sensors

MDPI

Article

Gaussian-Distributed Spread-Spectrum for Covert Communications

Ismail Shakeel *, Jack Hilliard, Weimin Zhang and Mark Rice

Information Sciences Division, Defence Science and Technology Group, Edinburgh, SA 5111, Australia
* Correspondence: ismail.shakeel@defence.gov.au

Abstract: Covert communication techniques play a crucial role in military and commercial applications to maintain the privacy and security of wireless transmissions from prying eyes. These techniques ensure that adversaries cannot detect or exploit the existence of such transmissions. Covert communications, also known as low probability of detection (LPD) communication, are instrumental in preventing attacks such as eavesdropping, jamming, or interference that could compromise the confidentiality, integrity, and availability of wireless communication. Direct-sequence spread-spectrum (DSSS) is a widely used covert communication scheme that expands the bandwidth to mitigate interference and hostile detection effects, reducing the signal power spectral density (PSD) to a low level. However, DSSS signals possess cyclostationary random properties that an adversary can exploit using cyclic spectral analysis to extract useful features from the transmitted signal. These features can then be used to detect and analyse the signal, making it more susceptible to electronic attacks such as jamming. To overcome this problem, a method to randomise the transmitted signal and reduce its cyclic features is proposed in this paper. This method produces a signal with a probability density function (PDF) similar to thermal noise, which masks the signal constellation to appear as thermal white noise to unintended receivers. This proposed scheme, called Gaussian distributed spread-spectrum (GDSS), is designed such that the receiver does not need to know any information about the thermal white noise used to mask the transmit signal to recover the message. The paper presents the details of the proposed scheme and investigates its performance in comparison to the standard DSSS system. This study used three detectors, namely, a high-order moments based detector, a modulation stripping detector, and a spectral correlation detector, to evaluate the detectability of the proposed scheme. The detectors were applied to noisy signals, and the results revealed that the moment-based detector failed to detect the GDSS signal with a spreading factor, $N = 256$ at all signal-to-noise ratios (SNRs), whereas it could detect the DSSS signals up to an SNR of −12 dB. The results obtained using the modulation stripping detector showed no significant phase distribution convergence for the GDSS signals, similar to the noise-only case, whereas the DSSS signals generated a phase distribution with a distinct shape, indicating the presence of a valid signal. Additionally, the spectral correlation detector applied to the GDSS signal at an SNR of −12 dB showed no identifiable peaks on the spectrum, providing further evidence of the effectiveness of the GDSS scheme and making it a favourable choice for covert communication applications. A semi-analytical calculation of the bit error rate is also presented for the uncoded system. The investigation results show that the GDSS scheme can generate a noise-like signal with reduced identifiable features, making it a superior solution for covert communication. However, achieving this comes at a cost of approximately 2 dB on the signal-to-noise ratio.

Keywords: covert communications; spread-spectrum schemes; communications signal processing; low probability of detection; secure communications; signal constellations

Citation: Shakeel, I.; Hilliard, J.; Zhang, W.; Rice, M. Gaussian-Distributed Spread-Spectrum for Covert Communications. *Sensors* **2023**, *23*, 4081. https://doi.org/10.3390/s23084081

Academic Editor: Pablo Angueira

Received: 3 March 2023
Revised: 30 March 2023
Accepted: 11 April 2023
Published: 18 April 2023

1. Introduction

Secure communication schemes are essential for transmitting mission-critical information securely and privately, especially in hostile environments. Traditional methods to achieve

secure communication can be broadly categorised into three main groups [1]: cryptographic methods, steganographic methods [2–4], and physical layer security techniques [5]. Cryptographic methods use encryption and decryption algorithms to prevent unauthorised access, disclosure, and alteration of data. Steganographic methods are primarily focused on concealing confidential information within non-sensitive objects, such as images, audio, and video files. On the other hand, physical layer security techniques aim to bolster the security of wireless communication systems by leveraging the unique properties of wireless channels. However, none of these methods can conceal the evidence of communication or protect against detection of the transmission. Therefore, an adversary can potentially intercept the transmission and take advantage of any vulnerabilities in the communication protocol to gain access to the secure data or launch electronic attacks against the user [6]. The operational needs of secure communication in contested electromagnetic environments go beyond just protecting the transmitted content; it also requires the concealment of the transmission behaviour [7]. This paper presents a new signalling scheme for covert communication. Covert communication, also known as communication with a low probability of detection (LPD), is centered around hiding any evidence of communication to avoid detection. This is achieved by reducing the received signal-to-noise ratio (SNR) at the eavesdropper [8–10].

Research published in the field of LPD communications can be categorised into two main areas: (i) information-theoretic aspects of LPD communications and (ii) designing waveforms for LPD communications. Information-theoretic studies focus on determining the fundamental limits of LPD communication in terms of the amount of information that can be conveyed from a transmitter to a receiver subject to a constraint on adversary's detection error probability [11,12]. The authors in [13] present a square root law (SRL) that defines the constraints and performance limits of LPD communication for the additive white Gaussian noise (AWGN) channel. The SRL law states that covert and reliable communication can be achieved provided no more than $\mathcal{O}\sqrt{n}$ bits are transmitted in n channel uses. This gives an information rate of $\mathcal{O}(1/\sqrt{n})$, which approaches 0 as n goes to infinity. Hence, recent studies have focused on developing LPD schemes to obtain a positive information rate [14].

This paper focuses on designing waveforms for LPD communication. For LPD communications, it is desirable to transmit with minimal PSD to hide the transmitted signal under the receiver's noise floor [7] and have random like characteristics such as non-repetitive features [15], making the signal indistinguishable from thermal white noise present at any receiver [16–18]. These properties are needed, as without them the waveform has the potential to be detected using advanced signal processing techniques such as cyclostationary analysis, higher-order moments analysis, energy detection methods, and time-frequency transforms [19–23].

Existing covert communication schemes use spread-spectrum, chaotic theory, or a combination of both to achieve covert communication. The proposed schemes vary: utilising machine learning [18], using noise envelopes to mask the signal [24], chaotic spreading and modulation [25,26], and using the message itself to spread the signal [27]. In addition to different waveform design approaches, there are also other methods proposed in the literature that exploit the uncertainties in the eavesdropping channel [28], noise power [29], transmit time [30], and interference power from friendly jammers [31] to reduce signal detectability and improve information rate [32]. Other non-conventional LPD techniques include methods based on (1) exploiting the multiplicity of users scattered across the wireless network and the channel variations caused by their mobility [33], (2) directional transmission using multiple antennas [34], (3) opportunistic power control similar to conventional power control with an on–off switch that turns off the transmitter when the channel gain falls below a threshold [35], (4) artificial noise generation to disguise the existence of covert channels [36], and (5) millimeter-wave communications that use feature steerable narrow beams operating in the frequency band of 30–300 GHz [37].

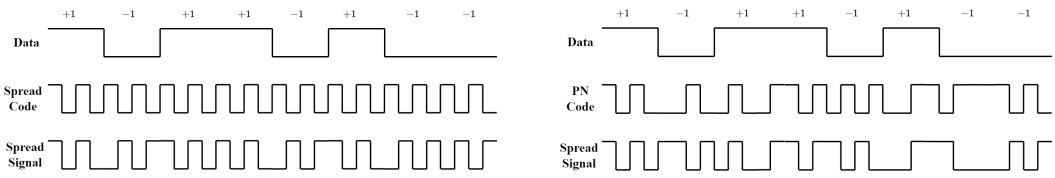
The proposed scheme in this paper uses thermal white noise of the system to obscure signals generated by a DSSS transmitter and produce a spread-spectrum waveform that

follows a Gaussian distribution (GDSS). The design of the GDSS scheme ensures that the receiver does not need any information about the sequences used to mask the signal to retrieve the message. To the best of our knowledge, this study represents the first investigation into utilising naturally occurring thermal noise for spread-spectrum communication. We conducted a performance evaluation of the proposed GDSS scheme and compared it to the widely used DSSS technique, which has several weaknesses that make it vulnerable to exploitation by adversaries. These vulnerabilities arise from the use of fixed modulation and repeatable spreading sequences.

