Physical-Layer Security With Optical Generalized Space Shift Keying

Erdal Panayirci, *Life Fellow, IEEE*, Anil Yesilkaya, *Student Member, IEEE*, Tezcan Cogalan, *Member, IEEE*, H. Vincent Poor, *Life Fellow, IEEE*, and Harald Haas, *Fellow, IEEE*

***Abstract*— Spatial modulation (SM) is a promising technique that reduces inter-channel interference while providing high power efficiency and detection simplicity. In order to ensure the secrecy of SM, precoding and friendly jamming are widely adopted in the literature. However, neither of those methods can take advantage of SM. In this paper, a novel spatial constellation design (SCD) technique is proposed to enhance the physical layer security (PLS) of optical generalized space shift keying (GSSK), which can retain some benefits of SM. Due to the lack of small-scale fading, the quasi-static characteristics of the optical channel is used to tailor the received signal at the legitimate user's (Bob's) side. The PLS of the system is guaranteed by the appropriate selection of the power allocation coefficients for randomly activated light emitting diodes (LEDs). With the aid of Bob's channel state information at the transmitter, the bit error ratio (BER) of Bob is minimized while the BER performance of the potential eavesdroppers (Eves) is significantly degraded. Monte-Carlo simulation results show that the proposed SCD-zero forcing precoding (ZFP) forces Eve to experience a BER of around 0.5 by outperforming both the conventional and ZFP based GSSK for all practical signal-to-noise-ratio regimes and Bob-Eve separations.**

***Index Terms*— PHY layer security, optical wireless communications (OWC), generalized space shift keying (GSSK), multiple-input multiple-output (MIMO) channels, secrecy capacity.**

I. Introduction

THE increasing capabilities of mobile devices and the growing user demand on data-driven applications such as the internet-of-things (IoT), device-to-device (D2D) and machine type communications (MTC) are constantly pushing the wireless networks to provide higher data rates. Future generation communication systems will aim to provide connectivity anywhere and at anytime, for anyone and anything. Therefore, the security of wireless networks is now as important as the high transmission rate. In order to achieve higher data rates along with enhanced security merits, wireless communication systems rely on: (i) using higher portions of the electromagnetic (EM) spectrum (i.e. mm-wave and optical bands) for transmission; and (ii) the utilization of multiple transmit and receive elements, which is referred to as multiple-input-multiple-output (MIMO).

The higher portion of the spectrum provides larger communication bandwidths, which in turn enables the dense deployment of small cells to achieve very high area spectral efficiencies [1]. Specifically, light-fidelity (LiFi) is a promising technology that utilizes the visible light and infra-red (IR) (THz) bands to convert every light emitting diode (LEDs) bulb into a small cell [2]. However, the broadcast nature of EM waves, including the optical band, and decentralized structure of the dense small cell networks make the wireless communication systems vulnerable to eavesdropping [3], [4]. Traditionally, security functions in a wireless network are provided within protocols by using password protection and/or secret key distribution. On the one hand, password protection and secret key distribution have their own vulnerabilities under the moderate-high computational power of the eavesdropper [5]. Moreover, managing and distributing the secret key over a densely deployed network is a challenging task [6]. On the other hand, all six upper layers of the open systems interconnect (OSI) model use the physical layer as the gateway to connect to the real world. Therefore, physical layer security (PLS) becomes a vital aspect of how trustworthy the transmission is. In [7], it is shown that the PLS relies on the information theoretic secrecy capacity of the channel by exploiting the channel characteristics to hide the information from unauthorized users. Hence, PLS could be ensured without requiring the sharing of the secret key [7].

The MIMO systems offer great potential to enhance achievable data rates and PLS simultaneously. In MIMO systems, more than one transmitter and receiver pair is deployed to exploit *diversity*, *array* and *multiplexing* gains. The diversity gain could provide increased system reliability and quality-of-service by exploiting the independent paths between

Manuscript received July 30, 2019; revised December 19, 2019; accepted January 15, 2020. Date of publication January 27, 2020; date of current version May 15, 2020. This research 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, by the U.S. National Science Foundation under Grants CCF-0939370 and CCF-1908308, and KAUST under Grant No. OSR-2016-CRG5-2958-02. A. Yesilkaya acknowledges the financial support from Zodiac Inflight Innovations (TriaGnoSys GmbH). H. Haas acknowledges support from the EPSRC under Established Career Fellowship Grant EP/R007101/1. He also acknowledges the financial support of his research by the Wolfson Foundation and the Royal Society. The associate editor coordinating the review of this article and approving it for publication was Dr. M. Secondini. *(Corresponding author: Anil Yesilkaya.)*

