and WiFi networks which, in turn, limits the applicability of this spoofing discrimination technique.

5.1.7. Cryptographic Authentication. Authentication techniques can be employed to detect spoofing threat in both civil and military applications. This capability is considered in military version of GPS signals; however, some articles have discussed authentication techniques for current civil GPS receivers [10, 15, 22, 23]. Reference [22] has proposed authentication techniques for GPS L2C and L5 and wide area augmentation system (WAAS) signals.

Most of the cryptographic authentication techniques require some modifications in the GPS signal structure. Therefore, this method does not seem to be applicable to GPS in short term.

5.1.8. Code and Phase Rates Consistency Check. In the case of authentic signals, the Doppler frequency and the code delay rate are consistent because they are both affected by the relative movement between GPS satellite and receiver [24]. This consistency requires that

$$f_l^a = -f_{\mathrm{RF}}\dot{\tau}_l^a, \tag{11}$$

where f_{RF} is the RF frequency of L1 GPS signals ($f_{\mathrm{RF}} = 1575.42$ MHz) and $\dot{\tau}_l^a$ is the code delay rate for the lth

Table 1: Summary of spoofing detection techniques.

Anti-Spoofing method	Spoofing feature	Complexity	Effectiveness	Receiver required capability	Spoofing scenario generality
C/N_0 monitoring	Higher C/N_0	Low	Medium	C/N_0 monitoring	Medium
Absolute power monitoring	Higher amplitude	Low	Medium	Absolute power monitoring	High
Power variation versus receiver movement	Higher power variations due to proximity	Low	Low	Antenna movement/C/N_0 monitoring	Low
L1/L2 power comparison	No L2 signal for spoofer	Medium	Low	L2 reception capability	Low
Direction of arrival comparison	Spoofing signals coming from the same direction	High	High	Multiple receiver antennas	High
Pairwise correlation in synthetic array	Spoofing signals coming from the same direction	Low	High	Measuring correlation coefficient	High
TOA discrimination	Inevitable delay of spoofing signal	Medium	Medium	TOA analysis	Low
Signal quality monitoring	Deviated shape of authentic correlation peak	Medium	Medium	Multiple correlators	Low
Distribution analysis of the correlator output	Perturbed amplitude distribution due to spoofing-authentic interaction	Low	Medium	Distribution analysis of correlator outputs	Medium
Consistency check with other solutions	Inconsistency of spoofing solution	High	High	Different navigation sensors	High
Cryptographic authentication	Not authenticated	High	High	Authentication	High
Code and phase rate consistency check	Mismatch between artificial code and phase rate	Low	Low	—	Low
GPS clock consistency check	Spoofing/authentic clock inconsistency	Low	Medium	—	Medium

authentic PRN signal. A low-quality spoofer might not keep this consistency between Doppler frequency and code delay rate [8]. As such, a spoofing aware receiver can successfully detect this type of spoofers if the loop filter output of phase locked loop (PLL) and delay locked loop (DLL) are not consistent. The PLL and DLL loop filter outputs are estimates of the phase and delay rates, respectively.

5.1.9. Received Ephemeris Consistency Check. The navigation message of each satellite contains some ephemeris information corresponding to the position of other GPS satellites. Any inconsistency among these ephemeris data can alert an unsynchronized spoofing attack.

5.1.10. GPS Clock Consistency Check. The navigation message of each PRN signal contains the GPS clock information. The GPS clock obtained from different satellites of GPS constellation should be consistent. However, the GPS time extracted from an unsynchronized spoofer might not be consistent with the GPS time extracted from other satellites and this can alert the presence of a spoofing attack.

Table 1 provides a summarized comparison among the previously discussed spoofing detection algorithms.

5.2. Spoofing Mitigation

5.2.1. Vestigial Signal Detection. Suppressing the authentic signal is very hard for GPS spoofers because it requires precise knowledge of the victim antenna phase centre position relative to spoofer antenna phase centre. In most cases, after successful lift-off, a vestige of the authentic signal that can be used for spoofing detection and mitigation remains. In [3] the authors have proposed a vestigial detection technique in which the receiver employs the following software-defined technique. First, the receiver copies the incoming digitized front-end data into a buffer memory. Second, the receiver selects one of the GPS signals being tracked and removes the locally regenerated version of this signal from the buffered signal. Third, the receiver performs acquisition for the same PRN signal on the buffered data. This technique is very similar to the successive interference cancellation (SIC) used for removing strong signals in order to combat the near/far

problem in direct sequence code division multiple-access (DS-CDMA) networks [24].