The paper is structured as follows. Section 2 describes the standard DSSS system, and Section 3 presents the proposed GDSS waveform scheme. In Section 4, we evaluate the LPD performance of the proposed scheme using higher-order moments, a modulation stripping signal detector, and cyclostationary analysis. Section 5 investigates the error-rate performance of both coded and uncoded systems and compares it with DSSS. Furthermore, a numerical expression for the bit error rate performance of the GDSS system is derived and presented in this section. Finally, we conclude the paper in Section 6 and provide limitations of this research and suggestions for future work.

2. DSSS Modulation

DSSS, or direct-sequence spread-spectrum, is a method of modulation in which the message bits are modulated by a pseudorandom bit sequence known as a spreading sequence. This sequence has a much higher rate than the original information rate, and a spreading factor N determines the number of spreading bits that map to a message bit. After spreading, the symbols to be transmitted are commonly referred to as chips. When a DSSS system maintains the same bit rate and energy per bit as before spreading, the signal bandwidth will be spread by a factor of N, and the magnitude of the PSD of the signal will be reduced by a factor of N. This reduction in PSD helps to mitigate interference from other signals. To spread the signal, the data are multiplied by a pseudo-noise (PN) sequence. This PN spreading sequence is unique to each transmitter and receiver pair and helps to ensure secure communication. A binary phase shift keying (BPSK) DSSS spreading process is illustrated in Figure 1.



(**a**) With a short repeating PN sequence. (**b**) With a long PN sequence.

Figure 1. Spreading process of BPSK DSSS with repeating short PN sequence and with a long PN sequence.

DSSS is an important technology for covert communications because it enables the system to operate under the thermal noise floor even at low SNR levels (i.e., much lower than 0 dB SNR). This means that the communication signal can be hidden in the noise, making it difficult for adversaries to detect and intercept the signal. The spreading process in DSSS spreads the signal across a wide bandwidth, which reduces the PSD of the signal. As a result, the signal is less susceptible to noise and interference, making it easier to detect at low SNR levels. This is particularly important for covert communications, where it is essential to maintain a low profile and avoid unfriendly detection.

The bit error rate (BER) performance of a DSSS system using quadrature phase shift keying (QPSK) spreading is given by

$$\text{BER} = 0.5\ \text{erfc}\left(\left(\sqrt{N(E_s/N_0)/2}\right)\right) \quad (1)$$

where erfc() is the complementary error function and E_s/N_0 is the energy per channel symbol to noise power spectral density ratio. This measure will also be referred to as signal-to-noise ratio (SNR) in this paper.

Examples for various spreading factors are shown in Figure 2. Figure 2 shows that the non-spread system achieves a target BER of 10^{-5} at 12.5 dB, whereas the DSSS system with a spreading factor of 256 achieves the same BER at −11.5 dB. It is further shown that as the spreading length increases, so does the system's ability to operate deeper in the noise floor. However, an increase of the spreading factor also causes a reduction in the bit rate if the system bandwidth is maintained fixed.

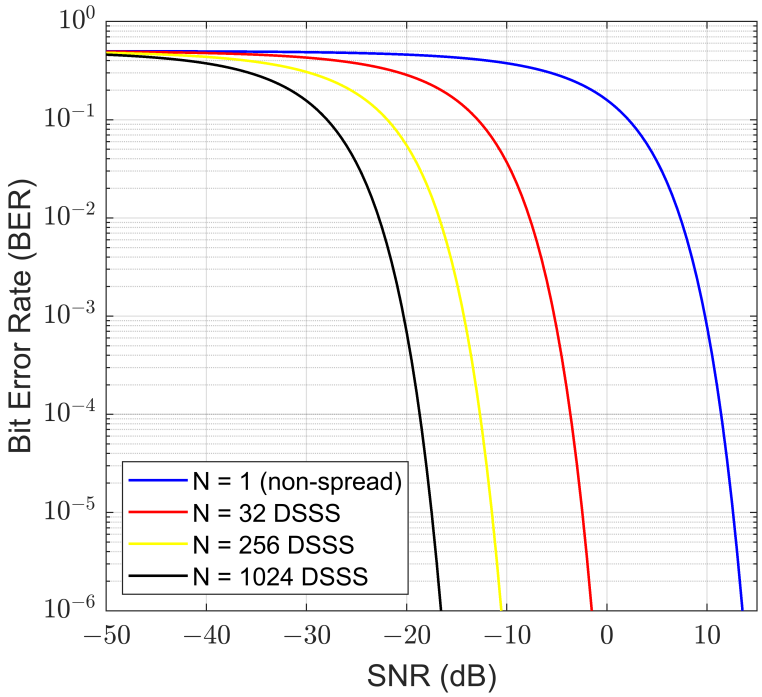


Figure 2. Theoretical BER performance of a DSSS-QPSK system with various spreading factors.

The standard DSSS system has several vulnerabilities and may not be ideal for covert communication. This system normally uses repeating patterns and has deterministic features that could be used for detection/interception. For example, Figure 3 shows the constellation of a typical DSSS-PN system with QPSK spreading. The points are color coded for future reference. As the amplitude and phase of the constellation points are fixed, they present deterministic features to the signal, making it easier for an adversary to detect the existence of the signal and possibly intercept the message using advanced signal processing methods [21]. The autocorrelation function (ACF) can be used to measure repeatable patterns of the PN sequences in a DSSS system. Some DSSS systems tackle the issue of predictable PN sequences by using a shared secret key in order to randomly generate the PN sequences [38]. However, implementation of such architectures for covert communication is difficult [39].

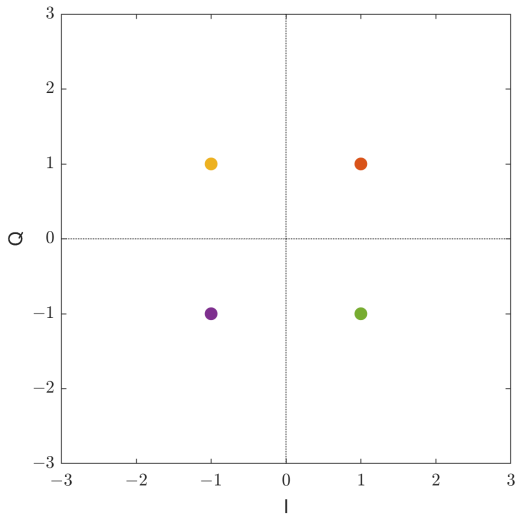


Figure 3. Signal constellation of the DSSS-PN QPSK noise-free transmit signal, colour coded for each position in a quadrant.

3. Proposed GDSS Scheme

The block diagram of the proposed GDSS scheme is illustrated in Figure 4.

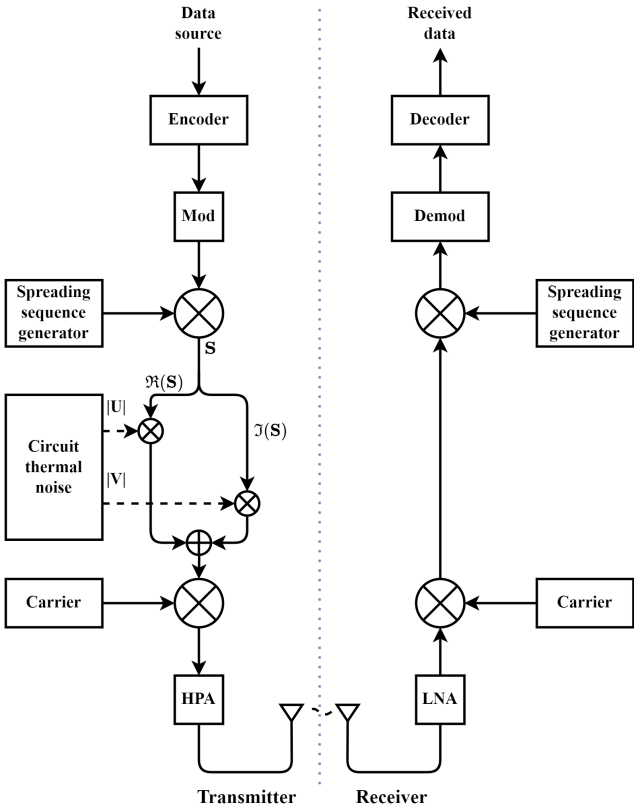


Figure 4. Proposed GDSS system.