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

Anil Yesilkaya, Tezcan Cogalan, and Harald Haas are with the LiFi Research and Development Centre, Institute for Digital Communications, School of Engineering, The University of Edinburgh, Edinburgh EH9 3FD, U.K. (e-mail: a.yesilkaya@ed.ac.uk; t.cogalan@ed.ac.uk; h.haas@ed.ac.uk).

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

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2020.2969867

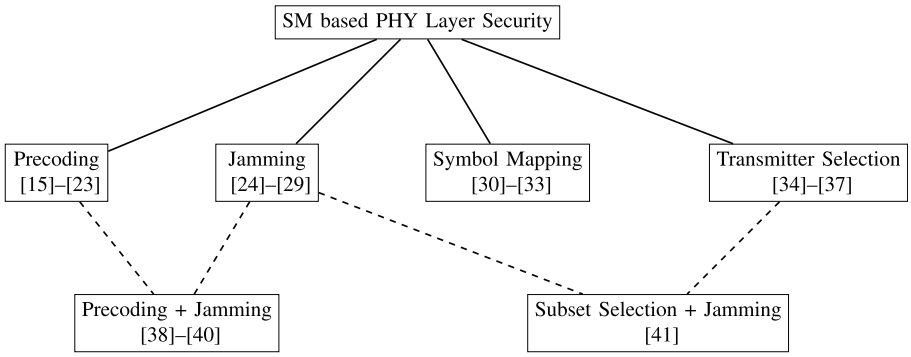


Fig. 1. Taxonomy of the PHY layer security for spatial modulation (SM) based systems.

transmitter and receiver. The coherent combination of the transmit signal to increase the effective received signal-to-noise-ratio (SNR) is referred to as the array gain. Alternatively, the multiple transmitter and receiver pair could be used to boost the data rate while keeping the occupied bandwidth and the SNR the same. spatial multiplexing (SMX) is a widely adopted MIMO transmission method which takes advantage of the multiplexing gain. However, in practical systems, the inter-channel interference (ICI) emerging from channel coupling reduces the achievable data rate of SMX while increasing the detection complexity w.r.t the number of transmit units [8], [9]. Therefore, an alternative MIMO transmission technique, referred to as SM, which activates only a single transmit entity per time instance is proposed [10]. In SM, the information is not only conveyed by the transmit signal but also by the selection of the index of an active transmit unit. As only a single transmitter is active per time instance, the ICI and inter-antenna synchronization problems are avoided while reducing the transmitter/receiver complexity [11]. Furthermore, higher power efficiency is also achieved due to the spatial index information encoding compared to SMX. In order to further simplify the detection complexity of SM systems, space shift keying (SSK) is proposed by [12], [13]. Unlike SM, the information carried by the signal is omitted in SSK whereas only the active transmitter index carries data. Thus, in SSK, detection complexity is reduced at the cost of a loss in spectral efficiency. In order to compensate for the spectral efficiency loss, a generalization to SSK, named generalized SSK (GSSK), is proposed in [14]. Accordingly, the number of active transmitters is chosen to be larger than one to extend the transmission symbols set. Hence, the amount of information carried in the spatial index domain is enhanced in exchange for the ICI and transmit power penalties. It is important to note that both SM based MIMO transmission (e.g SSK, SM, GSSK and generalized SM) and PLS exploit the randomness of the elements of the channel matrix that stems from multipath richness. In the literature, the SM based PLS is provided by various techniques such as precoding, jamming, transmit symbol mapping and subset selection. Furthermore, certain combinations of the mentioned methods are also investigated. A brief summary of the SM based PLS enhancement methods proposed for radio frequency (RF) and optical bands are given in Fig. 1.

