Spatial Constellation Design Based Generalized Space Shift Keying for Physical Layer Security of Multi-User MIMO Communication Systems

Nuğman Su, *Student Member, IEEE,* Erdal Panayirci, *Life Fellow, IEEE,* Mutlu Koca, *Senior Member, IEEE* and H. Vincent Poor, *Life Fellow, IEEE*

***Abstract*—We propose a novel spatial constellation design (SCD) method with generalized space shift keying (GSSK-SCD) signaling for physical layer security (PLS) in multi-user (MU) multiple-input multiple-output (MIMO) communication systems. In GSSK-SCD, the received spatial constellations are optimized through a novel precoding scheme, which minimizes the BERs at legitimate users and significantly worsens eavesdroppers' BER. In addition to extensive BER simulations, we also provide analytical expressions for the secrecy rate regions for the proposed GSSK-SCD. Both analytical derivations and simulation results, including comparisons with artificial noise aided conventional GSSK, reveal that the GSSK-SCD approach provides significant PLS improvements for MU-MIMO systems.**

***Index Terms*—Physical layer security (PLS), multi-user communication, generalized space shift keying (GSSK).**

I. Introduction

Wireless communication networks have been used for a large range of applications and services spanning business, government, military and personal interactions. However they are also open to a variety of malicious attacks, including eavesdropping, due to the broadcast nature of the networks. In this context, information security against these attacks can be enhanced on the physical link via physical layer security (PLS), by utilizing the channel characteristics of legitimate users and eavesdroppers (Eves), [1].

One of the fundamental tools for PLS provision is exploiting the randomness in wireless channels to deteriorate Eves' reception. In this regard, space shift keying (SSK) and generalized SSK (GSSK) have been among the effective modulation techniques for multiple-input multiple-output (MIMO) wireless systems with PLS benefits as reported in [2] and [3]. As shown in [4], it is possible to design secrecy capacity maximizing precoding systems for SSK for wireless multipath channels with an Eve even though this approach is computationally too complex to be applicable in practical communication systems. For this reason, other lower complexity transmission strategies exploiting the diversity provided by MIMO-GSSK to improve PLS have also been proposed. For instance, an optimal transmitter selection algorithm is proposed in [5] for a MIMO-GSSK broadcast system that enhances the achievable secrecy rate over a visible light communication channel. Another solution for PLS of MIMO-GSSK systems is proposed in [6], where the source transmits the confidential signal with a friendly jamming signal, which degrades the capacity of only Eve's channel, and thereby improving secrecy. Additionally, channel-inversion or zero-forcing (ZF) precoding is considered to be a practical transmission strategy to suppress the inter-user interference substantially and to improve the PLS of wireless communication systems as presented in [7].

The secrecy improvements in the aforementioned works are obtained in exchange for either *i)* increased computational complexity from extensive optimization, or *ii)* reduction in the available power for information-bearing signal transmission due to artificial noise addition. In this work, we propose a low-complexity spatial constellation design (SCD) technique combined with GSSK (GSSK-SCD) for multi-user (MU) MIMO communication systems, which does not rely on artificial noise but provides increased security. Prior to this work, the GSSK-SCD strategy has been shown to increase the secrecy capacity of visible light communication systems in [8], [9]. In the proposed GSSK-SCD, the legitimate users' CSI is exploited, which can be estimated at the receivers and fed back to the transmitter, as done similarly in e.g. [4], [7]. We do not utilize Eve's CSI, unlike some other works in the PLS literature, since its acquisition by the transmitter remains an open challenge as reported in [1]. The proposed GSSK-SCD improves the communication secrecy via *i)* random mapping between the transmitted symbols and activated antenna combinations, *ii)* emission power adjustment according to the legitimate users' CSI, and *iii)* optimized received spatial constellation for minimized bit error rates (BERs) at the legitimate users. Notice that antenna selection could be an alternative to GSSK, but the proposed technique is preferable for PLS for the two main reasons as follows: *i)* The random antenna and channel switching feature of GSSK makes it more difficult for the eavesdroppers to "guess" the intended user channels and therefore improves the PLS, *ii)* GSSK BER performance of the legitimate users can be shown to be generally superior to those obtained by the antenna selection methods. We show that through GSSK-SCD signaling, the BER performance of legitimate users is maximized, while Eve receives a jammed signal, reducing its BER performance significantly. The degradation in BER is shown to be effective even at high signal-to-noise ratios (SNRs). Furthermore, it is shown that the jamming is produced by only the GSSK-SCD signal modelling, and hence artifical noise transmission is not required.

This work has been supported by the Scientific and Technical Research Council of Turkey (TUBITAK) under the 1003-Priority Areas R&D Projects Support Program No. 218E034.

Nuğman Su, and Mutlu Koca are with the Wireless Communications Laboratory, Department of Electrical and Electronics Engineering, Boğaziçi University, 34342 Istanbul, Turkey (e-mail: {nugman.su; mutlu.koca}@boun.edu.tr).

