Accepted for publication in IEEE Wireless Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LWC.2025.3540043

Covert Communications Without Pre-Sharing of Side Information and Channel Estimation Over Quasi-Static Fading Channels

Hiroki Fukada, *Graduate Student Member, IEEE*, Hiroki Iimori, *Member, IEEE*, Chandan Pradhan, *Member, IEEE*, Szabolcs Malomsoky, and Naoki Ishikawa, *Senior Member, IEEE*.

***Abstract*—We propose a new covert communication scheme that operates without pre-sharing side information and channel estimation, utilizing a Gaussian-distributed Grassmann constellation for noncoherent detection. By designing constant-amplitude symbols on the Grassmann manifold and multiplying them by random variables, we generate signals that follow an arbitrary probability distribution, such as Gaussian or skew-normal distributions. The mathematical property of the manifold enables the transmitter's random variables to remain unshared with the receiver, and the elimination of pilot symbols that could compromise covertness. The proposed scheme achieved higher covertness and achievable rates compared to conventional coherent Gaussian signaling schemes, without any penalty in terms of complexity.**

***Index Terms*—Covert communications, Grassmann manifold, noncoherent detection, quasi-static fading channels.**

I. Introduction

COVERT communication aims to convey confidential information without revealing the existence of the communication itself to third parties [1]. This concept has been investigated for a multitude of communication systems, including military, cellular networks, IoT, unmanned aerial vehicles (UAVs), and satellite networks [2]. The performance of covert communications has been studied from theoretical as well as practical perspectives. It has been shown that when the input to an additive white Gaussian noise (AWGN) channel follows a Gaussian distribution, the information rate is proportional to the square root of the Gaussian channel length [3], and the covertness is maximized [4]. In parallel, the chaos-based modulation scheme has been proposed as an efficient approach for generating Gaussian-distributed signals [5], which can be considered suitable for covert communications.

For practical covert communication scenarios, channel estimation remains indispensable but poses a critical problem, as the frequent transmission of the pilots is required to improve the estimation accuracy, but simultaneously, it can be exploited by the third parties to estimate their channel, thereby leading to a significant reduction in covertness [6]. For such a problem, Katsuki et al. have proposed a new noncoherent communication system based on differential encoding [7], where the projection onto the Gaussian distribution generates Gaussian signaling: however, for decoding, it requires at least one substantial reference symbol block. In addition, similar to the chaos-based modulation [5], it necessitates the perfect sharing of a side information related to the projection in advance, which has been an open issue in the design of practical systems.

To address the limitations of conventional studies, we propose a noncoherent covert communication scheme, where the information can be decoded without channel estimation as well as side information (e.g., the chaos transition [5] and the projection matrix [7]) that generates Gaussian signals at legitimate transceivers. Unlike other benchmarks, our approach eliminates the necessity of transmitting any pilot symbols and sharing side information, making covert communications more practical. The major contributions are twofold.

1) *We design Grassmann symbols distributed on a unit circle and generate symbols that follow a Gaussian distribution* by multiplying them with Gaussian-distributed random variables. This process does not hinder noncoherent detection and requires no sharing of side information. Additionally, it can support symbol generations following an arbitrary probability distribution.[1]
2) *We compare the proposed noncoherent scheme with two coherent detection-based schemes considered as benchmarks, demonstrating a higher covertness.* Then, we analyze the channel estimation errors that occur when transmitting Gaussian-distributed pilot symbols, showing that the proposed scheme also excels in terms of achievable rate.

II. System Model

A quasi-static Rayleigh fading channel is considered in this letter. A legitimate transmitter, Alice, communicates with a legitimate receiver, Bob, and a warden, Willie, tries to detect the communication. We assume that the channel matrices between Alice-Bob and Alice-Willie are perfectly uncorrelated.

A. Alice-Bob Channel

Firstly, we consider coherent detection systems. Let $\mathcal{H}_1$ denote the event that Alice transmits information, and $\mathcal{H}_0$ the event that she does not. For simplicity, we assume the perfect timing synchronization between the legitimate transceiver.