The implementation of the vestigial signal detection increases the hardware and processing complexity of the receivers because this technique requires additional tracking channels to track both authentic and spoofing signals. In addition, in the presence of high power spoofing signals and limited bit resolution, the authentic vestige might not still be detectable since it might have been fallen under the sensitivity level of the GPS receiver quantizer.

5.2.2. Multiantenna Beam Forming and Null Steering. A multiantenna receiver can employ array processing techniques in order to shape its beam. As such, after detecting the direction of spoofing signal, this receiver can steer a null toward the spoofer source and suppress its harmful effect. Therefore, considering (3), spoofing signals can be mitigated if the received signal is multiplied by a complex $(N \times 1)$ weighting vector $(\mathbf{f})$ such that

$$\mathbf{f}^H\mathbf{b} = 0, \quad \text{constraint}: \|\mathbf{f}\| = 1. \tag{12}$$

The constraint avoids the trivial solution, which is $\mathbf{f} = \mathbf{0}$. Therefore, applying this gain vector to the sampled signal of (3), the following output signal will be achieved:

$$\begin{aligned} s(nT_s) = \mathbf{f}^H\mathbf{r}(nT_s) = &\sum_{m=1}^{N_{\text{Auth}}} \mathbf{f}^H\mathbf{a}_m\sqrt{p_m^a}F_m^a(nT_s) \\ &+ \underbrace{\mathbf{f}^H\mathbf{b}}_{=0}\sum_{q=1}^{N_{\text{Spoof}}}\sqrt{p_q^s}F_q^s(nT_s) + \mathbf{f}^H\boldsymbol{\eta}(nT_s). \end{aligned} \tag{13}$$

Consequently, the spoofing signal is removed after proper combination of signals for different antenna branches [14, 25].

In [14] a spoofing mitigation technique is proposed that employs a multiantenna GPS receiver toward mitigating the spoofing attack. McDowell's method can effectively discard the spoofing signals after determining the spatial correlation between different received signal pairs. However, this method considerably increases the receiver hardware and processing complexity since the proper gain vector can be achieved after processing the despread version of all received authentic and spoofing GPS signals.

In [25] a very low computational complexity double-antenna spoofing mitigation method is proposed that is able to spatially filter out the spoofing signals. This method cross-correlates the received signals from different antennas and extracts the spatial signature of spoofing signals based on their spatial power dominancy. All these operations are performed on the raw samples before despreading the authentic and spoofing signals. Assuming that spoofer module transmits several PRN signals each of which having a power level comparable to authentic ones, the steering vector corresponding to spoofing signals $(\mathbf{b})$ can be extracted because all spoofing signals are coming from the same direction. This method does not need array calibration or any prior information regarding antenna array orientation and can be employed as an in-line stand-alone antenna combining block that mitigates the spoofing signals at before entering the conventional GPS receivers.

Figure 9 shows the average SNR of the authentic and spoofing signals as a function of the average input spoofing power for both the single-antenna and the proposed double-antenna receivers. For the case of single-antenna receiver, the authentic SNR decreases as the input spoofing power increases. However, it is observed that after proper combining of the signals of both antennas, the SNR of the authentic signal almost remains constant while the spoofing SNR is always far below the detection threshold for different input spoofing powers.

The spoofing mitigation technique proposed in [25] successfully mitigates the spoofing signals as long as their TSP is considerably higher than the average power of authentic signals. Nevertheless, in some cases it might unintentionally reduce the power of some authentic signals due to the inherent cone of ambiguity in the double-antenna beam pattern. This problem can be solved by employing larger antenna arrays because the ambiguity region of antenna beam pattern considerably decreases as the number of array elements increases [26]. This spoofing mitigation technique might not perform well in the case of multiple-antenna spoofing transmission.