Erdal Panayirci is with the Department of Electrical and Electronics Engineering, Kadir Has University, 34083 Istanbul, Turkey (e-mail: eepanay@khas.edu.tr).

H. Vincent Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2021.3079875, IEEE Wireless Communications Letters

II. System Description

We consider the PLS for a wireless communications system based on the MIMO-GSSK modulation technique, where only a certain number of antennas are activated for transmission at each symbol instant and the selected antenna indices implicitly convey information [10]. The absence of information symbol transmission in GSSK significantly simplifies the radio-frequency (RF) detection complexity compared to spatial modulation (SM) while achieving similar performance gains.

In the considered MU-MIMO-GSSK system, K users, each equipped with N_r receiving antennas, are connected to a single wireless communications attocell with N_t transmitting antennas, $(N_r < N_t)$. We employ GSSK, with $N_a > 1$ activated antennas per transmission, where there is a total of $\binom{N_t}{N_a}$ distinct antenna combinations. In contrast to generalized SM systems, where the antenna transmission amplitude is modulated with information, in the proposed regime only the indices of the selected antennas are used as spatial constellation points, and convey information to the receivers. However, the number of combinations that can be considered for activation must be a power of two. Therefore, only $M_a = 2^m$ combinations are randomly selected to activate antennas, where $m = \lfloor \log_2 \binom{N_t}{N_a} \rfloor$ and $\lfloor . \rfloor$ is the floor operation. Consequently, random and independent binary data bits $\mathbf{b}^{(u)} = (b_1^{(u)}, b_2^{(u)}, \cdots, b_{m^{(u)}}^{(u)})$ enter a GSSK mapper for each user $u \in \{1, 2, \cdots, K\}$, where $m^{(u)} = \log_2(M_a^{(u)})$ is the spectral efficiency of the user u in terms of bits per channel use (bpcu). The GSSK mapper concatenates the groups of $m^{(u)}$ bits from all users, then $m = \sum_{u=1}^{K} m^{(u)}$ bits are mapped to a constellation point vector $\mathbf{x} = [x_1, x_2, \cdots, x_{N_t}]^T$. Since N_a antennas are active, only N_a elements in $\mathbf{x}$ are nonzero. We denote the constellation point of the user u with $\xi^{(u)} = 1, 2, \cdots, M_a^{(u)}$, which corresponds to the $m^{(u)}$ bits generated by that user. The GSSK constellation point, which corresponds to the total m bits, is defined as $\xi = \xi^{(1)} \times \xi^{(2)} \times \cdots \times \xi^{(K)} = \left(q^{(1)}, q^{(2)}, \cdots, q^{(K)}\right)$, where $q^{(u)} \in \{1, 2, \cdots, M_a^{(u)}\}$ and $\xi = 1, 2, \cdots, M_a$. Now we define

$$\mathbf{x}_{I_\xi} = \begin{bmatrix} 0 & \underset{\uparrow}{P_1} & \cdots & 0 & \cdots & \underset{\uparrow}{P_2} & \cdots & 0 & \cdots & \underset{\uparrow}{P_{N_a}} & \cdots \\ & x_{i_1} & & & & x_{i_2} & & & & x_{i_{N_a}} & \end{bmatrix}^T, \tag{1}$$

where $I_\xi = (i_1, i_2, \cdots, i_{N_a})$ stores the selected antenna indices for the GSSK constellation point ξ, and $\mathbf{x}_{I_\xi}$ is the GSSK transmit vector for ξ. Also, $\mathbf{P} = [P_1, P_2, \cdots, P_{N_a}]^T$ represents the radiation amplitudes of the selected antennas. The elements in $\mathbf{P}$ are found via precoding by exploiting the legitimate users' CSI at the transmitter as described in the next section. The pre-processed weight vector $\mathbf{P}$ is then transmitted by $\mathbf{x}_{I_\xi}$ over the user's respective channels $\mathbf{H}^{(u)} = [\mathbf{h}_1^{(u)}, \mathbf{h}_2^{(u)}, \ldots, \mathbf{h}_{N_t}^{(u)}] \in \mathbb{C}^{N_r \times N_t}$ where, $\mathbf{h}_k^{(u)} = [h_{1,k}^{(u)}, h_{2,k}^{(u)}, \ldots, h_{N_r,k}^{(u)}]^T$. The Rayleigh fading coefficients of each user's channel, $h_{n,k}^{(u)}$, are assumed to be complex Gaussian random variable with zero mean and unit variance. An N_r-dimensional additive, complex-valued white Gaussian noise (AWGN) vector, $\mathbf{w}^{(u)}$, with double sided power spectral density σ^2 is added to the received signal. Hence, the received signal by the uth user is given by