The proposed scheme builds upon the standard QPSK DSSS-PN system by utilising the naturally occurring thermal white noise from the transmitter's circuity. The independently obtained noise sequences are applied to the in-phase (I) and quadrature-phase (Q) components of the signal after spreading to perform the Gaussian masking. The Gaussian masking process for the scheme illustrated in Figure 4 can be expressed as follows. For each QPSK spread complex chip **S**, a complex value **U**+j**V** is taken from a transmitter's

circuitry with amplified thermal white noise. Let $\mathbf{I}$ and $\mathbf{Q}$ be the result of element wise multiplication such that $\mathbf{I} = \Re(\mathbf{S}) * |\mathbf{U}|$ and $\mathbf{Q} = \Im(\mathbf{S}) * |\mathbf{V}|$, where $\Re(\mathbf{S})$ and $\Im(\mathbf{S})$ are the real and imaginary components of $\mathbf{S}$, respectively. The resulting product to be transmitted is then expressed as $\mathbf{I} + j\mathbf{Q}$. The generated IQ values are upsampled, filtered, modulated with a RF carrier wave, amplified with a high power amplifier (HPA), and transmitted through the antenna. On the receiver side, the received signal is first amplified with a low noise amplifier (LNA) and passed through the RF demodulation and despreading steps to recover the transmitted message.

A snapshot of the varying constellation points generated by masking the fixed QPSK points is shown in Figure 5, where each QPSK chip symbol (in a quadrant) is mapped to a non-deterministic location within the same quadrant every time. The Gaussian masking process moves the original symbol position in Figure 3 by the absolute values of the measured I and Q thermal noise values. It means the noise masking process does not move the symbol into a different quadrant, as illustrated in the colour matching scheme between the two figures. However, the cost of this method is an increase in the system BER, or for a same BER, an increase of the TX power. For a same average TX power, some symbols would be more susceptible to noise than they originally were due to being moved closer to the quadrant boundaries—a decreased Euclidean distance. The impacts to the BER will be quantified later. However, the adversaries detectablility is not necessarily scarified, depending on the detection method.

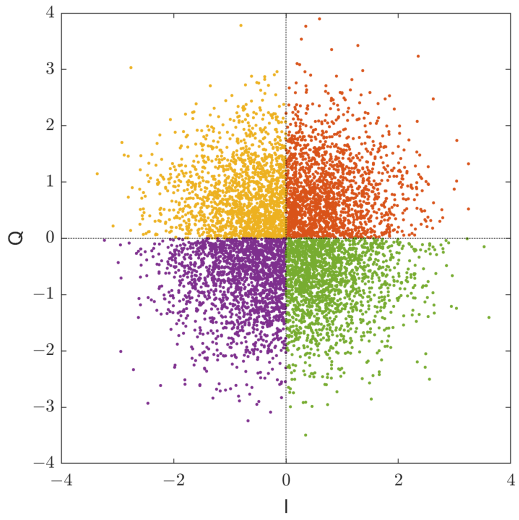


Figure 5. A collection of scattered constellation points of the proposed QPSK GDSS signal, with matching colours of QPSK DSSS in Figure 3.

Gaussianity of GDSS Signals

This section compares the distribution of the GDSS signals with the theoretical Gaussian distribution. The noise-free signal constellation of the GDSS scheme is shown in Figure 6. The figure shows that the signal constellation is sufficiently masked to appear as chaotic white noise to any adversary.

The probability density function of a random variable Z with Gaussian distribution is given by

$$f_Z(x) = \frac{1}{\sqrt{2\pi}} exp^{-x^2/2}. \tag{2}$$

Using Equation (2) its moments can be computed using

$$\mu_k = \int_{\infty}^{-\infty} x^k f_Z(x) dx. \tag{3}$$

A closed-form expression of Equation (3) for even orders of moments of the zero-mean unit-variance normal distribution can be expressed as [40]

$$\mu_k = \frac{k!}{2^{k/2}(k/2)!} \tag{4}$$

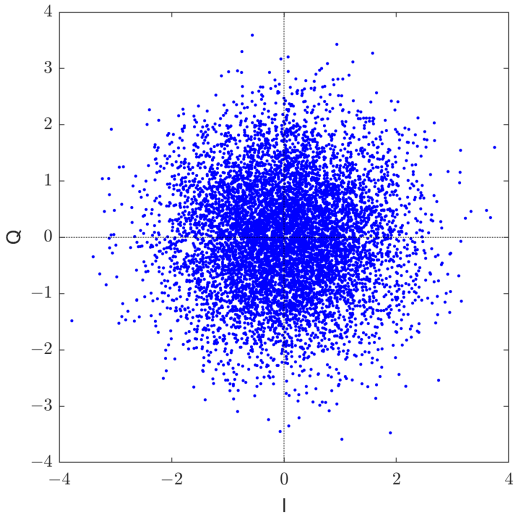


Figure 6. A collection of signal constellations of noise-free transmitted GDSS signal.

The transmitted noise free signal is compared against a standard Gaussian distribution (SGD) in Figure 7 and in Table 1 using 1×10^6 bits with a spreading factor of 256. The probability distribution shown in Figure 7 closely matches the theoretical Gaussian distribution. The Gaussian distribution is further supported in Table 1 from the estimated moments of the waveform depicting acceptable levels of commonality with the theoretical moments (calculated using Equation (4)).

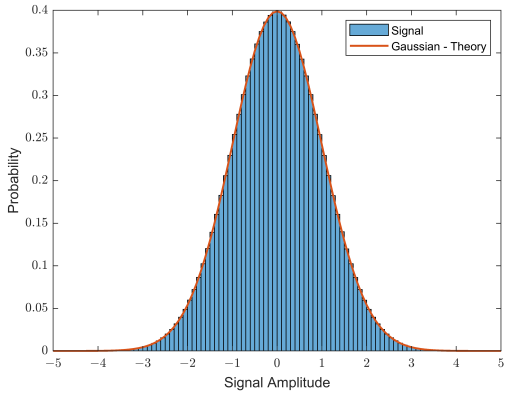


Figure 7. Distribution of the noise-free transmitted GDSS signal.

A random white noise signal would have an ACF of zero at all lags except a value of unity at lag zero, to indicate that the signal is uncorrelated and does not exhibit repetitive time-domain features. The repetitive features of the GDSS signals were analysed using the ACF. The results obtained showed no identifiable features for either GDSS or DSSS noise-free signals provided each uses non-repeating spreading sequences. However, for the case when these systems use a fixed pair of spreading sequences, the ACF for DSSS shows several very strong identifiable components across multiple lags. Compared to this, for the GDSS, the correlation magnitudes are small and are overall at an insignificant level.

Table 1. Moments of GDSS noise-free signal for $N = 256$.

Moment	SGD (Theory)	GDSS	DSSS
2nd	1	1	1
4th	3	3	1
6th	15	15	1
8th	105	105	1
10th	945	947	1
12th	10,395	10,428	1
14th	135,135	135,524	1
16th	2,027,025	2,025,880	1
18th	34,459,425	34,102,797	1
20th	654,729,075	634,790,833	1

4. Detectability of GDSS Signals

This section investigates detectability of the GDSS waveform at low SNR using higher-order moments and modulation stripping and compares the performance with DSSS signals. Simulated noise is generated using a random number generator to create a sequence of values that mimic the behaviour of real-world noise. The noise power is adjusted based on the desired SNR value to create noisy signals at different SNR levels.

4.1. Detection Using High-Order Moments

Moments are statistical parameters that can be used to measure Gaussian distribution as discussed in the previous section. In this section, the 20th-order moment is used to assess the detectability of the GDSS and DSSS signals operating under the noise floor. The 20th-order moment of the zero-mean unit-variance Gaussian distribution is 654,729,075. The moments of the GDSS and DSSS signal components are estimated at various SNR and then compared with the theoretical moment value using the absolute deviation between the estimated and theoretical values. The results are generated by averaging results from five tests and expressing the average deviation as a percentage of the theoretical value. Each test result is conducted using a spreading factor of 256 on 1×10^6 message bits. The signal values are first standardised using Equation (5) to have a mean of 0 and a standard deviation of 1 before estimating the moment:

$$z_i = \frac{r_i - \overline{r}}{\sigma} \tag{5}$$

where $\overline{r}$ and σ denote the mean and standard deviation of the signal values, respectively. The average deviation measures are plotted in Figure 8.