In [17], [21], [23], the SM-based PLS is provided by the optimal precoding technique. Specifically, zero forcing precoding (ZFP) is used in most research papers as the main precoding method due to its simplicity. The precoding matrix coefficients are engineered by using the channel state information (CSI) at the transmitter (CSIT) of the legitimate user and the eavesdropper. Thus, the confidential message is perceived by the legitimate user clearly while it is hidden from the eavesdropper. The major drawback of the optimal precoding systems is said to be the eavesdropper's CSIT requirement. In practical systems, the network might be completely unaware of the passive eavesdroppers and potential interceptions. Therefore, suboptimal precoding methods without utilizing the eavesdropper's CSIT are investigated for SM systems in [22], [38]. It is important to note that if the eavesdropper knows the CSI of the legitimate user, the secrecy of the precoding based systems drops dramatically. Moreover, the system complexity of the precoding based systems are proportional to the number of transmitters and receivers. In [15], a precoding matrix is used for realizing SM at the receiver side, referred to as SM (PSM), by encoding spatial information to the receiver indexes. The secrecy performance of this receiver PSM system is investigated in [16], [18], [20].

In order to avoid the problems mentioned above, another well-known method, namely friendly jamming, is proposed for SM based PLS systems in [24]–[29]. The main objective of friendly jamming is to create an artificial noise which lies in the nullspace of the legitimate user. After the confidential information is combined with the jamming signal at the transmitter side, only the eavesdropper will experience destructive effects from the jamming signal. It is worth noting that both the components of the confidential message i.e. spatial and constellation parts, must be encoded in order to provide security. In the precoding based systems, the secrecy emerges intrinsically in both domains due to the matrix multiplication. However, the spatial information is not hidden from the eavesdropper in jamming systems. Therefore, all the transmitters are fed with artificial noise to ensure the spatial domain secrecy in jamming based systems. Compared with the precoding method, friendly jamming could achieve better secrecy as the CSI information of the legitimate user is not sufficient in avoiding artificial noise [38]. Nonetheless, the power efficiency of the SM based systems, which activate

only a subset of the transmitters, is compromised for the spatial domain secrecy.

Transmit symbol mapping based secrecy enhancement for SM related techniques is proposed in [30]–[33]. Specifically, the secrecy is maintained by an encryption key for the given modulation, where the same key is used at the legitimate user's side to decode the confidential message. Note that the secret key is generated by using the channel state information (CSI) of the legitimate user. Hence, there is no need for secret key sharing if perfect CSIT of the legitimate user is assumed. However, due to the look-up table based nature of those methods, the future generation IoT and MTC applications with virtually unlimited numbers of users could introduce severe latency and memory overload in the access points.

The transmitter subset selection is another SM-PLS enhancement technique proposed in [34]–[37]. Accordingly, a specific subset of the transmit entities are chosen such that the radiation pattern of the transmit units are modulated. The confidential signal set could be designed to maximize the minimum Euclidean distance or the SNR at the legitimate user. Hence, the achievable performance of the eavesdropper would be lower than that of the legitimate user. However, the number of bits conveyed in the spatial domain reduces as a side effect of the subset selection process. It is also worth noting that the subset selection method effectively corresponds to the suboptimal precoding [42]. Thus, the subset selection also suffers from the CSI knowledge of the legitimate user at the eavesdropper side, similar to the precoding systems. In order to cope with this problem, friendly jamming is combined with precoding and subset selection methods in [38]–[40] and [41], respectively. Therefore, even the perfect knowledge of the legitimate user's (Bob's) CSI at eavesdropper's (Eve's) side becomes insufficient to decode the transmitted symbols. Again, the intrinsic power penalty of friendly jamming compared to conventional SM based systems persists.

In this paper, we propose a novel power allocation aided spatial constellation design (SCD) technique for GSSK based LiFi systems to increase the PLS. Accordingly, the proposed SCD technique maximizes the minimum Euclidean distance of the transmission set for the legitimate user by designing the power coefficients of the active LEDs. Then, a ZFP, which is based on the CSIT of the legitimate user, is used in order to receive the designed transmission set at the legitimate user's side. Unlike PSM based PLS, the proposed technique retains all the advantages of conventional SM based methods while ensuring the secrecy of the transmission.