We focus on the event with $\mathcal{H}_1$. As illustrated in Fig. 1, a frame consists of T_P symbols $\mathbf{p} = [p_1 \ \cdots \ p_{T_P}] \in \mathbb{C}^{T_P}$ for pilot transmission and T_D symbols $\mathbf{s} = [s_1 \ \cdots \ s_{T_D}] \in \mathbb{C}^{T_D}$ for data transmission carrying B information bits. Let $T \triangleq T_P + T_D$, and the transmit symbol vector is expressed as $[\mathbf{p} \ \mathbf{s}] \in \mathbb{C}^T$. The received symbol vector at Bob is given by

$$\mathbf{y}_b = \mathbf{s}h_b + \mathbf{n}_b, \tag{1}$$

H. Fukada and N. Ishikawa are with the Faculty of Engineering, Yokohama National University, 240-8501 Kanagawa, Japan (e-mail: ishikawa-naoki-fr@ynu.ac.jp). H. Iimori, C. Pradhan, and S. Malomsoky are with Ericsson Research, Ericsson Japan K.K., 220-0012 Kanagawa, Japan.

[1]In terms of mutual information, the Gaussian signaling can be outperformed by the skew-normal signaling [4], which is supported by our scheme.

©2025 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. DOI: 10.1109/LWC.2025.3540043

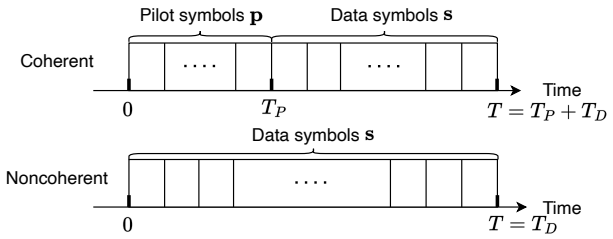


Fig. 1. Frame structure assumed in coherent and noncoherent systems.

where $h_b \sim \mathcal{CN}(0,1)$ denotes the channel coefficient of Bob, and $\mathbf{n}_b$ denotes an AWGN vector with each element following $\mathcal{CN}\big(0,\sigma_b^2\big)$. The received signal-to-noise ratio (SNR) at Bob is then defined as $\gamma_b \triangleq \mathbb{E}[\|\mathbf{s}h_b\|^2]/\mathbb{E}[\|\mathbf{n}_b\|^2] = 1/\sigma_b^2$.

Bob estimates his own channel by the minimum mean square error (MMSE) equalizer. Let $\mathbf{y}_{b,P} \in \mathbb{C}^{T_P}$ denote the received symbols corresponding to the pilot symbols, and the estimated channel is then expressed as $\hat{h}_b = \mathbf{y}_{b,P}(\|\mathbf{p}\|^2 + \sigma_b^2)^{-1}\mathbf{p}^{\mathrm{H}}$, with $(\cdot)^{\mathrm{H}}$ representing the conjugate transpose. Note that the pilot symbols used for channel estimation have to be shared with the legitimate receiver before data transmission.

B. Detection Error Probability at Willie

Willie monitors the Alice-Bob communication channel and aims to detect the existence of their communication. We assume that Willie can perform perfect synchronization such that the received signal is sampled at the Nyquist rate. The received symbol vector is $\mathbf{y}_w = \mathbf{n}_w$ for $\mathcal{H}_0$ and $\mathbf{s}h_w + \mathbf{n}_w$ for $\mathcal{H}_1$, where $h_w \sim \mathcal{CN}(0,1)$ denotes the channel coefficient of Willie and $\mathbf{n}_w$ denotes an AWGN vector. The received SNR at Willie is defined as $\gamma_w \triangleq \mathbb{E}[\|\mathbf{s}h_w\|^2]/\mathbb{E}[\|\mathbf{n}_w\|^2] = 1/\sigma_w^2$.

Assuming that $\mathbf{s}$ consists of independent and identically distributed (i.i.d) Gaussian random variables (RVs) of length T, Willie estimates the existence of communication with a threshold λ and the radio meter detection [8]

$$\frac{\|\mathbf{y}_w\|^2}{T} \underset{\hat{\mathcal{H}}_0}{\overset{\hat{\mathcal{H}}_1}{\gtrless}} \lambda, \tag{2}$$

where $\hat{\mathcal{H}}_i$ with $i \in \{0,1\}$ is the estimated event by Willie.[2]