This figure shows that the average deviation of the DSSS signals are significantly large compared to GDSS values, indicating non-Gaussian features of the DSSS signal even in the presence of high noise levels. Unlike DSSS signals, the measures obtained for the GDSS signals show deviation values very close to zero across all SNR values.

Assuming an average deviation threshold of 10% (to achieve detection with high confidence), the moment-based detector will fail to detect the presence of a GDSS signal, whereas the same detector can easily detect the DSSS signals for SNR > −12 dB. It should be noted that the standard DSSS signal can be Gaussian distributed if the system operates at a sufficiently low SNR. However, this would require an increase in the spreading factor, resulting in a reduction of data rate.

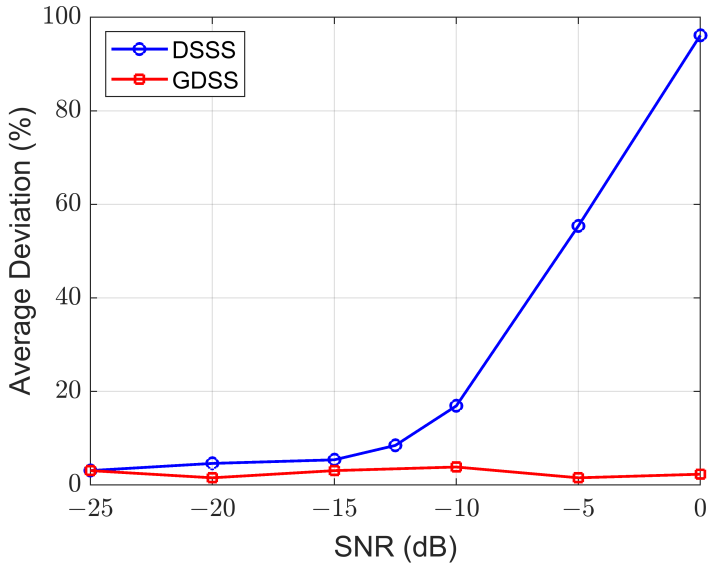
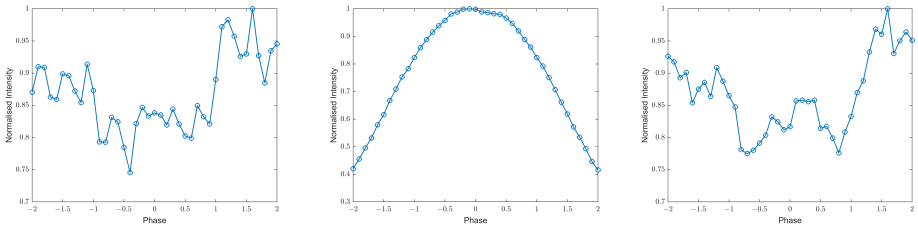


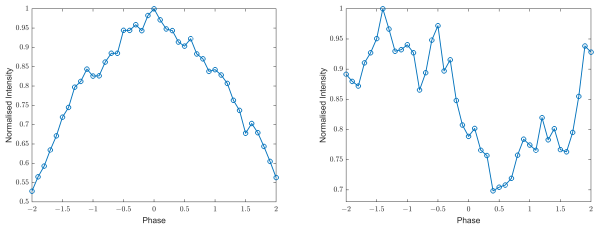
Figure 8. Average deviation of the estimated 20th-order moment from theory for $N = 256$.

4.2. Detection Using Modulation Stripping

In this section, a simple modulation stripping method is used to evaluate the detection performance of the GDSS signals. A non-linearity can be applied to the signal to produce discrete spectral spurs to aid detection. As an example, in the case of QPSK modulation, a fourth power produces a discrete spur at four times the carrier frequency offset. Figure 9 shows the distribution plots obtained for both GDSS and DSSS signals at different SNRs. The distribution plot generated from the detector for a set of Gaussian distributed complex values (Gaussian noise) is presented as a reference in Figure 9a. It should be noted that the developed GDSS scheme in Figure 9c,e also appear random with no significant phase distribution convergence. However, Figures 9b,d show a bell shaped distribution for the DSSS. This means that the phase distribution converges to a particular point, which gives evidence for a set constellation scheme being used, as opposed to the GDSS scheme and Gaussian noise.



(**a**) Gaussian Noise. (**b**) DSSS, SNR = 0 dB. (**c**) GDSS, SNR = 0 dB.



(**d**) DSSS, SNR = −5 dB. (**e**) GDSS, SNR = −5 dB.

Figure 9. Phase angle modulation stripping detector with QPSK, normalised intensity versus phase, $N = 256$.

4.3. Energy Detector

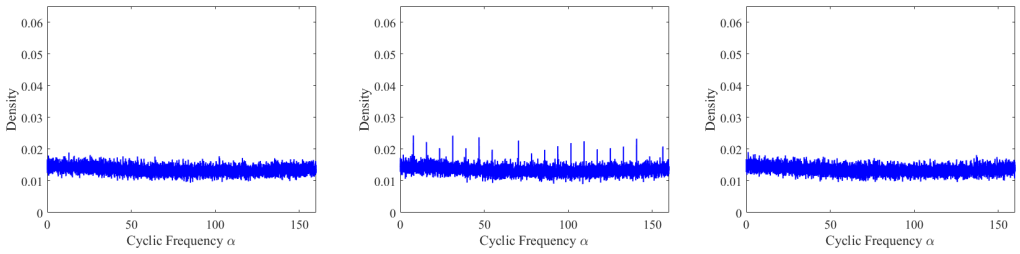
Energy detection is another commonly used method for detecting communication signals. The basic idea behind energy detection is to compare the energy of the received signal to a pre-defined threshold. If the energy of the received signal exceeds this threshold, the signal is assumed to be present. One of the advantages of the energy detection method is its simplicity and low computational complexity. However, energy detection can suffer from high false alarm rates in low SNR environments, where the noise can easily exceed the detection threshold. Therefore, energy detectors are generally not effective for detecting signals, such as DSSS and GDSS signals, operating under the noise floor. As the GDSS system requires more power than the DSSS system to achieve the same BER performance, it is expected that GDSS signals can be more likely detected compared to DSSS signals using an energy detector in high SNR conditions.

4.4. Cyclostationary Analysis

Signal detectors based on cyclostationary analysis offer superior detection performance compared to energy detectors in low SNR environments. However, they may require more computational resources and expertise in signal properties. Cyclostationary analysis is a powerful technique used for detecting and analysing communication signals by leveraging their cyclostationary properties. These properties refer to repetitive characteristics of the signal, such as a constant modulation and coding scheme or a fixed synchronisation sequence embedded in the communication waveform. By exploiting these properties, cyclostationary analysis can provide more reliable detection and analysis of signals in challenging environments with low SNR.

Cyclostationary analysis normally involves estimating the spectral correlation function (SCF) of a signal. The SCF is a measure of the correlation between different frequency components of the signal, as a function of frequency offset and time lag. In a cyclostationary signal, the SCF exhibits peaks at certain frequency offsets and time lags, known as cyclic frequencies and cycle periods, respectively. These peaks correspond to the cyclostationary properties of the signal and can be used to detect the presence of the signal operating under the noise floor. By exploiting these peaks, cyclostationary analysis can offer a more robust and reliable detection of weak signals.

This section aims to validate the effectiveness of GDSS signals in hiding under the noise floor using the fast spectral correlation method proposed in [41]. We present a comparison of the results obtained with the DSSS signal, as shown in Figure 10.



(**a**) Gaussian Noise. (**b**) DSSS, SNR = −12 dB. (**c**) GDSS, SNR = −12dB.

Figure 10. Spectral correlation spectrum for various signals, $N = 256$.