The contributions of the proposed technique can be summarized as follows:

- The received multidimensional lattice design technique, referred to as SCD, to maximize the minimum Euclidean distance at Bob's side with the aid of its CSIT is proposed. Thus, the bit error ratio (BER) performance of Bob is maximized while a jamming signal is introduced by both SCD and ZFP to the eavesdropper(s) (Eve(s)). The proposed technique provides secret downlink transmission with reduced ICI, power and complexity penalties as opposed to precoding and jamming based PLS methods for SM.
- Analytical upper and lower bounds of the secrecy capacity are derived for the GSSK systems. Furthermore, the obtained bounds are evaluated by computer simulations.
- Lastly, the secrecy performance of the proposed technique compared with both the conventional and precoding based GSSK systems via computer simulations. Specifically, the effect of Bob and Eve's mobility within a given room is studied for the secrecy performance. It is shown that the secrecy rate of the proposed method outperforms the conventional GSSK and precoded GSSK techniques, even when Bob and Eve are located closely together.

The remainder of the paper is structured as follows: In Section II, we present details of the proposed system. The power allocation aided SCD scheme is introduced in Section III. In Section IV, lower and upper bounds for the secrecy capacity are obtained. Finally, computer simulation results are presented in Section V and conclusions are drawn in Section VI.

Notation: Throughout the paper, matrices and column vectors are in bold uppercase and lowercase letters, respectively. The m^{th} row and n^{th} column element of the matrix $\mathbf{A}$ is denoted by $A_{m,n}$. Similarly, the m^{th} element of the vector $\mathbf{a}$ is given by a_m. The transpose, trace, Euclidean norm, determinant and Hadamard product operations are expressed by $(\cdot)^{\text{T}}$, $\text{tr}(\cdot)$, $\|\cdot\|$, $\det(.)$ and $\circ$, respectively. The operation that obtains the main diagonal of the matrix $\mathbf{A}$ is denoted by $\text{diag}(\mathbf{A})$. The real normal distribution is given by $\mathcal{N}(\mu, \sigma^2)$ where μ represents the mean and σ^2 is the variance. The $m \times n$ ring of real numbers is denoted by $\mathbb{R}_{m\times n}$. Statistical expectation, argument maximum, argument minimum, floor and ceiling operations are represented by $\text{E}\{\cdot\}$, $\arg\max\{\cdot\}$, $\arg\min\{\cdot\}$, $\lfloor\cdot\rfloor$ and $\lceil\cdot\rceil$, respectively. The component-wise inequality between two vectors and the component-wise absolute value is given by $\preceq$ and $|.|$, respectively.

II. System Description

In this work, we consider a novel power allocation technique to increase PLS in MIMO-GSSK based LiFi systems. The GSSK, proposed in [14], is a low complexity and bandwidth efficient SM derivative which only conveys information by the active transmitter indexes. Unlike conventional SM, the absence of information carried in the signal domain simplifies the detection complexity in GSSK. The number of active transmitters per time instant is set to become greater than one in GSSK while this number is strictly one in conventional SSK systems. Thus, the spectral efficiency of GSSK becomes much higher than in SSK. Furthermore, the multiple active transmitters provide a higher degree of freedom for power allocation. We consider a LiFi system where the mobile devices of the legitimate user and eavesdropper are equipped with N_{r} photo-diodes (PDs). Moreover, the transmitter, which effectively covers the given room, consists of N_{t} LEDs. As the users have simple handheld mobile devices in practice, $N_{\text{r}} < N_{\text{t}}$ is assumed due to the potential restrictions. Randomly generated incoming user bits are parsed to permutation vectors of length L, $\mathbf{b}_l = [b_{l,1}, b_{l,2}, \cdots, b_{l,L}]^{\text{T}}$ which are one-to-one mapped onto the k^{th} transmission vector,

$\mathbf{s}_k = [s_{k,1}, s_{k,2}, \cdots, s_{k,N_\mathrm{t}}]^\mathrm{T}$. The parameter L denotes the number of bits carried per transmission symbol. The l^{th} binary permutation vector $\mathbf{b}_l$ consists of $b_{l,j} \in \{0,1\}$ for $1 \le l \le 2^L$ and $1 \le j \le L$. Similarly, the corresponding k^{th} GSSK transmission vector $\mathbf{s}_k$ is chosen from the alphabet given by

$$\mathcal{S} = \left\{ s_{k,i} \in \{0, I\},\ 1 \le i \le N_\mathrm{t},\ 1 \le k \le K \ \middle|\ \sum_{i=1}^{N_\mathrm{t}} s_{k,i} = N_\mathrm{a} I,\ \ \forall k \right\}. \quad (1)$$