Under the assumption that both events $\mathcal{H}_0$ and $\mathcal{H}_1$ occur with an equal probability, the detection error probability (DEP) at Willie is given by $P_{e,w}(\lambda) = (P_{\mathrm{FA}}(\lambda) + P_{\mathrm{MD}}(\lambda))/2$ [3], where $P_{\mathrm{FA}}(\lambda)$ and $P_{\mathrm{MD}}(\lambda)$ are the probabilities of the false alarm and the miss detection, respectively. Both are expressed as $P_{\mathrm{FA}}(\lambda) \triangleq P(\hat{\mathcal{H}}_1 \mid \mathcal{H}_0) = 1 - \gamma(T, T\lambda/\gamma_w^{-1})/(T-1)!$ and $P_{\mathrm{MD}}(\lambda) \triangleq P(\hat{\mathcal{H}}_0 \mid \mathcal{H}_1) = \gamma(T, T\lambda/(|h_w|^2 + \gamma_w^{-1}))/(T-1)!$. Here, the lower incomplete Gamma function is given by $\gamma(x,a) = \int_0^a t^{x-1}e^{-t}dt$.

For a fading channel, the effects of channel must be considered, and Willie estimates the existence of communication using a threshold determined by channel state information (CSI), which is assumed to be perfectly known in advance. In this case, the optimal threshold corresponds to the value minimizing $P_{e,w}(\lambda)$ and is expressed as [8]

$$\lambda_{\mathrm{CSI}} = \frac{\gamma_w^{-1}\left(|h_w|^2 + \gamma_w^{-1}\right)}{|h_w|^2} \log\left(\frac{|h_w|^2 + \gamma_w^{-1}}{\gamma_w^{-1}}\right). \tag{3}$$

III. Benchmark Coherent Schemes

In this section, we introduce coherent Gaussian signaling schemes as benchmarks for our proposed system. Then, we analyze the effect of channel estimation errors on the achievable rate when using Gaussian-distributed pilot symbols.

A. Coherent Gaussian Signaling Schemes

Gaussian signaling (GS) is a modulation scheme that transmits data symbols following a Gaussian distribution. The first scheme, PSK-based GS (PSK-GS), is essentially equivalent to the one proposed in [7], and the second scheme, chaos-based GS (chaos-GS) [5], is superior in terms of performance when the transmission rate is equivalent to BPSK.

1) PSK-GS [7]: This scheme is a special case of the conventional differential scheme of [7], which relies on the property that the probability distribution does not change when a data symbol distributed on a unit circle is multiplied by a random variable following a specific distribution due to its circular symmetry. Let M denote the modulation order of PSK symbols and let $\mathcal{X} = \left\{e^{j\frac{m}{M}\pi} \mid m = 0, \cdots, M-1\right\}$ denote the constellation set. The kth modulated symbol is generated as $s_k = g \cdot e^{j\frac{m_k}{M}\pi}$, where g is the Gaussian RV based on a pre-shared seed. The Gaussian RV g can also be varied as g_k depending on the index k.

The fundamental limitation of PSK-GS is the need for Alice and Bob to have exactly the same seed value, which must be perfectly shared in advance. This pre-shared seed enables modulation and demodulation. If the seed value is even slightly incorrect, the performance will be significantly degraded.

2) Chaos-GS [5]: This scheme is based on chaos theory and efficiently generates symbols that follow a Gaussian distribution. Originally proposed as a secure modulation scheme, it is readily applicable to covert communication scenarios. As with PSK-GS, this scheme also requires the pre-sharing of a seed value, which enables coherent detection of the received symbols. The detailed construction process is also described in [9].[3]

In both cases, the transmit symbol vector is estimated by the maximum likelihood detector (MLD) $\hat{\mathbf{s}} = \arg\min_{\mathbf{s}\in\mathcal{S}}\|\mathbf{y}_b - \mathbf{s}\hat{h}_b\|^2$, where $\mathcal{S}$ denotes a GS codebook constructed with a seed shared without error for generating RVs.

B. Channel Estimation with Gaussian-Distributed Pilots

In typical communication systems, the transmission power allocated for pilot symbols is higher than the one for data symbols to enable accurate channel estimation. By contrast, in the context of covert communication with channel estimation, the DEP can be minimized when the transmission power is

[2] An exhaustive search-based strategy can be considered ideal, but we expect it decreases DEPs for coherent and noncoherent schemes almost equally.