$$\mathbf{y}^{(u)} = \mathbf{H}^{(u)}\mathbf{x}_{I_\xi} + \mathbf{w}^{(u)} = \beta \mathbf{h}_{I_\xi,\text{eff}}^{(u)} + \mathbf{w}^{(u)} \tag{2}$$

where $\mathbf{h}_{I_\xi,\text{eff}}^{(u)} = \sum_{k=1}^{N_a} \mathbf{h}_{i_k}^{(u)} P_k$. Note that $\mathbf{h}_{I_\xi,\text{eff}}^{(u)}$ is called an "effective column vector" for $\xi^{(u)}$, representing the weighted-sum of the N_a distinct columns of $\mathbf{H}^{(u)}$ and β is a normalizing constant to be estimated. At each user's side, detection of antenna indices is done by the optimal maximum likelihood (ML) rule given as

$$\begin{aligned} I_{\hat{\xi}}^{(u)} &= \arg\max_{\xi} p(\mathbf{y}^{(u)} | \mathbf{x}_{I_\xi}, \mathbf{H}^{(u)}) \\ &= \arg\min_{\xi} \parallel \mathbf{y}^{(u)} - \beta \mathbf{H}_{I_\xi}^{(u)} \mathbf{P} \parallel_F^2 \end{aligned} \tag{3}$$

where $I_{\hat{\xi}}^{(u)} = (\hat{i}_1, \hat{i}_2, \ldots, \hat{i}_{N_a})$ denotes the estimated antenna indices and $\mathbf{H}_{I_\xi}^{(u)}$ is obtained from $\mathbf{H}^{(u)}$ as

$$\mathbf{H}_{I_\xi}^{(u)} = \begin{bmatrix} h_{1,i_1}^{(u)} & h_{1,i_2}^{(u)} & \cdots & h_{1,i_{N_a}}^{(u)} \\ h_{2,i_1}^{(u)} & h_{2,i_2}^{(u)} & \cdots & h_{2,i_{N_a}}^{(u)} \\ \vdots & \ddots & \ddots & \\ h_{N_r,i_1}^{(u)} & h_{N_r,i_2}^{(u)} & \cdots & h_{N_r,i_{N_a}}^{(u)} \end{bmatrix} \in \mathcal{C}^{N_r \times N_a}. \tag{4}$$

The main problem with the detection rule in (3) is that the information detected by each user contains its own message along with those of other users. This would endanger the confidentiality of the information sent by the source to each user and make it difficult to establish secure transmission in the physical layer. Hence, we propose a novel precoding scheme for downlink MU-GSSK systems with two main advantages: (i) The precoder is capable of eliminating the MU interference completely so that the users can only receive their respective information sent by the source. (ii) The precoder is designed in such a way that effective channel vectors at the receiver are contained in a square QAM constellation in N_r-dim Euclidean space resulting in an improved BER performance while degrading Eve's BER performance profoundly.

III. SCD-based PLS Improvement Technique

In this section, we describe the proposed GSSK-SCD technique. We refer to the source and the multiple legitimate users, as 'Alice' and 'Bobs', respectively. The data sent by Alice is received by Bobs and Eve via their respective channels. In the proposed technique, a suitable precoder is designed without Eve's CSI, which is different from most of the PLS methods in the literature. Our precoder design forces the effective channel column vectors received by Bobs to be equally-spaced in N_r dimensions. Consequently, it is ensured that Bobs receive the transmitted information with very high BER performance while Eve does not receive any reliable information at all. The precoder is presented in the following subsection.

1) Precoder Design: The proposed precoder shapes original channel's effective column vectors of all users, $\mathbf{H}_{\text{eff}}^{(u)} = [\mathbf{h}_{1,\text{eff}}^{(u)}, \ldots, \mathbf{h}_{M_a^{(u)},\text{eff}}^{(u)}] \in \mathcal{R}^{N_r \times M_a^{(u)}}$, scattered in N_r-dim Euclidean space so that they are maximally separated from each other. They are chosen from the set of vectors $\mathcal{V}_{M^{(u)}-\text{GQAM}}^{(u)} = \{\mathbf{v}_1^{(u)}, \mathbf{v}_2^{(u)}, \ldots, \mathbf{v}_{M^{(u)}}^{(u)}\}$, in an N_r-dim Euclidean space, forming a $M^{(u)}$-ary generalized quadrature-amplitude modulated ($M^{(u)}$-GQAM) signal constellation $(M^{(u)} \geq M_a^{(u)})$, where

$$\mathbf{v}_k^{(u)} = [v_k^{(u)}(1), v_k^{(u)}(2), \ldots, v_k^{(u)}(N_r)]^T \in \mathcal{R}^{N_r}, \tag{5a}$$

$$v_k^{(u)}(\ell) \in \{\pm A, \pm 3A, \ldots, \pm(L^{(u)} - 1)A\} \tag{5b}$$

for $k = 1, 2, \ldots, M^{(u)}$, and $u = 1, 2, \ldots, K$. Here, $L^{(u)} = \left(M^{(u)}\right)^{1/N_r}$ for $L^{(u)} = 2, 4, 6, \ldots$.