5.2.3. Receiver Autonomous Integrity Monitoring (RAIM). Spoofing signals effectively inject counterfeit pseudoranges into the receiver measurements. These measurements might not be consistent and consequently do not lead to a reasonable position solution. Most of the GPS receivers perform measurements integrity monitoring in order to detect and reject the outlier measurements; this technique is known as receiver autonomous integrity monitoring [27]. In [7] the authors propose an extended RAIM technique that is able to detect and exclude the outlier measurements injected by the spoofing threat. In [11] a vulnerability index against spoofing (VIAS) is proposed that investigates the vulnerability of a GPS receiver that is protected by RAIM technique in the presence of misleading spoofing measurements. The author has shown that the maximum position deviation is the product of the RAIM level with the VIAS index.

RAIM techniques can be employed as useful antispoofing techniques at the position solution level. However, these methods are effective only in cases where only one or two spoofing measurements are present among several authentic pseudoranges; otherwise, if the spoofed pseudorange measurements are in majority, the RAIM technique might reject authentic measurements in order to decrease the residuals.

Table 2 provides a summarized comparison among the previously discussed spoofing mitigation algorithms.

5.3. Antispoofing Techniques from a Multilayer Perspective. From a multilayer perspective, the antispoofing techniques can be investigated in three different levels, namely, the signal processing, data bit and position solution, and navigation levels. Spoofing threat might be detected/mitigated at any

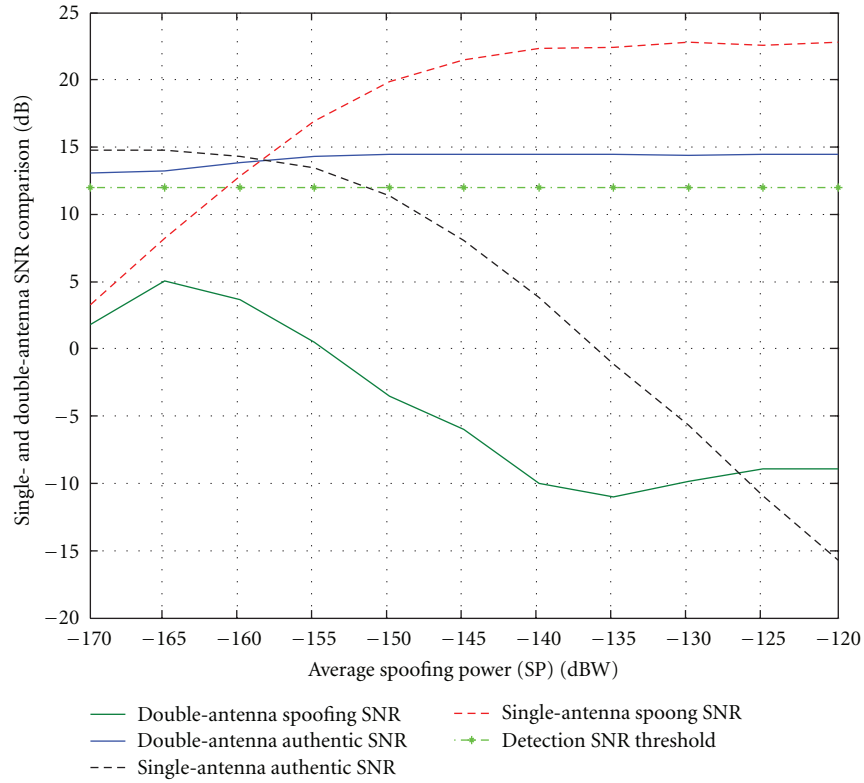

Figure 9: Authentic and spoofed SNR variations as a function of average spoofing power [25].

Table 2: Summary of spoofing mitigation techniques.