[3] The open-source implementation of chaos-GS is available at https://github.com/ishikawalab/wiphy/blob/master/wiphy/examples/okamoto2012chaos.py

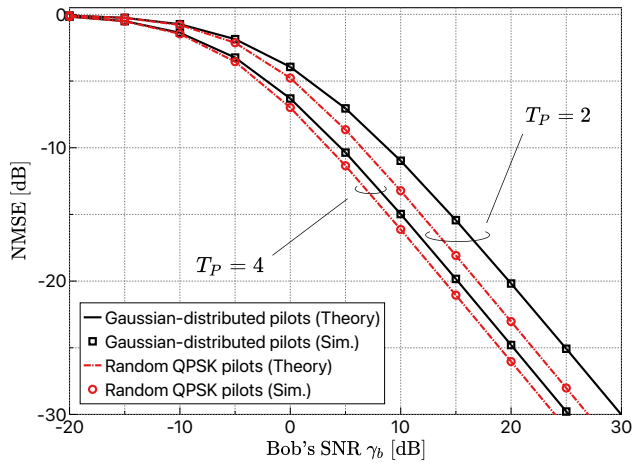


Fig. 2. Comparisons of channel estimation accuracy.

equally distributed between pilot and data symbols [10], which is the assumption followed in this letter as well.

The estimated channel considering estimation errors is $\hat{h} = \sqrt{1-\beta^2}h + \beta e$ [11], where $e \sim \mathcal{CN}(0,1)$ is an error and $\beta \in [0,1]$ is the uncertainty of estimation. The estimation error can be evaluated by the normalized minimum square error (NMSE) given by

$$\sigma_e^2 \triangleq \mathbb{E}\left[\left|\hat{h}-h\right|^2\right] \,/\, \mathbb{E}\left[|h|^2\right], \tag{4}$$

and that calculated by MMSE equalization with known pilot symbols is expressed as $\sigma_e^2 = 2\cdot(1-\sqrt{1-\beta^2}) = (1+\gamma_b\|\mathbf{p}\|^2)^{-1}$ [11].

We use Gaussian-distributed pilot symbols in this letter, as they can maintain the achievable rate of the coherent GS schemes while ensuring maximum covertness. Here, we assume that the generated pilot symbols vary with each instance $\mathcal{H}_1$ and behave as i.i.d Gaussian RVs. NMSE is calculated by the numerical integration of

$$\sigma_e^2 = \mathbb{E}_{\mathbf{p}}\left[\left(1+\gamma_b\|\mathbf{p}\|^2\right)^{-1}\right] \tag{5}$$

over the Erlang distribution

$$f\left(\|\mathbf{p}\|^2\right) = \frac{\|\mathbf{p}\|^{T_P-1}}{(T_P-1)!}\exp\left(-\|\mathbf{p}\|^2\right), \tag{6}$$

which has not been investigated in existing studies [7, 8], and is newly developed for evaluating the channel estimation error in the benchmark coherent schemes.

As an example, Fig. 2 shows a comparison of channel estimation errors induced by MMSE with Gaussian-distributed pilot symbols as well as the random QPSK symbols defined in 5G NR, where the simulation (4) and theoretical values (5) were considered. As shown in Fig. 2, the simulation and theoretical values matched perfectly, indicating that the theoretical analysis is correct. Also, the channel estimation accuracy improved as the number of Gaussian pilot symbols increased, although it was inferior to the reference QPSK case.

C. Achievable Rate Assuming Channel Estimation Errors

The ideal transmission rate per slot when transmitting B bits over T slots can be defined as $R \triangleq B/T$, and the achievable rate corresponding to a benchmark coherent scheme is given by [11]

$$R_e = R - \frac{1}{T|\mathcal{S}|}\mathbb{E}_{\hat{h},\mathbf{n}}\left[\sum_{i=1}^{|\mathcal{S}|}\log_2\left(\frac{\sum_{j=1}^{|\mathcal{S}|}p\left(\mathbf{y}_i \mid \hat{h},\mathbf{s}_j\right)}{p\left(\mathbf{y}_i \mid \hat{h},\mathbf{s}_i\right)}\right)\right], \tag{7}$$