It can be shown that, for a given $M_a^{(u)}$ and N_r, the size of the GQAM constellation, $M^{(u)}$, can be determined as follows.

$$M^{(u)} = \begin{cases} M_a^{(u)}; & \text{if } N_r = 1 \\ \left(2\left\lceil \frac{1}{2}\left(M_a^{(u)}\right)^{1/N_r}\right\rceil\right)^{N_r}; & \text{if } N_r > 1 \end{cases} \tag{6}$$

where $\lceil\cdot\rceil$ denotes ceiling operation. $A > 0$ is a real normalizing constant, whose value is determined by equating the average power of the signal constellation $\mathcal{V}_{M^{(u)}-\text{GQAM}}$ to that of the original effective channel vectors, that is

$$P_{av}(\mathbf{v}) = \mathbb{E}(\mathbf{v}^{(u)\dagger}\mathbf{v}^{(u)}) = P_{av}(\mathbf{h}_{I,\text{eff}}^{(u)}) \equiv 1, \tag{7}$$

where $(\cdot)^\dagger$ denotes the Hermitian operation. The sequence of information bits transmitted to the respective users is mapped to the GSSK transmit vector $\mathbf{x}$, which specifies the activated antennas. Each combination $I \Leftrightarrow \{i_1, i_2, \cdots, i_{N_a}\}$ has the form given in (1). The received signal vector at the user u is required to be proportional to $\beta\mathbf{v}_k^{(u)}$ so that multiuser interference (MUI) is suppressed. To satisfy this condition, we design a precoder at the transmit unit with inputs $\mathbf{H}_{I_{\xi^{(u)}}}^{(u)} \in \mathcal{C}^{N_r \times N_a}$, $\xi^{(u)} = 1, 2, \cdots, M_a^{(u)}$ and $\mathbf{P}$. Consequently, the optimal precoding vector, $\mathbf{P}_{\text{opt}}$ is determined to ensure that each user u receives an energy leak-free signal as follows:

$$\mathbf{H}_{I_{\xi^{(u)}}}^{(u)}\mathbf{P}_{\text{opt}} = \mathbf{v}_{\xi^{(u)}}^{(u)}, \quad u = 1, 2, \cdots, K. \tag{8}$$

Combining the outcomes for all users, the relationship in (8) can be written as

$$\mathbf{H}_{I_\xi}\mathbf{P}_{\text{opt}} = \mathbf{v}_{I_\xi}, \tag{9}$$

where $\mathbf{H}_{I_\xi} = [\mathbf{H}_{I_{\xi^{(1)}}}^{(1)T}, \mathbf{H}_{I_{\xi^{(2)}}}^{(2)T}, \cdots, \mathbf{H}_{I_{\xi^{(K)}}}^{(K)T}]^T \in \mathcal{C}^{KN_r \times N_a}$, $\mathbf{v}_{I_\xi} = [\mathbf{v}_{\xi^{(1)}}^{(1)T}, \mathbf{v}_{\xi^{(2)}}^{(2)T}, \cdots, \mathbf{v}_{\xi^{(K)}}^{(K)T}]^T \in \mathcal{C}^{KN_r}$. Given that the matrix $\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi}$ is nonsingular, the optimal precoding vector can be found with the generalized inverse of $\mathbf{H}_{I_\xi}$, as

$$\mathbf{P}_{\text{opt}} = \left(\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi}\right)^{-1}\mathbf{H}_{I_\xi}^\dagger\mathbf{v}_{I_\xi}, \tag{10}$$

which satisfies (9), if $\mathbf{U} \triangleq \mathbf{H}_{I_\xi}\left(\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi}\right)^{-1}\mathbf{H}_{I_\xi}^\dagger = \mathbf{I}_{KN_r}$ holds, where $\mathbf{I}_{KN_r} \in \mathcal{C}^{KN_r \times KNr}$ is a unit matrix. Because $\mathbf{H}_{I_\xi}$ in (9) has more columns than rows ($N_a \geq KN_r$), the matrix $\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi}$ in (10) is positive semi-definite and therefore (9) may not have a unique solution. Hence, we apply linear processing exploiting regularization as in [11] to all $\mathbf{v}_{I_\xi}$ vectors. Consequently, the optimal precoding vector becomes

$$\mathbf{P}_{\text{opt}} = \left(\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi} + \epsilon\mathbf{I}_{N_a}\right)^{-1}\mathbf{H}_{I_\xi}^\dagger\mathbf{v}_{I_\xi}, \tag{11}$$

where the regularization parameter, $0 < \epsilon < \lambda_{\min}$ makes $\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi}$ positive definite. Here, $\lambda_{\min}$ is the smallest nonzero eigenvalue of the matrix $\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi}$.