The DSSS signal is generated using a repetitive spreading sequence, and the Gaussian masking process is applied to develop the GDSS signal. To ensure a fair comparison, we keep the observation period and spreading factor constant for both the DSSS and GDSS signals. By analysing the spectral correlation of the two signals, we demonstrate that the GDSS signal provides superior hiding capabilities compared to the DSSS signal under similar conditions. Our findings highlight the potential of GDSS signals for use in low-

power and covert communication systems where signal detection and interception are critical concerns.

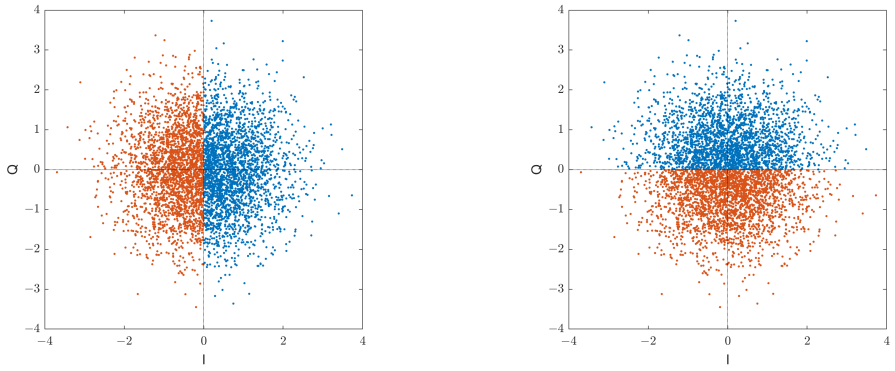
The spectral correlation density plots shown in Figure 10 illustrate the significant difference between the DSSS and GDSS signals. The DSSS signal exhibits prominent peaks in its spectrum, indicating the presence of repetitive spreading sequences and modulation. In contrast, the application of the Gaussian masking process to the DSSS signal has almost entirely eliminated these peaks. As a result, the GDSS spectrum closely resembles the spectral correlation spectrum generated for the noise-only case (i.e., without any signal). GDSS signal exhibits a much flatter spectrum, with no noticeable peaks. These findings provide strong evidence supporting the superiority of the GDSS method over the DSSS. By eliminating the characteristic peaks of the DSSS signal, the GDSS signal is much harder to detect and intercept, making it a better choice for covert communication systems.

5. BER Performance

This section investigates the BER performance of the uncoded and coded GDSS systems and compares them with the corresponding DSSS systems.

5.1. Uncoded BER Performance

In this section we develop a semi-numerical calculation of the BER performance for the uncoded GDSS system and compare it with the simulated results. The BER performance can be analysed from the I or Q component. Assuming Gray coding is used, the two components are equivalent to two independent BPSK GDSS schemes (Figure 11). The BER performance of the QPSK GDSS is identical to the BPSK GDSS in terms of energy per bit to noise power spectral density ratio (E_b/N_0) or 3dB worse in terms of SNR.



(**a**) BPSK GDSS on I axis. (**b**) BPSK GDSS on Q axis.

Figure 11. Component BPSK GDSS scatters of the QPSK GDSS signal.

Our objective is to determine the probability density function (PDF) of the decision variable z, which is the result of the de-spreading process using a binary spreading sequence (rather than a Gaussian sequence). Here, z is the sum of N noisy chips during a bit period

$$z = \sum_{i=1}^{N} r_i \tag{6}$$

where $r_i = s_i + n_i$ is a received chip, s_i and n_i are members of the signal sequence $s = (s_1, s_2, \cdots, s_N)$ and noise sequence $n = (n_1, n_2, \cdots, n_N)$, respectively.

The BER is the probability the decision variable becoming negative due to noise disturbance

$$\text{BER} = \int_{-\infty}^{0} p_z(z)dz \tag{7}$$

In order to find $p_z(z)$, we start at one chip's PDF. The signal chip s_i follows a half-normal distribution [42,43]

$$s_i \sim p_{s_i}(x) = \begin{cases} \frac{\sqrt{2}}{\sigma_s\sqrt{\pi}} \exp\left(\frac{-x^2}{2\sigma_s^2}\right), & x \geq 0, \\ 0, & x < 0 \end{cases} \tag{8}$$

The corresponding noise n_i follows a Gaussian distribution

$$n_i \sim p_{n_i}(x) = \frac{1}{\sigma_n\sqrt{2\pi}} \exp\left(\frac{-x^2}{2\sigma_n^2}\right) \tag{9}$$

Since s_i and n_i are mutually independent, the PDF of the sum r_i is the convolution of PDF's of the summands

$$r_i \sim p_{r_i}(x) = p_{s_i}(x) * p_{n_i}(x) \tag{10}$$

where $*$ denotes a convolution. Using Mathematica, we derive the PDF of one noisy chip

$$p_{r_i}(x) = \frac{\exp\left(\frac{-x^2}{2(\sigma_s^2+\sigma_n^2)}\right)\left(1+\operatorname{erf}\left(\frac{\sigma_s x}{\sigma_n\sqrt{2(\sigma_s^2+\sigma_n^2)}}\right)\right)}{\sqrt{2\pi(\sigma_s^2+\sigma_n^2)}} \tag{11}$$

It can be expressed as a function of SNR. For QPSK GDSS, the SNR in dB is

$$\xi = 10\log_{10}\left(\frac{\sigma_s^2}{\sigma_n^2}\right) \tag{12}$$

For BER calculations we can let $\sigma_s^2 = 1$ without loss of generality. We have

$$p_{r_i}(x) = \frac{\exp\left(\frac{-x^2}{1+10^{-\xi/10}}\right)\left(1+\operatorname{erf}\left(\frac{x10^{\xi/20}}{\sqrt{1+10^{-\xi/10}}}\right)\right)}{\sqrt{\pi(1+10^{-\xi/10})}} \tag{13}$$

If we can find the characteristic function of $p_{r_i}(x)$ then $p_z(z)$ is the inverse Fourier transform of the Nth power of the characteristic function. Regrettably, we are unable to obtain an analytical expression for it. An alternative approach is to use self-convolution. As z is the sum of N independent r_i, its PDF is the $N-1$ self-convolutions

$$p_z(z) = \underbrace{p_{r_i}(x) * p_{r_i}(x) * p_{r_i}(x) * \cdots * p_{r_i}(x)}_{N} \tag{14}$$

where * denotes a convolution. Once again, we were unable to derive an analytical solution and had to resort to numerical convolution techniques. To avoid overflow issues when dealing with large values of N, we created a normalized function

$$y_1(x) = p_{r_i}(x)\Delta_x \tag{15}$$

so that $\sum_x y_1(x) = 1$, where Δ_x is the increment of the x vector. For the sum of N received chips, the PDF is proportional to the $N-1$ self numerical convolutions (also denoted by $*$)

$$y_N(x) = \underbrace{y_1(x) * y_1(x) * \cdots * y_1(x)}_{N} = \overbrace{*}^{N-1} y_1(x) \tag{16}$$

Performing $N-1$ numerical convolutions using brute force computation is both expensive and unnecessary for large values of N. Instead, a faster algorithm can be implemented, as illustrated below.

We calculate $m = \lfloor \log_2 N \rfloor$ pairs of convolutions first:

$$\begin{aligned} y_2(x) &= y_1(x) * y_1(x) \\ y_4(x) &= y_2(x) * y_2(x) \\ y_8(x) &= y_4(x) * y_4(x) \\ &\cdots \\ y_{2^m}(x) &= y_{2^{m/2}}(x) * y_{2^{m/2}}(x) \end{aligned} \tag{17}$$

If N is an integer that is a power of two, our objective has been achieved. However, if N lies in the range $2^m < N < 2^{m+1}$, further convolutions are necessary, using the m results from Equation (17) as the foundational building blocks. Only those terms corresponding to the ones of N in binary form N_{bin} are required. For example, $N = 50 = 2^5 + 2^4 + 0 + 0 + 2^1 + 0$, in binary form it is $N_{bin} = 110,010$. Only two more convolutions are required.

$$y_{50}(x) = y_{2^5}(x) * y_{2^4}(x) * y_{2^1}(x) = y_{32}(x) * y_{16}(x) * y_2(x) \tag{18}$$

We see that instead of 49 convolutions, we only need to conduct 7 of them. In general, the required number of convolutions is

$$n_c = \lfloor \log_2 N \rfloor + \mathrm{W}(N_{bin}) - 1 \tag{19}$$

where $\mathrm{W}(N_{bin})$ is the binary weight function, producing the sum of ones in the binary number N_{bin}. The n_c is upper bounded by $2m$. These are plotted in Figure 12.