where $\mathbf{y}_i = \mathbf{s}_i\hat{h} + \mathbf{n}$ is a received symbol vector given a codeword $\mathbf{s}_i \in \mathcal{S}$ and the likelihood ratio is expressed as $p(\mathbf{y}_i \mid \hat{h},\mathbf{s}_j)/p(\mathbf{y}_i \mid \hat{h},\mathbf{s}_i) = \exp[(-\|\mathbf{n}_{i,j}\|^2 + \|\mathbf{n}_{i,i}\|^2)/(\sigma_b^2+\sigma_e^2)]$ with $\mathbf{n}_{i,j} = \mathbf{y}_i - \mathbf{s}_j\hat{h}$.

IV. Proposed Noncoherent Covert Communication

In this section, we design GS using Grassmann codewords, which is referred to as *Grassmann-based GS (Grass-GS)*, for noncoherent covert communication. Then, we analyze the achievable rate when using the proposed Grass-GS.

A. Design of Grass-GS

Following the coherent system model of (1), the transmit symbol vector is denoted by $\mathbf{s} = [s_1 \ \cdots \ s_T]$, since Bob can decode information without channel estimation. That is, we set $T_P = 0$ and $T_D = T$ here to provide fair comparisons between both coherent and noncoherent schemes, as illustrated in Fig. 1. A well-known method constructs a Grassmann constellation using the matrix exponential map [12]. Another method constructs it to be uniformly distributed on the Grassmann manifold [13] based on numerical optimization [14], termed *original manopt constellation*.

In constructing the manopt constellation, if the starting point for optimization is set randomly and a simple gradient descent method is used, the phases of the optimized constellation generally follow a uniform distribution. Here, by imposing a constraint in the optimization process that all symbols have constant amplitude, it is possible to generate symbols that follow an arbitrary distribution in a manner similar to PSK-GS, at the expense of a reduced minimum distance of codewords.

Let $\mathcal{G}(T,1)$ denote the Grassmann manifold, representing the set of all 1-dimensional subspaces in $\mathbb{C}^T$, and let $\mathbf{c}_i \in \mathcal{C} \in \mathcal{G}(T,1)$ represent a Grassmann codeword chosen from the codebook $\mathcal{C}$ of size 2^B. In the design of Grass-GS, we use the minimum chordal distance (MCD), because it is a standard design metric and can be approximated by the log-sum-exp function. But, essentially, any design metric can be used. The design of the constant-amplitude Grassmann constellation can then be formulated as

$$\begin{aligned} \underset{\mathcal{C}}{\text{minimize}} \quad & \log \sum_{1\le i<j\le|\mathcal{C}|}\exp\left(\frac{|\mathbf{c}_i^{\mathrm{H}}\mathbf{c}_j|}{\epsilon}\right) \\ \text{s.t.} \quad & \mathbf{c}_i \in \mathcal{G}(T,1),\ \forall\, i=\{1,\cdots,|\mathcal{C}|\}, \\ & |c_{i,t}| = 1,\ \forall\, t=\{1,\cdots,T\}, \end{aligned} \tag{8}$$

where ϵ represents a smoothing constant and is set to $\epsilon = 10^{-2}$ in this letter.

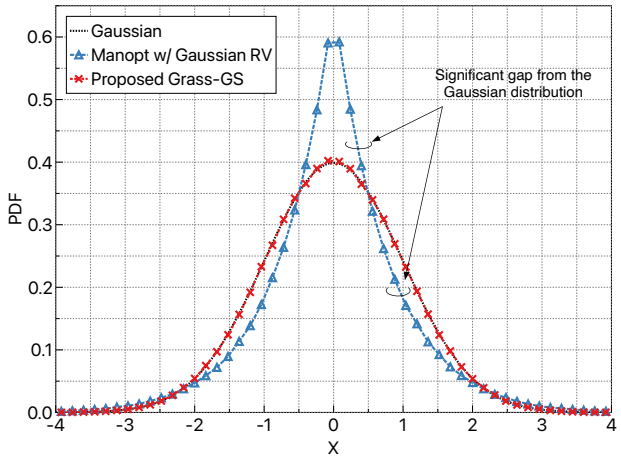


Fig. 3. PDF of the real or imaginary component of generated symbols.