2) Transmit Power Normalization: The signal components of $\mathbf{P}_{\text{opt}}$ arriving at each transmit antenna have substantial power fluctuations in a wide dynamic range. To prevent these, the output power after precoding is normalized by the power-normalization factor β given by $\beta = N_r/\text{Tr}\left\{\left(\mathbf{H}_{I_\xi}\mathbf{H}_{I_\xi}^\dagger\right)^{-1}\right\}$, [11], where $\text{Tr}\{(\cdot)\}$ is the trace operation. An average power constraint can also be employed as done in [12], such that $\beta = N_r\mathbb{E}\left[1/\text{Tr}\left\{\left(\mathbf{H}_{I_\xi}\mathbf{H}_{I_\xi}^\dagger\right)^{-1}\right\}\right]$ which makes β become a constant, depending only on the channel statistics. It can then be computed at the transmitter and passed on to the users.

3) MU Receiver with an Eavesdropper: The legitimate users receive the broadcast as

$$\mathbf{y} = \beta\mathbf{H}_{I_\xi}\mathbf{P}_{\text{opt}} + \mathbf{w} = \beta\mathbf{v}_{I_\xi} + \mathbf{w}, \tag{12}$$

where $\mathbf{y} = [\mathbf{y}^{(1),T}, \mathbf{y}^{(2),T}, \cdots, \mathbf{y}^{(K),T}]^T$. With the proposed GSSK-SCD technique, the received signals at the legitimate users are shaped according to (8) and (9). Hence, the received signal at the uth legitimate user is obtained with zero MUI as

$$\mathbf{y}^{(u)} = \beta\mathbf{H}_{I_\xi}^{(u)}\left(\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi} + \epsilon\mathbf{I}_{N_a}\right)^{-1}\mathbf{H}_{I_\xi}^\dagger\mathbf{v}_{I_\xi} + \mathbf{w}^{(u)} \tag{13a}$$

$$= \mathbf{s}^{(u)} + \mathbf{w}^{(u)}, \quad u = 1, 2, \ldots, K. \tag{13b}$$

where $\mathbf{s}^{(u)} \triangleq \beta\mathbf{v}_{I_\xi}^{(u)}$ is the observed transmitted signal by the uth user. Eve receives the broadcast as

$$\mathbf{y}^{(E)} = \mathbf{s}^{(E)} + \mathbf{w}^{(E)}, \tag{14}$$

where $\mathbf{s}^{(E)} \triangleq \beta\mathbf{H}_{I_\xi}^{(E)}\left(\mathbf{H}_{I_\xi}^\dagger\mathbf{H}_{I_\xi} + \epsilon\mathbf{I}_{N_a}\right)^{-1}\mathbf{H}_{I_\xi}^\dagger\mathbf{v}_{I_\xi}$ is Eve's received signal. (14) indicates that GSSK-SCD introduces a *friendly* jamming signal for Eve, mainly due to the random switching phenomenon in GSSK. Hence, $\mathbf{v}^{(u)}$ for any u, cannot be perfectly recovered by Eve. The jamming signal, $\mathbf{J}^{(u)}$ observed in GSSK-SCD when Eve wiretaps the uth user, can be expressed by rewriting Eve's signal in (14) as

$$\mathbf{y}^{(u,E)} = \mathbf{s}^{(u)} + \mathbf{J}^{(u)} + \mathbf{w}^{(E)}, \tag{15}$$

where $\mathbf{J}^{(u)}$ is the jamming signal at Eve, wiretapping the uth user, which is expressed as

$$\mathbf{J}^{(u)} = \beta\left(\mathbf{H}_I^{(E)} - \mathbf{H}_I^{(u)}\right)\mathbf{P}_{\text{opt}}. \tag{16}$$

Note that the term $\mathbf{J}^{(u)}$ in (16) represents an effective jamming signal generated purely by channel differences between the legitimate users and Eve, as opposed to being generated separately by the multiple transmitting antennas. It is approximately an AWGN vector with zero mean and covariance $\mathbb{C}_{\mathbf{J}^{(u)}}$. As will shortly be seen from the computer simulations, the jamming signal $\mathbf{J}^{(u)}$ is very effective in increasing the interference experienced by Eve and degrades her BER substantially. From (15), we define $\mathbf{n} \triangleq \mathbf{J}^{(u)} + \mathbf{w}^{E}$, which is a colored zero-mean Gaussian vector with the covariance matrix

$$\mathbb{C}_{\mathbf{n}} = \mathbb{E}\{\mathbf{n}\mathbf{n}^\dagger\} = \mathbb{C}_{\mathbf{J}^{(u)}} + \sigma_E^2\mathbb{I}_{N_r}. \tag{17}$$