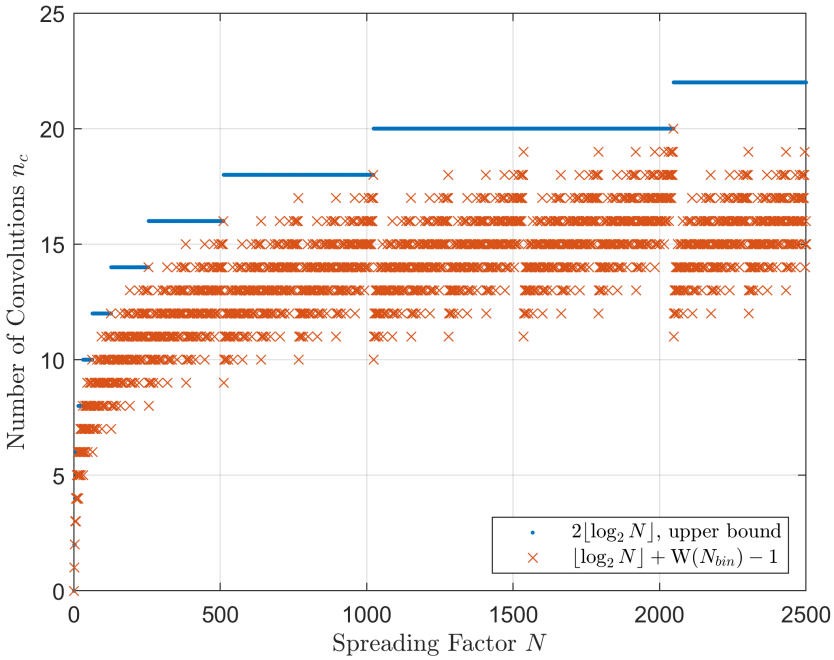


Figure 12. Uncoded GDSS BER computation: number of numerical convolutions n_c and its upper bound, versus spreading factor N.

Finally, the PDF for the decision variable, the sum of N de-spread chips, is

$$p_z(z) = \frac{y_N(x)}{\Delta_x} = \frac{\overbrace{* \; y_1(x)}^{N-1}}{\Delta_x} \tag{20}$$

Note here we did not distinguish the variables z and x. Some computed $p_z(z)$ and histograms are plotted in Figure 13. Calculations and simulations agree very well.

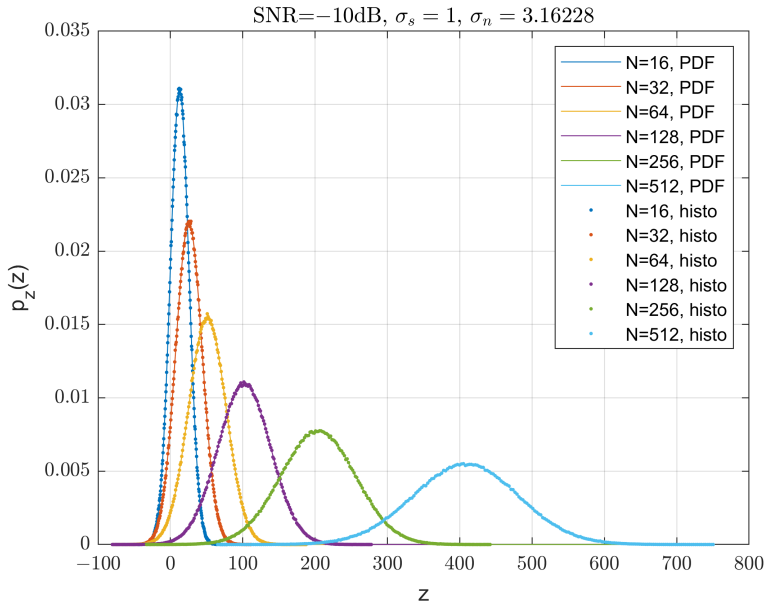


Figure 13. A selection calculated PDFs of the decision variable $p_z(z)$ and Monte Carlo histograms.

In numerical calculations

$$\text{BER} = \sum_{x_i=x_{min}}^{0} p_z(x_i)\Delta x \tag{21}$$

where x_{min} and Δx need to be chosen carefully to ensure the calculation is valid. To check it, we test if the total sum is one or near one. Practically, we use $\Delta x = 0.01$ and satisfy

$$\sum_{x_i=x_{min}}^{x_{max}} p_z(x_i)\Delta x \geq 0.995 \tag{22}$$

It is only difficult to satisfy this condition at very low SNRs, for example, $\xi = -35$ dB. For medium low to high SNRs, most sums are equal to 1. It also depends on the spreading factor N. The $x_{max} = -x_{min}$ are pre-calculated by a trial-and-error method. For $N = [16, 32, 64, 128, 256, 512, 1028, 2048]$, the x_{max} obtained are $x_{max} = [7700, 9900, 14300, 10450, 9900, 8800, 5500, 5500]$. The batch computation for the 8 BER curves in Figure 14 took about 12 h on a desktop PC with an i7 CPU at 3 GHz.

The BER performance of the uncoded QPSK DSSS systems are also plotted in Figure 14. The theoretic calculations and Monte Carlo simulations agree very well.

The figure shows that the Gaussian distributed scheme performs 2.5 dB worse than DSSS for a spreading factor of $N = 64$ at a target BER of 10^{-5}. This loss reduces to 2 dB when $N \geq 512$.

5.2. LDPC-Coded GDSS System

This section investigates the use of low density parity check (LDPC) coding to improve the performance for the GDSS scheme. LDPC codes are a type of linear block error correction codes with parity-check matrices (H) that contain a very small number of non-zero entries. The sparseness of H guarantees the minimum Hamming distance and decoding complexity to increase linearly with the code length. Some of the published results show that these codes can perform close to 0.0045 dB away from the Shannon Limit, making it one of the most powerful error-correction codes known today [44]. To reduce the decoding latency a short half-rate LDPC code with number of message bits k = 324 and codeword length n = 648 bits were used for both the GDSS and the traditional DSSS system. The results obtained are presented in Figure 15.

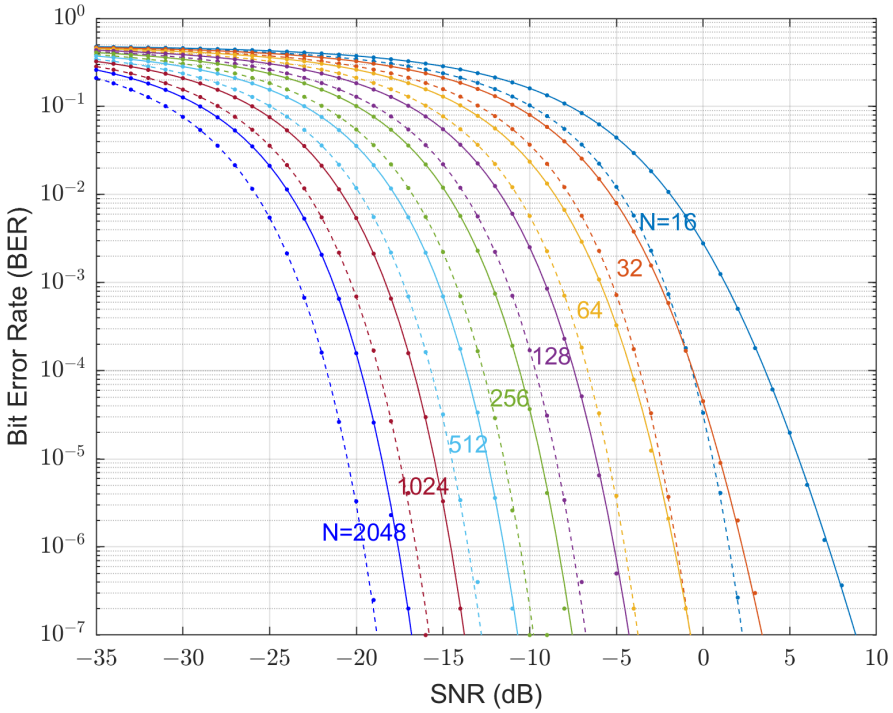


Figure 14. Uncoded BER performance: theoretical QPSK GDSS (solid lines) and QPSK DSSS (dashed lines) with various spreading factor N, and corresponding simulation results (dots).