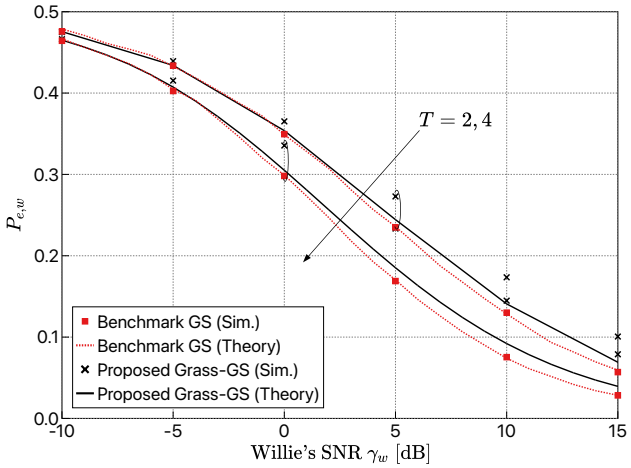


Fig. 4. Comparison of DEP at Willie that corresponds to the covertness.

The proposed Grass-GS codeword is generated by multiplying the codeword $\mathbf{c}_i \in \mathcal{C}$ by a Gaussian RV at Alice, i.e.,

$$\mathbf{s} = g \cdot \mathbf{c}_i. \tag{9}$$

At Bob, MLD is performed on the received symbols. Since g is unshared with Bob, its product with the channel coefficient h_b yields the equivalent channel which includes the effect of g, and the likelihood function of the received symbol given $\mathbf{c}_i$ is expressed as

$$p(\mathbf{y}_b \mid \mathbf{c}_i) = \frac{\exp\left(-\operatorname{tr}\left\{\mathbf{y}_b^{\mathrm{H}}\left(\mathbf{I}_T + \mathbf{c}_i\mathbf{c}_i^{\mathrm{H}}\right)^{-1}\mathbf{y}_b\right\}\right)}{\pi^T \det\left(\mathbf{I}_T + \mathbf{c}_i\mathbf{c}_i^{\mathrm{H}}\right)} \tag{10}$$

$$= \frac{\exp\left(-\|\mathbf{y}_b\|^2 + \frac{1}{1+\|\mathbf{c}_i\|^2}\left|\mathbf{y}_b^{\mathrm{H}}\mathbf{c}_i\right|^2\right)}{\pi^T\left(1+\|\mathbf{c}_i\|^2\right)}. \tag{11}$$

Thus, the received symbol is estimated as follows:

$$\hat{\mathbf{c}} = \arg\max_{\mathbf{c}\in\mathcal{C}} \left|\mathbf{y}_b^{\mathrm{H}}\mathbf{c}\right|^2, \tag{12}$$

where the RV g multiplied at Alice is no longer required. The benchmark schemes, PSK-GS and Chaos-GS, require the legitimate transceiver to share the random seed, while the proposed Grass-GS can avoid the sharing process that diminishes covertness. Note that all the considered schemes still require the pre-sharing of the codebook.

To evaluate Gaussianity, Fig. 3 shows the probability distribution function (PDF) of the real or imaginary component of the proposed Grass-GS, where the parameters were set to $T = 4$ and $B = 2$. Additionally, we also considered a naive noncoherent GS schemes which multiplies the original manopt constellation by a Gaussian RV. As shown in Fig. 3, the proposed Grass-GS exactly followed a Gaussian distribution, which was self-evident. Also, the naive noncoherent GS schemes, which did not impose the circular symmetry constraint, deviated significantly from the Gaussian distribution.

B. Detection Error Probability at Willie

Unlike the coherent scenario in Section II-B with the assumption of perfect CSI at Willie, in the noncoherent scenario, the existence of communication is estimated at Willie using channel distribution information (CDI) since he cannot access CSI due to the absence of pilots. In this case, the optimal threshold is obtained by employing the numerical search of

$$\lambda_{\mathrm{CDI}} = \arg\min_{\lambda^*} \mathbb{E}_{|h_w|^2}[P_{e,w}(\lambda^*)], \tag{13}$$

where the expectation is taken over the PDF of $|h_w|^2$.