The parameter N_a denotes the number of active LEDs for the GSSK. The average light intensity transmitted by an active LEDs is given by I where its value is chosen to be within the dynamic range of the LEDs. The cardinality of the set $\mathcal{S}$ becomes, $K = 2^L = 2^{\left\lfloor \log_2 \binom{N_\mathrm{t}}{N_\mathrm{a}} \right\rfloor}$ in order to map each $\mathbf{b}_l$ to the $\mathbf{s}_k$. Therefore, only K out of $\binom{N_\mathrm{t}}{N_\mathrm{a}}$ combinations could be used for the data transmission. The number of bits transmitted by the GSSK becomes,

$$\eta_{\text{GSSK}} = \left\lfloor \log_2 \binom{N_\mathrm{t}}{N_\mathrm{a}} \right\rfloor \ \text{ bits per symbol.} \quad (2)$$

It should be noted that in conventional SM systems, N_t is taken as a power of two as a rule of thumb. Thus, the optimum number of active transmitters for the maximum spectral efficiency becomes, $\hat{N}_\mathrm{a} = \arg\max_{N_\mathrm{a}} \{\eta_{\text{GSSK}}\} = N_\mathrm{t}/2$. Then, the k^{th} transmit signal vector, $\mathbf{s}_k$, chosen from the set $\mathcal{S}$ is fed into digital-to-analogue converter and N_t LEDs, consecutively. At the receiver, optical-to-electrical conversion is performed by the PDs and analogue-to-digital conversion is also utilized. The resultant $N_\mathrm{r} \times 1$ received baseband electrical domain signal vector is given by

$$\mathbf{y} = \mathbf{H}\mathbf{s}_k + \mathbf{n} = \mathbf{r}_k + \mathbf{n}. \quad (3)$$

The $N_\mathrm{r} \times 1$ dimensional additive white Gaussian noise (AWGN) vector is denoted by $\mathbf{n}$. The elements of $\mathbf{n}$ follows $\mathcal{N}(0, \sigma_n^2)$. Moreover, the $N_\mathrm{r} \times N_\mathrm{t}$ optical channel impulse response vector is denoted by $\mathbf{H}$. Without loss of generality, digital-to-analog, analog-to-digital, electrical-to-optical and optical-to-electrical conversion coefficients are assumed to be unity. Unlike RF, the multipath richness of the MIMO channel in optical wireless communications (OWC) is quite limited due to the lack of small scale-fading and multipath reflections [43]. It is reported in [43] that the OWC channel could be practically taken as only line-of-sight (LoS) if the mobile user is far from the edges of the room, which is the likely case. Hence, in this work we will consider a simple LoS MIMO-OWC channel model. The $N_\mathrm{r} \times N_\mathrm{t}$ LoS channel matrix is given by

$$\mathbf{H} = \begin{bmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,N_\mathrm{t}} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,N_\mathrm{t}} \\ \vdots & \ddots & \ddots & \\ h_{N_\mathrm{r},1} & h_{N_\mathrm{r},2} & \cdots & h_{N_\mathrm{r},N_\mathrm{t}} \end{bmatrix} \in \mathbb{R}^+, \quad (4)$$

where the channel coefficients between r^{th} PD and t^{th} LED are given as follows [44]:

$$h_{r,t} = \frac{(m+1)A_{\text{PD}}}{2\pi d_{r,t}^2} \cos^m(\phi_{r,t}) \cos(\theta_{r,t}) \mathbb{1}_{\Psi_{1/2}}(\theta_{r,t}). \quad (5)$$

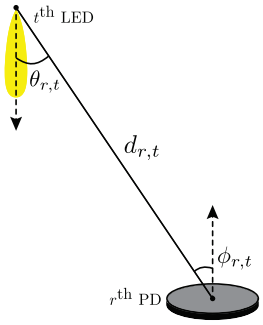


Fig. 2. Representation of the channel parameters.