The receivers extract the spatial information, I, from the observed signals at (13) and (14) by the ML criterion as

$$\widehat{I}_{\hat{\xi}}^{(u)} = \arg\max_{\xi}\left\{\parallel \mathbf{y}^{(u)} - \mathbf{s}^{(u)} \parallel^2\right\}, \tag{18a}$$

$$\widehat{I}_{\hat{\xi}}^{(E)} = \arg\max_{\xi}\left\{\parallel \mathbf{y}^{(E)} - \mathbf{s}^{(u)} \parallel^2\right\}. \tag{18b}$$

Notice that the transmitter has to compute $\mathbf{P}_{\text{opt}}$ as given in (10), so that secure GSSK-SCD signals are realized at each legitimate user. Therefore, there is a computational cost at the transmitter. On the other hand, the computational complexity at the receivers is small since they do not need to perform any post-processing for PLS, and can extract secure information with simple maximum likelihood detection.

4) Achievable Secrecy Sum Rates: We now consider the secrecy rates for the proposed system in the presence of a single Eve that can easily be extended to the multiple Eve case. In the proposed technique, the interference among users is cancelled completely as given in (13). For the proposed system, the achievable secrecy sum-rate R_s is found as the sum of the achievable secrecy rates of all users, $R_s^{(u)}$, in the presence of one Eve:

$$R_s = \sum_{u=1}^{K} R_s^{(u)}, \tag{19}$$

Assuming that the messages transmitted to each user u belong to the standard Gaussian distribution, $R_s^{(u)}$ can be written as

$$R_s^{(u)} = \left[\log_2(1+\text{SNR}^{(u)}) - \log_2(1+\text{SNR}^{(E)}) \right]^+ \tag{20}$$

where $[a]^+ = a$, if $a \geq 0$, $[a]^+ = 0$, if $a < 0$. Exact closed-form expressions for mutual information and achievable secrecy rates for GSSK cannot be obtained analytically, since the message input distribution $P(\mathbf{x}_{I_\xi}) = 1/N_t$ does not maximize the secrecy capacity of the MU-GSSK system with one Eve. However, in [13], secrecy rates were computed through numerical evaluations for SSK. Similarly, a lower bound for the secrecy sum-rate achievable by the proposed system can be obtained from (18), (19) and (20) as

$$R_s \geq \sum_{u=1}^{K} \left[\log_2\left(1+\log_2\left(\frac{\beta^2}{N_r\sigma_w^2}\right)\right) - \log_2\left(1+\log_2\left(\frac{\beta^2}{\text{Tr}(\mathbb{C}_{\mathbf{J}^{(u)}}+\sigma_w^2\mathbf{I})N_r}\right)\right)\right]^+. \tag{21}$$

IV. Simulation Results

In this section, we present the security performance of the proposed GSSK-SCD system in terms of BER and achievable secrecy regions. The channel gains of all users and Eve are drawn independently from the standard complex Gaussian distribution. We assume that only legitimate user CSI is available at the access point and each user is aware of only own CSI. For benchmark comparisons, both conventional GSSK and GSSK with artificial noise have been considered. Consider the conventional GSSK signal model

$$\mathbf{y}^{(u)} = \mathbf{H}^{(u)}\mathbf{x}_{\text{GSSK}} + \mathbf{w}^{(u)}, \tag{22}$$

where $\mathbf{x}_{\text{GSSK}}$ is the GSSK transmit vector. The signal model in (22) is not useful for PLS purposes, since any third party can decode $\mathbf{x}_{\text{GSSK}}$ by a simple zero-forcing equalizer. In order to increase the resilience against Eves, a popular approach is to transmit an *artificial noise*, $\mathbf{n}_{\text{art}}$, which is superposed on the transmitted information signal, such that

$$\mathbf{y}^{(u)} = \mathbf{H}^{(u)}\left(\mathbf{x}_{\text{GSSK}} + \sqrt{\rho\beta}\mathbf{n}_{\text{art}}\right) + \mathbf{w}^{(u)}, \tag{23}$$

where $\mathbf{n}_{\text{art}}$ has unit energy, and $0 \leq \rho \leq 1$ is the power ratio of the artificial noise and $\mathbf{x}_{\text{GSSK}}$. The artificial noise vector must be selected from the nullspace of $\mathbf{H} = [\mathbf{H}^{(1)T}, \mathbf{H}^{(2)T}, \cdots, \mathbf{H}^{(K)T}]^T \in \mathcal{C}^{KN_r \times N_t}$, so that none of the legitimate users are affected. Then, Eve's signal becomes

$$\mathbf{y}^{(E)} = \mathbf{H}^{(E)}\mathbf{x}_{\text{GSSK}} + \tilde{\mathbf{n}} + \mathbf{w}^{(E)}, \tag{24}$$

where $\tilde{\mathbf{n}} = \mathbf{H}^{(E)}\sqrt{\rho\beta}\mathbf{n}_{\text{art}}$. Here, the signal received by legitimate users is still given by (22).