C. Achievable Rate of Grass-GS

The achievable rate of Grass-GS is given by [11]

$$R_g = R - \frac{1}{T|\mathcal{C}|}\mathbb{E}_{h,g,\mathbf{n}}\left[\sum_{i=1}^{|\mathcal{C}|}\log_2\left(\frac{\sum_{j=1}^{|\mathcal{C}|} p(\mathbf{y}_i \mid \mathbf{c}_j)}{p(\mathbf{y}_i \mid \mathbf{c}_i)}\right)\right], \tag{14}$$

where $\mathbf{y}_i = \mathbf{c}_i \cdot g \cdot h + \mathbf{n}$ is the received symbol when $\mathbf{c}_i \in \mathcal{C}$ is transmitted and the likelihood ratio is

$$\frac{p(\mathbf{y}_i \mid \mathbf{c}_j)}{p(\mathbf{y}_i \mid \mathbf{c}_i)} = \exp\left(\frac{\left|\mathbf{y}_i^{\mathrm{H}}\mathbf{c}_j\right|^2 - \left|\mathbf{y}_i^{\mathrm{H}}\mathbf{c}_i\right|^2}{\sigma_b^2(T+\sigma_b^2)}\right). \tag{15}$$

Since we have $\mathbf{y}_i = \mathbf{c}_i \cdot g \cdot h + \mathbf{n}$, this expression is not strictly identical to the one given in [11]. Due to the constant-amplitude constraint, MCD decreases compared to the original manopt constellation, which is a disadvantage of the proposed approach.

V. Performance Comparisons

In this section, we evaluate the performance of the benchmark coherent schemes, PSK-GS [7] and Chaos-GS [5], and the proposed noncoherent scheme, Grass-GS, in terms of the DEP at Willie and the achievable rate at Bob.

A. Detection Error Probability

First, Fig. 4 shows DEP comparison upon increasing the received SNR at Willie, where the detections of the benchmark coherent and the proposed noncoherent GS were performed using the thresholds evaluated with (3) and (13), respectively. The number of time slots was $T = 2$ or 4 in both cases. For the benchmark coherent GS, pilot and data symbols

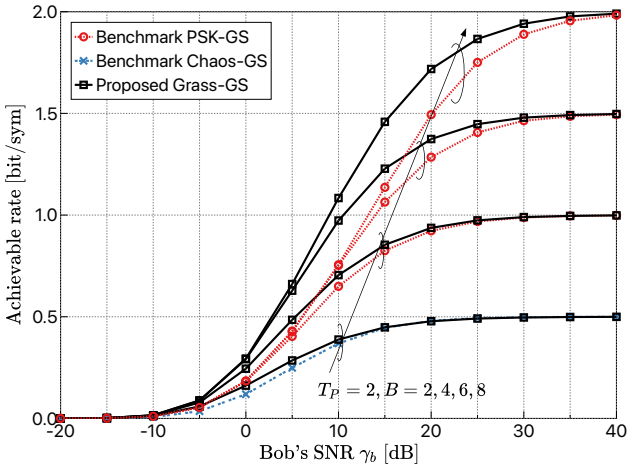


Fig. 5. Achievable rates of the benchmark and proposed GS schemes.

TABLE I
COMPLEXITY COMPARISONS.

	Number of RVs	Decoding complexity
Conv. PSK-GS [7]	$\mathcal{O}(T)$	$4 \cdot 2^{B/T} T = \mathcal{O}(2^{B/T} T)$
Conv. Chaos-GS [5]	$\mathcal{O}(2^B T)$	$4 \cdot 2^B T = \mathcal{O}(2^B T)$
Prop. Grass-GS	$\mathcal{O}(1)$	$4 \cdot 2^B T = \mathcal{O}(2^B T)$

were used for detection. As shown in Fig. 4, the proposed scheme outperformed the benchmarks in all SNR region, but it surpassed the theoretical curve as the SNR increased. This gap occurred due to the time correlation in the received symbols, implying that the proposed GS might be detected by evaluating the correlation. By contrast, the gap narrowed as the length T was decreased. Then, short data symbols are favorable for maintaining robustness against a correlation-based detection. Overall, the proposed noncoherent GS remains effective for the radio meter detection, particularly when compared with the coherent benchmarks.