Anti-spoofing method	Spoofing feature	Complexity	Effectiveness	Receiver required capability	Spoofing scenario generality
Vestigial signal detection	The authentic signal is still present and can be detected	High	Medium	Multiple receive channels	Medium
Multi-antenna null steering	Spoofing signals coming from the Same direction	Medium	High	Multiple receiver antennas	High
RAIM	Higher residuals for spoofed measurements	Medium	Medium	—	Medium

of the above-mentioned levels. In other words, a successful spoofer should be able to overcome the antispoofing techniques implemented in different layers. In addition to the previously discussed antispoofing methods, cross-layer techniques can be developed to incorporate measurements from different operational levels in order to combat the harmful effect of spoofing signals. Figure 10 shows some of the previously discussed antispoofing techniques in a multilayer approach.

6. Spoofing/Antispoofing Test Scenarios

Testing a spoofer/antispoofer system is challenging since radio transmission regulations prohibit outdoors radio frequency (RF) power transmission in the GPS band. Therefore, special considerations should be taken into account in order to test a spoofing/antispoofing system in the presence of authentic satellites signals. This section presents some test scenarios that can be used for evaluating the performance of the antispoofing methods in real-world spoofing scenarios.

6.1. GPS Indoor Signal Retransmission. In [2] a rooftop GPS antenna has been used to receive authentic GPS signals. The received signals are amplified and then retransmitted indoors from a point source antenna. In this case, the spoofing transmission can take place indoors where it does not violate radio transmission regulations. This setup seems to be appropriate although it does not exactly represent real outdoor spoofing scenarios, especially for the case of multiantenna antispoofing techniques. In this case all authentic signals are also retransmitted from the single antenna (see Figure 11). Multipath propagation and relative spoofing and authentic signal powers are other issues that should be considered while employing indoor retransmission.

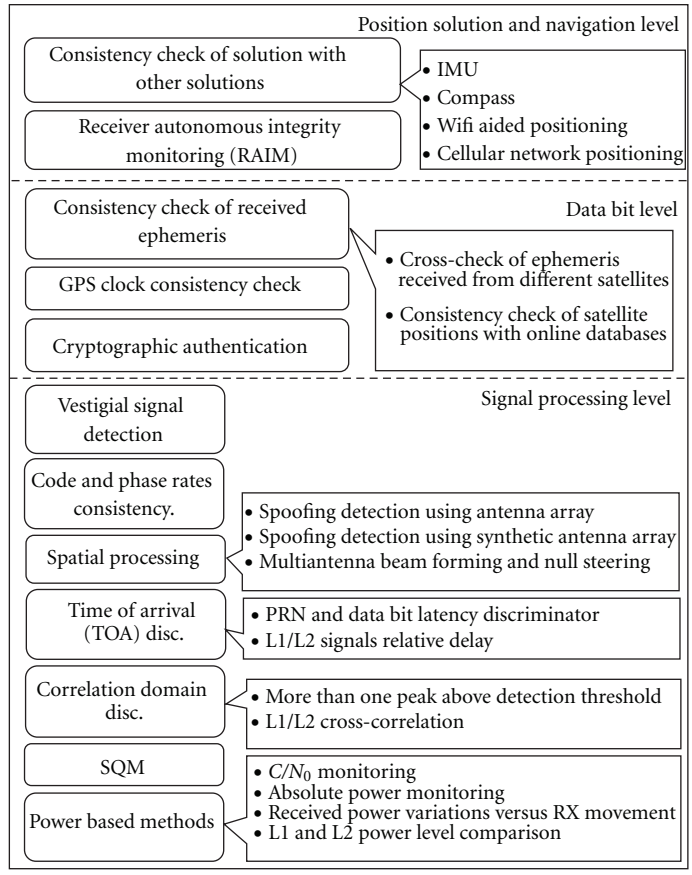

Figure 10: A multilayer approach to antispoofing techniques.

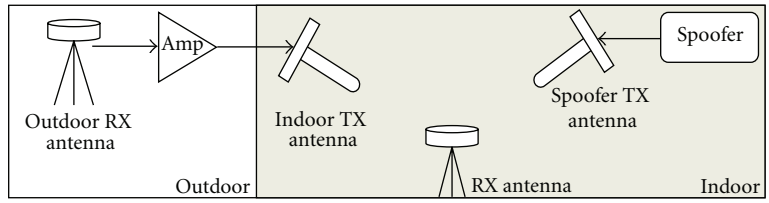

Figure 11: Spoofing test using GPS indoor signal retransmission.