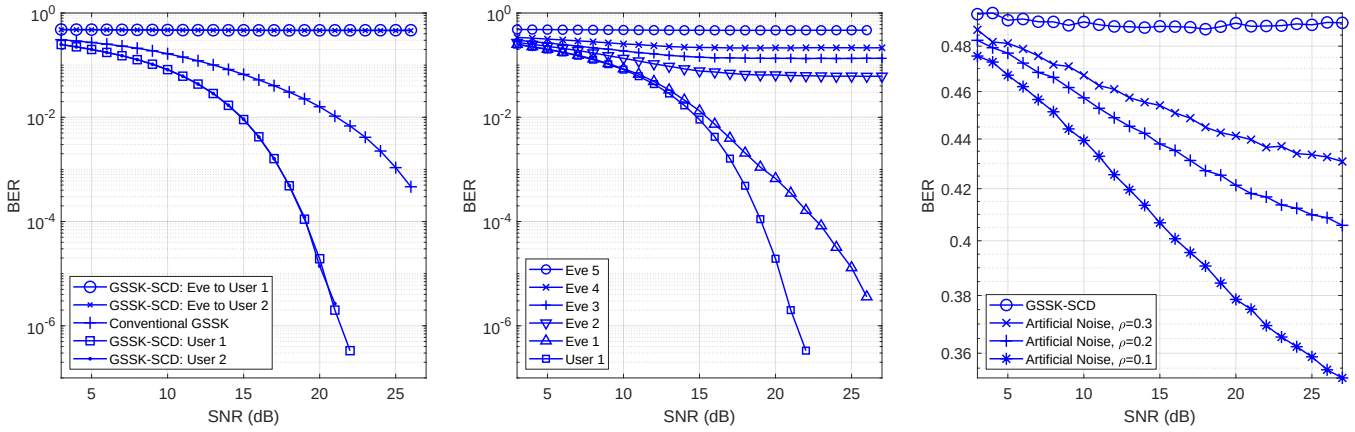
For BER performance evaluations, we have assumed that there are $K = 2$ legitimate users and one Eve; and $N_t = 8$, $N_r = 2$ and $N_a = 4$. In this case, $m = \lfloor \log_2 \binom{N_t}{N_a} \rfloor = 6$ bpcu are transmitted, and $M^{(1)} = M^{(2)} = 2^{m/2} = 8$ since m is divided evenly among the legitimate users. Since $N_r = 2$ and $M = 8$, $\mathcal{V}^{(1)}$ and $\mathcal{V}^{(2)}$ are optimally chosen to be $8-$QAM symbol constellations. The BER performance results for this system are presented comparatively in Fig. 1a. These results indicate that GSSK-SCD provides minimized BERs to both legitimate users, due to the optimal precoding in (10). GSSK-SCD outperforms the conventional GSSK in terms of the legitimate user BERs whereas Eve's BER is degraded significantly to the 0.5-level.

Next in Fig. 1b, we apply GSSK-SCD on the considered system in Fig. 1a, but the number of Eves are increased to 5. Here, the channel coefficients of Eve i ($i = 1, \ldots, 4$) are chosen as functions of the CSI of User 1, as $\mathbf{H}^{(E_i)} = \mathbf{H}^{(1)} + \kappa_i\mathbf{I}$, with $\kappa_i = \{0.1, 0.5, 1, 2\}$. The channel of Eve 5 is independent of other parties. According to the results in Fig. 1b, Eve's BER improves as its channel coefficients resemble more the legitimate user's CSI. This makes sense, since the energy of the GSSK-SCD jamming signal is small if the channel resemblance of Eve and the User is high, which is deduced from (16). Still, for larger κ values, Eve's communication is corrupted with large BERs. Thus, GSSK-SCD results in degraded BER performance at Eve for $\kappa > 0.5$. The results in Fig. 1a and 1b suggest that the proposed GSSK-SCD system provides secure communication, unless Eves' channel is almost identical to that of any legitimate user's.

In Fig. 1c, the proposed GSSK-SCD is compared with the GSSK system with artificial noise, in terms of Eve's BER performance. In this case, $N_t = 12$ and $N_a = 6$ are assumed, so $N_a > KN_r$ holds and (23) can be applied since the nullity of $\mathbf{H}_{I_\xi}$ is positive. The system is simulated for the artificial noise power ratios of $\rho = \{0.1, 0.2, 0.3\}$. The results indicate that the conventional GSSK system with artificial noise results in degraded BER performance at Eve, for all considered ρ values. However, the proposed system ensures Eve to operate close to the 0.5 BER level, which is still larger than the benchmark strategy. Notice that the benchmark strategy dissipates a significant amount of power for artificial noise transmission. On the other hand, this is not needed in GSSK-SCD as it provides friendly jamming by the optimal spatial constellation design and uses all available power for only information broadcast. Therefore, the GSSK-SCD system is a low-cost PLS strategy, offering reduced interceptibility of the transmitted information.