Figure 15 compares SNR for fixed bandwidth, i.e., the same chip rate in each case. The 1/2-rate coded-GDSS [N = 128] scheme has a power advantage of approximately 5 dB against the uncoded DSSS [N = 256] on the basis of identical information bit rate. However, a comparison of both coded systems (coded-GDSS with coded-DSSS) showed similar performance reduction that was observed for the uncoded system comparison in Section 5.1.

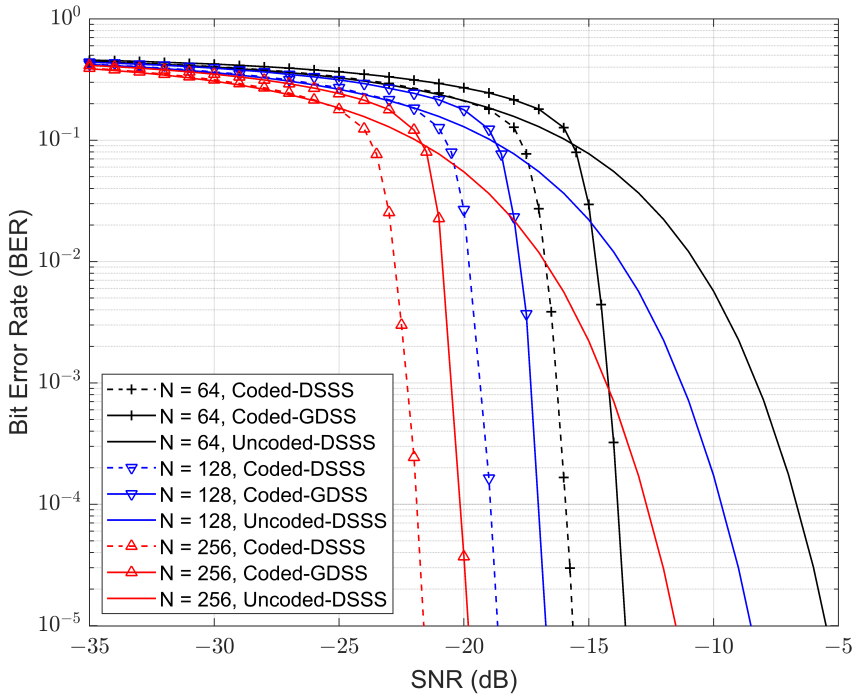


Figure 15. Comparison of LDPC encoded GDSS QPSK system with varying spreading factors against the theoretical DSSS QPSK system's upper performance bound.

6. Conclusions

In this paper, we propose a novel signalling scheme called GDSS for covert (LPD) communications, which aims to conceal the existence of wireless transmissions for enhanced security compared to cryptography and steganography-based schemes. We evaluate the performance of GDSS and compare it with the commonly used DSSS technique, which, despite its popularity, is susceptible to exploitation by adversaries due to various weaknesses. These vulnerabilities stem from the use of fixed modulation and repeatable spreading sequences. In contrast, the proposed GDSS scheme takes advantage of naturally occurring thermal noise at the transmitter to create non-repetitive, featureless signals for communication, which eliminates many of the shortcomings associated with DSSS. In this paper, the proposed GDSS scheme is compared with the DSSS system. The findings indicated that the signals produced by the GDSS approach have fewer distinctive characteristics compared to the DSSS signals, resulting in a reduced likelihood of detection for anyone attempting to intercept the transmission. The Gaussianity test demonstrated that the distribution of the noise-free GDSS signals closely resembled that of the naturally occurring noise in the receiver. To assess the detectability of the signals generated by the proposed scheme by an adversary, this study utilised three detectors: a high-order moments based detector, a modulation stripping detector, and a detector based on cyclostationary analysis. These detectors are applied to signals corrupted with noise. The results showed that the moment-based detector failed to detect the GDSS signal with $N = 256$ at all SNRs, whereas it could easily detect the DSSS signals as low as −12 dB. We applied the modulation stripping detector to both the GDSS and DSSS signals at an SNR of 0 dB and −5 dB, respectively. Our analysis revealed that the GDSS signals exhibited no significant phase distribution convergence, similar to the noise-only case (i.e., without any signal). In contrast, the DSSS signals generated a phase distribution with a distinct shape, indicating the presence of a valid signal. Moreover, we applied the spectral correlation detector to the GDSS signal at an SNR of −12 dB. Our analysis showed no identifiable peaks on the spectral correlation spectrum, providing additional evidence of the effectiveness of the GDSS scheme and the lack of distinguishable peaks in the spectrum suggests that the GDSS signal is difficult to detect and intercept, making it an ideal choice for covert communication applications.

A quasi-analytical expression is also used to derive the BER for the uncoded GDSS, and the results were consistent with the simulation. The comparison of BER between the uncoded GDSS and DSSS systems showed a penalty of 2 to 3 dB for GDSS. However, LDPC coding helped recover this loss and significantly improved the overall BER performance. As expected, the LDPC-coded GDSS performed about 2 dB worse than the corresponding LDPC-coded DSSS system.

This paper did not investigate the effects of high power amplifiers on the generated GDSS signals. The GDSS scheme is capable of generating signals with a high peak-to-average power ratio (PAPR), which is a measure of the dynamic range of a signal. Consequently, amplifying GDSS signals can cause distortion or clipping, as the amplifier may not be able to handle the high instantaneous power levels (albeit rarely happen), which can result in reduced signal quality and performance degradation.

In future work, we plan to analyse the information-theoretic optimality of the proposed GDSS scheme and its variants. We would also like to investigate the impact of real-world factors such as radio impairments, channel effects, and receiver synchronisation on the performance of the GDSS system. These factors can significantly affect the quality and reliability of the communication channel, and thus it is crucial to study their effects on the proposed scheme. Additionally, we plan to explore ways to mitigate the high PAPR issue of the GDSS signals, which can lead to performance degradation.