6.2. Spoofing Using Recorded Data with No RF Transmission. In this scenario, no real spoofer RF transmission takes place; instead, the intermediate frequency (IF) authentic GPS L1 signal is digitized and stored on a hard disk; then, the recorded data is fed to the GPS receiver-spoofer, which tracks present GPS signals and generates corresponding spoofing signals. These signals are combined into a quantized output bit stream. The output bit stream is then combined with the original data by interleaving, and the result of this process is fed to the target receiver [3]. Figure 12 depicts a block diagram of this test scenario.

6.3. Employing RF Combiners to Combine Authentic and Spoofing Signals. Authentic GPS signals can be combined with locally generated spoofing signals using RF power combiners. Spoofing signal power can be adjusted using a cascaded setup of amplifier and variable attenuator. Figure 13 shows the block diagram of this test setup for validating the proper performance of a multiantenna antispoofing technique.

7. Conclusions

Spoofing attack on GPS receivers has been considered as a serious threat to safety of life applications; since there is enough motivation for illicit application of spoofers, the realization of spoofers is not prohibitively costly. As such, it is anticipated that many research activities will be conducted on increasing the security of GPS receivers against spoofing and jamming attacks. In this paper different spoofing/antispoofing scenarios were described and the vulnerabilities of GPS that can potentially be exploited

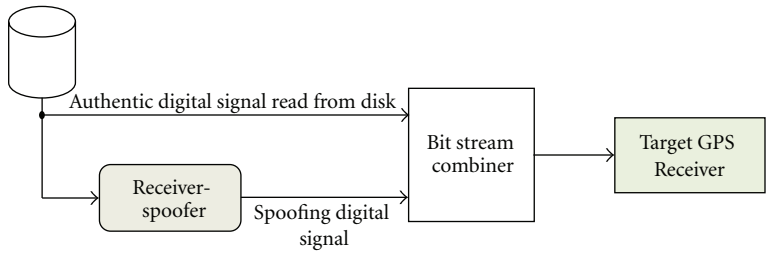

Figure 12: Spoofing test using recorded GPS data (modified after [3]).

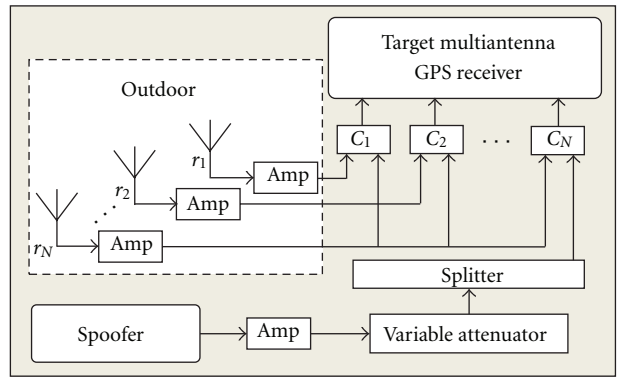

Figure 13: Spoofing test setup using RF combiners for a multiantenna GPS receiver.

by a spoofer were discussed in a multilayer GPS processing approach. It was shown that commercial GPS receivers are quite vulnerable to spoofing attacks generated by different spoofing scenarios. Nevertheless, by applying modest modifications, low-complexity spoofing detection and mitigation techniques can be employed in order to increase the robustness of commercial GPS receivers against spoofing attacks. Countermeasures to spoofing signals can be introduced in any (or all) of the processing levels of a GPS receiver. A powerful antispoofing technique should ideally be of low computational complexity and be effective for generic spoofing scenarios. Based on this paper, since most of the practical spoofing scenarios employ a single antenna to transmit counterfeit signals, the spatial characteristics of spoofing signals are different from those of authentic GPS signals. Therefore, spatial-processing-based antispoofing techniques can be employed as a generic and very effective countermeasure against most spoofing signals currently envisaged.

References

[1] X. J. Cheng, K. J. Cao, J. N. Xu, and B. Li, "Analysis on forgery patterns for GPS civil spoofing signals," in *Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09)*, pp. 353–356, Seoul, Korea, November 2009.