The geometrical representation of the parameters of $h_{r,t}$ are given in Fig. 2. Accordingly, the angles $\phi_{r,t}$ and $\theta_{r,t}$ represent the angle of emergence and angle of incidence between the r^{th} receive PD and t^{th} transmit LED , respectively. Also the distance between the r^{th} receive PD and t^{th} transmit LED is denoted by $d_{r,t}$. The parameter m is the Lambertian emission order of the light source and defined as $m = -1/\log_2(\cos(\Phi_{1/2}))$ where $\Phi_{1/2}$ is the semi-angle of the half power of the LED. The A_{PD} indicates the effective area of the non-imaging PD. The indicator function $\mathbb{1}_{\Psi_{1/2}}(\cdot)$ determines whether the incidence angle is within the field-of-view (FoV) of the PD as follows:

$$\mathbb{1}_{\Psi_{1/2}}(x) = \begin{cases} 1, & \text{if } |x| \le \Psi_{1/2} \\ 0, & \text{otherwise} \end{cases} \quad (6)$$

where $\Psi_{1/2}$ is the half-angle of FoV of the PD. Then, at the receiver, the maximum-likelihood (ML) detector is utilized to estimate the transmitted vector as follows:

$$\hat{\mathbf{s}}_k = \arg\max_{\mathbf{s}_k \in \mathcal{S}} p(\mathbf{y} \mid \mathbf{H}, \mathbf{s}_k) = \arg\min_{\mathbf{s}_k \in \mathcal{S}} ||\mathbf{y} - \mathbf{H}\mathbf{s}_k||, \quad \forall k. \quad (7)$$

It is worth noting from (7) that $\hat{\mathbf{s}}_k$ also reveals the active LED indexes. Finally, an inverse mapping function is utilized after ML detector to obtain the transmitted bits back.

III. Physical Layer Security Enhancement for GSSK

In this section, we propose a novel power allocation based PLS method for MIMO-GSSK systems. The proposed technique addresses the downlink transmission security by exploiting the quasi-static characteristics of the optical channels. Compared to SSK with power allocation [45], GSSK exploits higher degrees of freedom due to the larger number of active transmit elements, which yields a better secrecy performance. Thus, in this paper, SCD is proposed for GSSK transmission technique. We consider an indoor LiFi network with an access point (Alice), a legitimate user (Bob) and a passive eavesdropper (Eve). However, there might be more than one passive eavesdropper within a LiFi system. Therefore, the system designed such that it would not be effected by the number of eavesdroppers. The block diagram of the MIMO-GSSK based downlink LiFi structure is depicted in Fig. 3. Accordingly, the proposed PLS enhancement of the MIMO-GSSK is achieved in three steps; SCD for the received

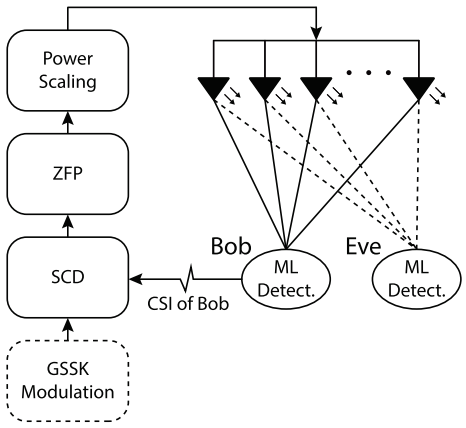


Fig. 3. Schematic of proposed PLS technique for MIMO-GSSK.

symbols, ZFP and power scaling. Each step of the proposed method will be detailed in the following subsections.

A. Spatial Constellation Design

In this subsection, the optimal design of the received signal set, namely SCD will be considered to increase PLS for MIMO-GSSK systems. The design of the received symbols by using the quasi-static characteristics of the optical channel is investigated in [46] for multiple-input-single-output (MISO) systems. In this work, the power allocation based received SCD is carried to MIMO-GSSK while generalizing the concept to arbitrary number of transmitters and receivers. The proposed method maximizes the minimum Euclidean distance in the Bob's received vectors set with the aid of its CSIT. As the SCD is tailored for the benefit of Bob, the signal reception at the Eve's side will negatively be effected due to the CSI difference. Specifically, both SCD and ZFP introduce a jamming signal at the Eve's side which constitutes the main factor of the PLS in the proposed technique. It will be shown via computer simulations in Section V that the proposed method ensures the secrecy even when Eve is in the vicinity of Bob. Compared to only ZFP based method, the superiority of SCD in terms of the secrecy performance is also proven. For the considered MIMO-GSSK system, only some of the elements are non-zero in the transmit vector $\mathbf{s}_k$. Thus, the received signal model of GSSK systems, given in (3), could further be simplified as follows:

$$\mathbf{y} = \tilde{\mathbf{H}}_k \tilde{\mathbf{s}}_k + \mathbf{n}, \tag{8}$$

where $\tilde{\mathbf{s}}_k = [\tilde{s}_{k,1}, \tilde{s}_{k,2}, \cdots, \tilde{s}_{k,N_\mathrm{a}}]^\mathrm{T}$ represents the effective constellation symbols vector for the k^{th} transmit symbol. In other words, $\tilde{\mathbf{s}}_k$ only contains the non-zero elements of $\mathbf{s}_k$. Similarly, $\tilde{\mathbf{H}}_k \in \mathbb{R}^{N_\mathrm{r} \times N_\mathrm{a}}$ is the effective channel matrix which only conveys the column vectors of $\mathbf{H}$ corresponding to the active LEDs. The indexes of the active LEDs for the k^{th} transmit symbol are forming a set $\mathcal{I}_k = \{\mathcal{I}_{k,1}, \mathcal{I}_{k,2}, \cdots, \mathcal{I}_{k,N_\mathrm{a}}\}$. Thus, $\tilde{\mathbf{H}}_k = [\mathbf{h}_{\mathcal{I}_{k,1}}, \mathbf{h}_{\mathcal{I}_{k,2}}, \cdots, \mathbf{h}_{\mathcal{I}_{k,N_\mathrm{a}}}]$ where $\mathbf{h}_i$ denotes the i^{th} column vector of $\mathbf{H}$. It is important to note from (3) and (8) that $\mathbb{R}^{N_\mathrm{t}}$ and $\mathbb{R}^{N_\mathrm{a}}$ dimensional spaces are projected onto $\mathbb{R}^{N_\mathrm{r}}$-space by the transformation matrices $\mathbf{H}$ and $\tilde{\mathbf{H}}_k$, respectively. From (8), the received vector is simply a linear combination of the effective column vectors of the channel matrix $\mathbf{H}$. Since the constellation symbols are omitted in GSSK, $\tilde{\mathbf{s}}_k = I\mathbf{1}_{N_\mathrm{a}}$, the received signal model reduces to

$$\mathbf{y} = I\left(\sum_{\forall i \in \mathcal{I}_k} \mathbf{h}_i\right) + \mathbf{n} = I\tilde{\mathbf{h}}_k + \mathbf{n}, \tag{9}$$

where the effective channel matrix $\tilde{\mathbf{H}}_k$ is further reduced to the effective channel vector denoted by $\tilde{\mathbf{h}}_k$ in conventional GSSK. The received signal set for the conventional GSSK, given by (9), is depicted in Fig. 4(a). As it can be inferred from (9) and Fig. 4(a), the channel parameters will dictate the detection performance in conventional GSSK. Since the location, orientation and blockage properties of the legitimate user (Bob) play a significant role on the elements of channel matrix, PLS cannot be maintained reliably. Therefore, we propose a power allocation based SCD method which separates Bob's received signal points (vectors) maximally from each other. By using (8), if we choose $\tilde{\mathbf{s}}_k$ such that the received signal at Bob's side after direct-current (DC) bias compensation becomes,

$$\mathbf{y} = \rho \mathbf{v}_k + \mathbf{n}. \tag{10}$$

The vector $\mathbf{v}_k \in \mathbb{R}^{N_\mathrm{r} \times 1}$ represents a desired received constellation point at Bob's side which corresponds to k^{th} transmit symbol. In order to obtain the desired signal set, the transmitted signals must be engineered such that $\tilde{\mathbf{s}}_k = \rho \mathbf{P}_k \mathbf{v}_k + B_\mathrm{DC}$. The precoding matrix $\mathbf{P}_k \in \mathbb{R}^{N_\mathrm{a} \times N_\mathrm{r}}$ which removes the coupling between LEDs and PDs will be detailed in the following subsection. The DC bias, B_DC, ensures that the transmit signal is positive valued, which is an essential limitation of intensity-modulation and direct-detection (IM/DD) systems. Furthermore, the main functionality of LiFi is not only to provide broadband data but also satisfy the minimum illumination requirement in a certain area. Hence, the DC bias will be imposed on all the LEDs to make the average optical intensity of the transmit signal B_DC. Similarly, the power scaling factor, ρ, fits the maximum value of the transmit signal within the linear dynamic range of the LEDs. Therefore, the upper and lower clipping of the designed signal as well as the noise induced by the clipping are avoided. Calculation of both parameters, ρ and B_DC, will be detailed in the Section III-C. If the N_r-dimensional desired received vectors set is given by