Author Contributions: Conceptualization, I.S.; Methodology, I.S.; Software, I.S., J.H. and W.Z.; Validation, I.S., J.H. and W.Z.; Formal analysis, I.S. and W.Z.; Investigation, I.S., J.H. and W.Z.; Uncoded BER calculation: W.Z.; Writing—original draft, I.S., J.H. and W.Z.; Writing—review & editing, M.R., I.S. and W.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Varghese, F.; Sasikala, P. A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography. *Springer Wirel. Pers. Commun.* **2023**, *129*, 2291–2318. [CrossRef]
2. Oladipupo, E.T.; Abikoye, O.C.; Imoize, A.L.; Awotunde, J.B.; Chang, T.Y.; Lee, C.C.; Do, D.T. An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks. *IEEE Access* **2023**, *11*, 1306–1323. [CrossRef]
3. Li, M.; Liu, Y.; Tian, Z.; Shan, C. Privacy Protection Method Based on Multidimensional Feature Fusion Under 6G Networks. *IEEE Trans. Netw. Sci. Eng. (Early Access)* **2022**, *1*, 1–14. [CrossRef]
4. Ambika; Virupakshappa; Veerashetty, S. Secure Communication over Wireless Sensor Network using Image Steganography with Generative Adversarial Networks. *Meas. Sens.* **2022**, *24*, 100452.
5. Sharma, H.; Kumar, N.; Tekchandani, R. Physical Layer Security using Beamforming Techniques for 5G and Beyond Networks: A Systematic Review. *Phys. Commun.* **2022**, *54*, 101791.
6. Glenn, A. Low Probability of Intercept. *IEEE Commun. Mag.* **1983**, *21*, 26–33. [CrossRef]
7. Turner, L.The Evolution of Featureless Waveforms for LPI Communications. In Proceedings of the IEEE 1991 National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 20–24 May 1991; 1325–1331.
8. Makhdoom, K.; Abolhasan, M.; Lipman, J. A Comprehensive Survey of Covert Communication Techniques, Limitations and Future Challenges. *Comput. Secur.* **2022**, *120*, 102784. [CrossRef]
9. Anand, A.; Singh, A.K. A Comprehensive Study of Deep Learning-based Covert Communication. ACM Transactions on Multimedia Computing. *Commun. Appl.* **2022**, *18*, 1–19.
10. Huang, K.W.; Wang, H.M.; Towsley, D.; Poor, H.V. LPD Communication: A Sequential Change-Point Detection Perspective. *IEEE Trans. Commun.* **2020**, *68*, 2474–2490. [CrossRef]
11. Bash, B.A.; Goeckel, D.; Towsley, D.; Guha, S. Hiding Information in Noise: Fundamental Limits of Covert Wireless Communication. *IEEE Commun. Mag.* **2015**, *53*, 26–31.
12. Yan, S.; Zhou, X.; Hu, J.; Hanly, S.V. Low Probability of Detection Communication: Opportunities and Challenges. *IEEE Wirel. Commun.* **2019**, *26*, 19–25. [CrossRef]
13. Bash, B.A.; Goeckel, D.; Towsley, D. Limits of Reliable Communication With Low Probability of Detection on AWGN Channels. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1921–1930. [CrossRef]
14. Ma, R.; Yang, W.; Tao, L.; Lu, X.; Xiang, Z.; Liu, J. Covert Communications With Randomly Distributed Wardens in the Finite Blocklength Regime. *IEEE Trans. Veh. Technol.* **2022**, *71*, 533–544. [CrossRef]
15. Kaddoum, G. Wireless Chaos-based Communication Systems: A Comprehensive Survey. *IEEE Access* **2016**, *4*, 2621–2648. [CrossRef]
16. Eisencraft, M.; Monteiro, L.H.; Soriano, D.C. White Gaussian Chaos. *IEEE Commun. Lett.* **2017**, *8*, 1719–1722. [CrossRef]
17. Michaels, A.J.; Chester, D.B. Efficient and Flexible Chaotic Communication Waveform Family. In Proceedings of the 2010—Milcom 2010 Military Communications Conference, San Jose, CA, USA, 31 October 2010–3 November 2010.
18. Shakeel, I. Machine Learning Based Featureless Signalling. In Proceedings of the MILCOM 2018— 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018.
19. Norris, J.; Nieto, J. Application of Sub-Sample Dithering to Reduce Probability of Signal Detection. In Proceedings of the 2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 29 November 2021–2 December 2021; pp. 916–920.
20. Zhu, Z.A.; Nandi, A.K. *Automatic Modulation Classification: Principles, Algorithms and Applications*; Wiley: London, UK, 2015.
21. Burel, G.; Bouder, C. Blind Estimation of the Pseudo-random Sequence of a Direct Sequence Spread Spectrum Signal. In Proceedings of the MILCOM 2000 Proceedings, 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No.00CH37155), Los Angeles, CA, USA, 22–25 October 2000.
22. Gardner, W.A.; Spooner, C.M. Signal Interception Performance Advantages of Cyclic-feature Detectors. *IEEE Trans. Commun.* **1992**, *40*, 149–159. [CrossRef]
23. Vlok, J.D.; Olivier, J.C. Blind Sequence-length Estimation of Low-SNR Cyclostationary Sequences. *IET Commun.* **2014**, *8*, 1578–1588. [CrossRef]
24. Choi, J.; Ahn, J.; Choe, C.; Shin, Y.; Park, D.; Ahn, S. Practical LPI Communication with Noise-Shaped Signaling. In Proceedings of the 2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 16–18 October 2019; pp. 332–337.

25. Michaels, A.J.; Chester, D.B. Featureless Chaotic Spread Spectrum Modulation of Arbitrary Data Constellations.In Proceedings of the 2011 IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications, San Francisco, CA, USA, 26–29 June 2011; pp. 36–40.
26. Guo, S.; Fu, Y. A Time-Varying Chaotic Multitone Communication Method Based on OFDM for Low Detection Probability of Eavesdroppers. *IEEE Access* **2021**, *9*, 107566–107573. [CrossRef]
27. Nguyen, L. Self-encoded Spread Spectrum and Multiple Access Communications. In Proceedings of the 2000 IEEE Sixth International Symposium on Spread Spectrum Techniques and Applications. ISSTA 2000. Proceedings (Cat. No.00TH8536), Parsippany, NJ, USA, 6–8 September 2000; pp. 394–398.
28. Shahzad, K.; Zhou, X.; Yan, S. Covert Communication in Fading Channels under Channel Uncertainty. In Proceedings of the IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, Australia, 4–7 June 2017; pp. 1–5.
29. He, B.; Yan, S.; Zhou, X.; Lau, V.K. On Covert Communication with Noise Uncertainty. IEEE *Commun. Lett.* **2017**, *21*, 941–944. [CrossRef]
30. Bash, B.; Goeckel, D.; Towsley, D. Covert Communication Gains from Adversary's Ignorance of Transmission Time. *IEEE Trans. Wirel. Commun.*, **2016**, *15*, 8394–8405. [CrossRef]
31. Sobers, T.; Bash, B.A.; Guha, S.; Towsley, D.; Goeckel, D. Covert Communication in the Presence of an Uninformed Jammer. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 6193–6206. [CrossRef]
32. Zhang, Y.; Li, Y.; Xiang, W.; Wang, J.; Xiao, S.; Li, X.; Tang, W. The Optimal Precoded Faster-Than-Nyquist Signaling for Covert Communications. *IEEE Commun. Lett.* **2022**, *26*, 1249–1253. [CrossRef]
33. Kim, S.W.; Ta, H.Q. Covert Communication by Exploiting Node Multiplicity and Channel Variations. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
34. Zheng, T.X.; Wang, H.M.; Ng, D.W.K.; Yuan, J. Multi-antenna Covert Communications in Random Wireless Networks. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 1974–1987. [CrossRef]
35. Lee, K.A.; Barry, J.R. Opportunistic Power Control for Low Probability of Detection Communication. In Proceedings of the IEEE Military Communications Conference, Rockville, MD, USA, 28 November 2022–2 December 2022; pp. 667–671.
36. Soltani, R.; Goeckel, D.; Towsley, D.; Bash, B.A.; Guha, S. Covert Wireless Communication with Artificial Noise Generation. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 7252–7267. [CrossRef]
37. Jamali, M.V.; Mahdavifar, H. Covert Millimeter-Wave Communication: Design Strategies and Performance Analysis. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 3691–3704. [CrossRef]
38. Sudhakar, J.; Shaik, F.B.; Hari, J. FPGA Implementation of PN-sequence Generator with Binary Chaos Synchronization. In Proceedings of the 2014 International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 13–14 February 2014; pp. 1–7.
39. Popper, C.; Strasser, M.; Capkun, S. Anti-jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques. *IEEE J. Sel. Areas Commun.* **2010**, *28*, 703–715. [CrossRef]
40. Bohm, G.; Zech, G. *Introduction to Statistics and Data Analysis for Physicists*; Verlag Deutsches Elektronen-Synchrotron: Berlin, Germany, 2010.
41. Antoni, J.; Xin, G.; Hamzaoui, N. Fast Computation of the Spectral Correlation. *Mech. Syst. Signal Process.* **2017**, *92*, 248–277. [CrossRef]
42. Half-Normal Distribution, from Wikipedia, the Free Encyclopedia. Available online: https://en.wikipedia.org/wiki/Half-normal_distribution (accessed on 30 March 2023).
43. Weisstein, E.W. Half-Normal Distribution, From MathWorld—A Wolfram Web Resource. Available online: https://mathworld.wolfram.com/Half-NormalDistribution.html (accessed on 30 March 2023).
44. Chung, S.Y.; Chung, S.Y.; Forney, G.D.; Richardson, T.J.; Urbanke, R. On the Design of Low-Density Parity-Check Codes within 0.0045 dB of the Shannon Limit. *IEEE Commun. Lett.* **2001**, *5*, 58–60. [CrossRef]