Finally, we present the secrecy rate regions of 2 users employing GSSK-SCD for different SNR levels in Fig. 2. These curves are obtained for $N_t = 8$, $N_a = 4$ and $m^{(1)} = m^{(2)} = 3$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2021.3079875, IEEE Wireless Communications Letters



(a) (b) (c)

Fig. 1: BER performance curves obtained by GSSK-SCD of a) 2 legitimate users and Eve, b) multiple Eves. c) BER performance comparison of GSSK-SCD and GSSK with artificial noise.

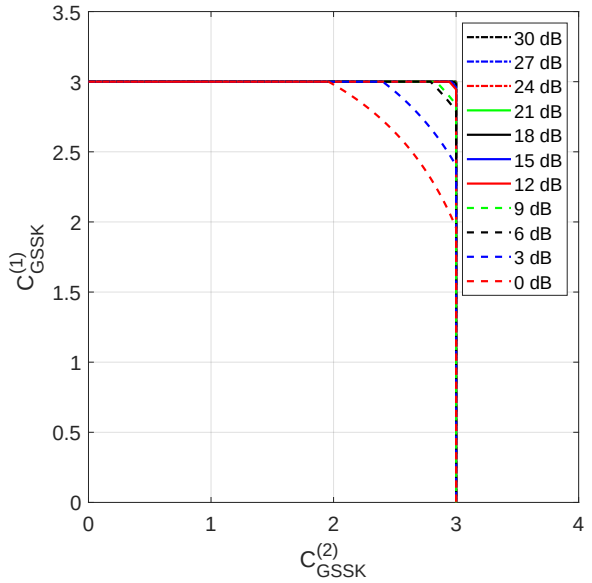


Fig. 2: Secrecy rate regions of the $2-$user GSSK-SCD.

bpcu which is the maximum achievable secrecy rate per user. It can be seen that at low SNR levels (0-12 dB), both users cannot be provided with the maximum achievable secrecy at the same time. For instance, at 0 dB SNR, if one user's secrecy rate is more than 2 bpcu, then the other user's secrecy rate cannot be maximized. On the other hand, GSSK-SCD ensures a secrecy rate of 2.5 bpcu to both users at 0 dB SNR. As expected the secrecy rates provided to both users increases with SNR and for the SNR > 12 dB, both users are provided with maximum achievable secrecy rate.

V. Conclusion

In this work, we have presented GSSK-SCD, a novel SCD strategy based on GSSK, for PLS improvements in MU-MIMO communication systems with one or more Eves. In the proposed strategy, the GSSK signal is optimally reshaped with legitimate users' CSI to minimize their BERs. GSSK-SCD signaling simultaneously produces jamming in Eve's received signal, causing significant degradation in Eve's BER performance. The performance is evaluated for the $2-$user setting via Monte Carlo simulations which indicate significant improvements compared to conventional GSSK and artificial noise aided GSSK strategies. The provided secrecy is quantified with analytical expressions for both users, through which we conclude that both users can be provided with maximum achievable secrecy rate for SNR levels greater than 12 dB.

References

[1] Y. Zou et al., "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] M. Wen, B. Zheng, K. J. Kim, M. Di Renzo, T. A. Tsiftsis, K. Chen, and N. Al-Dhahir, "A survey on spatial modulation in emerging wireless systems: Research progresses and applications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 9, pp. 1949–1972, 2019.

[3] Y. Wei et al., "Analysis of secrecy rate against eavesdroppers in MIMO modulation systems," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2015, pp. 1–5.

[4] S. R. Aghdam and T. M. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 180–183, 2016.

[5] F. Wang et al., "Secrecy analysis of generalized space-shift keying aided visible light communication," *IEEE Access*, vol. 6, pp. 18310–24, 2018.

[6] F. Wang et al., "Optical jamming enhances the secrecy performance of the generalized space-shift-keying-aided visible-light downlink," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4087–4102, 2018.

[7] F. Wu et al., "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, 2016.

[8] E. Panayirci et al., "Physical-layer security with optical generalized space shift keying," *IEEE Trans. Commun.*, pp. 1–1, 2020.

[9] A. Yesilkaya et al., "Physical-layer security in visible light communications," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[10] P. Lv, W. Yu, and N. Chen, "GSSK: A generalization step safe algorithm in anonymizing data," in *Proc. Int. Conf. Commun. Mobile Comput.*, 2010, vol. 1, pp. 183–187.

[11] C. B. Peel et al., "A vector-perturbation technique for near-capacity multiantenna multiuser communication-part I: Channel inversion and regularization," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, 2005.

[12] A. Dytso et al., "Upper and lower bounds on the capacity of amplitude-constrained MIMO channels," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2017, pp. 1–6.

[13] G. Geraci et al., "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, 2012.