B. Achievable Rate Comparisons

Next, Fig. 5 compares the achievable rates of the benchmark and the proposed GS. The lengths of data and pilot symbols were $T_D = T_P = 2$, resulting in the total length of $T = 4$. The number of the transmission bits was set to $B = 4$, 6 or 8 for PSK-GS and $B = 2$ for Chaos-GS. The channel estimation error in the benchmark schemes was evaluated with (5). Note that both schemes were fairly compared in terms of R. As shown in Fig. 5, the proposed Grass-GS exhibited similar performance to Chaos-GS at low rates and significantly outperformed PSK-GS at high rates, achieving its half-rate at an SNR up to 4.7 dB lower than the coherent benchmarks. This means that Grass-GS can accordingly reduce the transmit signal power, thereby offering a substantial advantage in enhancing covertness. Note that similar trends were observed for a smaller pilot ratio $T_P/T = 4/14 \approx 0.286$. Although bit error rate comparisons were omitted, Grass-GS achieved higher diversity orders than the coherent benchmarks.

C. Complexity Analysis

Finally, we compare the computational complexity required for the three considered schemes. Specifically, for T time slots, we derived the complexities for generating RVs and performing MLD, summarized in Table I. Evidently, the conventional coherent benchmarks require additional complexity for channel estimation, but since there are a number of methods available, it was omitted here. As given, the proposed Grass-GS requires the lowest number of RVs while maintaining the same decoding complexity as the benchmarks, making covert communications more practical.

VI. CONCLUSIONS

We have proposed a noncoherent covert communication scheme that employs constant-amplitude Grassmann constellation to generate GS. For fair comparisons, the benchmark coherent schemes have been introduced, and the achievable rate under channel estimation errors when using Gaussian-distributed pilot symbols has been evaluated. Our performance comparison demonstrated that the proposed Grass-GS achieved both higher covertness and achievable rates than the coherent benchmarks. Future work will focus on a MIMO system and its optimal detection at Willie.

REFERENCES

[1] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 2, pp. 1173–1198, 2023.

[2] Y. Jiang, L. Wang, H. Chen, and X. Shen, "Physical layer covert communication in B5G wireless networks—its research, applications, and challenges," *Proc. IEEE*, vol. 112, no. 1, pp. 47–82, 2024.

[3] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Select. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, 2013.

[4] S. Yan, Y. Cong, S. V. Hanly, and X. Zhou, "Gaussian signalling for covert communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3542–3553, 2019.

[5] E. Okamoto, "A chaos MIMO transmission scheme for channel coding and physical-layer security," *IEICE Trans. Commun.*, vol. E95.B, no. 4, pp. 1384–1392, 2012.

[6] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 19–25, 2019.

[7] Y. Katsuki, G. T. F. de Abreu, K. Ishibashi, and N. Ishikawa, "A new noncoherent gaussian signaling scheme for low probability of detection communications," *IEEE Wireless Commun. Lett.*, vol. 12, no. 3, pp. 545–549, 2023.

[8] K. Shahzad and X. Zhou, "Covert wireless communications under quasi-static fading with channel uncertainty," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1104–1116, 2021.

[9] N. Ishikawa, J. M. Hamamreh, E. Okamoto, C. Xu, and L. Xiao, "Artificially time-varying differential MIMO for achieving practical physical layer security," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2180–2194, 2021.

[10] T. Xu, L. Sun, S. Yan, J. Hu, and F. Shu, "Pilot-based channel estimation design in covert wireless communication," *arXiv:1908.00226*, 2019.

[11] N. Endo, H. Iimori, C. Pradhan, S. Malomsoky, and N. Ishikawa, "Boosting spectral efficiency with data-carrying reference signals on the Grassmann manifold," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 10 137–10 149, 2024.

[12] I. Kammoun, A. M. Cipriano, and J. C. Belfiore, "Non-coherent codes over the Grassmannian," *IEEE Trans. Wireless Commun.*, vol. 6, no. 10, pp. 3657–3667, 2007.

[13] K. H. Ngo, A. Decurninge, M. Guillaud, and S. Yang, "Cube-split: A structured Grassmannian constellation for non-coherent SIMO communications," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1948–1964, 2020.

[14] N. Boumal, B. Mishra, P. Absil, and R. Sepulchre, "Manopt, a matlab toolbox for optimization on manifolds," *J. Mach. Learn. Res.*, vol. 15, no. 42, pp. 1455–1459, 2014.