[2] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the Institute of Navigation—International Technical Meeting (ITM '09)*, pp. 124–130, Anaheim, Calif, USA, January 2009.

[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. 2314–2325, Savannah, Ga, USA, September 2008.

[4] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," in *Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC '10)*, pp. 1–6, December 2010.

[5] A. Cavaleri, M. Pini, L. Lo Presti, and M. Fantino, "Signal quality monitoring applied to spoofing detection," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS '11)*, Portland, Ore, USA, September 2011.

[6] J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing detection and mitigation with a moving handheld receiver," *GPS World*, vol. 21, no. 9, pp. 27–33, 2010.

[7] 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 Institute of Navigation—International Technical Meeting (ITM '10)*, pp. 698–712, San Diego, Calif, USA, January 2010.

[8] H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS '05)*, pp. 1285–1290, Long Beach, Calif, USA, September 2005.

[9] S. Savasta, L. Lo Presti, F. Dovis, and D. Margaria, "Trustworthiness GNSS signal validation by a time-frequency approach," in *Proceedings of the 22nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '09)*, pp. 66–75, Savannah, Ga, USA, September 2009.

[10] X. J. Cheng, J. N. Xu, K. J. Cao, and W. Jie, "An authenticity verification scheme based on hidden messages for current civilian GPS signals," in *Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09)*, pp. 345–352, Seoul, Korea, November 2009.

[11] J. C. Juang, "GNSS spoofing analysis by VIAS," in *Coordinates Magazine*, 2011.

[12] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181–191, 2012.

[13] E. D. Kaplan and C. J. Hegarty, *Understanding GPS Principles and Applications*, Artech House, Boston, Mass, USA, 2nd edition, 2006.

[14] C. E. McDowell, "GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling—US Patent 7250903 B1," 2007.

[15] S. C. Lo and P. K. Enge, "Authenticating aviation augmentation system broadcasts," in *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS '10)*, pp. 708–717, Indian Wells, Calif, USA, May 2010.

[16] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal Authentication, a secure civil GNSS for today," *GNSS magazine*, pp. 30–39, 2009.

[17] R. E. Phelts, *Multicorrelator techniques for robust mitigation of threats to GPS signal quality [Ph.D. thesis]*, Standford University, Palo Alto, Calif, USA, 2001.

[18] D. Shepard and T. Humphreys, "Characterization of receiver response to a spoofing attack," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS '11)*, p. 2608, Portland, Ore, USA, September 2011.

[19] N. A. White, P. S. Maybeck, and S. L. DeVilbiss, "Detection of interference/jamming and spoofing in a DCPS-aided inertial system," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 34, no. 4, pp. 1208–1217, 1998.

[20] A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attack on a vector based tracking GPS receiver," in *Proceedings of the International Technical Meeting of The Institute of Navigation*, Newport Beach, Calif, USA, January 2012.

[21] M. G. Petovello, *Real-time integration of a tactical-grade IMU and GPS for high-accuracy positioning and navigation [Ph.D. thesis]*, Department of Geomatics Engineering, University of Calgary, Alberta, Canada.

[22] L. Scott, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS '03)*, Portland, Ore, USA, September 2003.

[23] G. W. Hein, F. Kneissl, J. A. Avila-Rodriguez, and S. Wallner, "Authenticating GNSS: Proofs Against Spoofs Part 2," *GNSS magazine*, pp. 58–63, 2007.

[24] S. Moshavi, "Multi-user detection for DS-CDMA communications," *IEEE Communications Magazine*, vol. 34, no. 10, pp. 124–135, 1996.

[25] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low complexity gnss spoofing mitigation technique using a double antenna array," *GPS World Magazine*, vol. 22, no. 12, pp. 44–46, 2011.

[26] H. L. V. Trees, *Optimum Array Processing, Detection, Estimation, and Modulation Theory Part IV*, John Wiley & Sons, New York, NY, USA, 2002.

[27] H. Kuusniemi, A. Wieser, G. Lachapelle, and J. Takala, "User-level reliability monitoring in urban personal satellite-navigation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 43, no. 4, pp. 1305–1318, 2007.