$$\mathcal{V} : \left\{\mathbf{v}_k = [v_{k,1}, v_{k,2}, \cdots, v_{k,N_\mathrm{r}}]^\mathrm{T}, 1 \leq k \leq K\right\}, \tag{11}$$

where the $\mathbf{v}_k$'s are forming a K-ary received signal constellation in N_r-space. By altering the elements of $\mathbf{v}_k$ we can design a uniform constellation where it would maximize the minimum Euclidean distance under a given power constraint. It is shown in [46] that the design and analysis of the unipolar constellations becomes very complex rapidly due to the asymmetry. Hence, a bipolar symmetric constellation is designed in this work and the resultant values are made positive by a DC bias addition. In order to satisfy the optimality of the designed constellation under AWGN, $\mathbf{v}_k$'s should be at the edges of a hyper-rectangular constellation in $\mathbb{R}^{N_\mathrm{r}}$. The design of the M-ary hyper-rectangular constellation is done

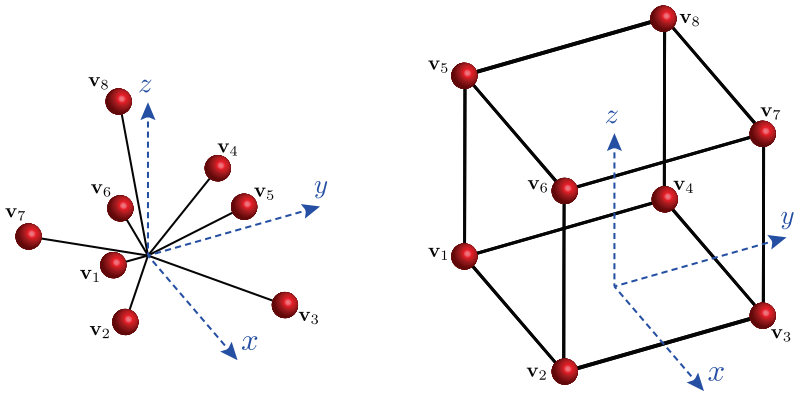


Fig. 4. Received signal constellation points; (a) conventional GSSK, (b) SCD-GSSK for $N_{\rm t}=5$, $N_{\rm r}=3$, $N_{\rm a}=3$.

in the 1-D space first then the design is extended to the $N_{\rm r}$-dimensions. The parameter M denotes the order of the extended constellation which will be explained shortly. The $\sqrt[N_{\rm r}]{M}$-ary pulse amplitude modulation (PAM) constellation set in 1-D simply becomes, $\mathcal{P}^1 \in \{\pm\alpha, \pm 3\alpha, \cdots, \pm(\sqrt[N_{\rm r}]{M}-1)\alpha\}$. The parameter α denotes the signal amplitude in $\sqrt[N_{\rm r}]{M}$-ary PAM which is chosen by $\alpha=\sqrt{\frac{3}{M^{2/N_{\rm r}}-1}}$ to normalize the electrical power of the constellation. The order of the extended constellation set is calculated by

$$M=\begin{cases} K; & \text{if} \quad N_{\rm r}=1 \\ \left(2\lceil\frac{1}{2}K^{1/N_{\rm r}}\rceil\right)^{N_{\rm r}}; & \text{if} \quad N_{\rm r}>1. \end{cases} \tag{12}$$

It is worth noting from (12) that the order of $\mathcal{P}^1$, $\sqrt[N_{\rm r}]{M}$, might not be an even number which would yield an unbalanced constellation in $N_{\rm r}$-space. To avoid asymmetry, the order of $\mathcal{P}^1$ is simply rounded up to the nearest consecutive even number. In other words, the K-ary constellation is extended to the M-ary possibilities constellation. Then, K points, which yield the SCD vectors, are chosen out of M. The optimal selection of K out of M points is out of scope of this work. Hence, a random selection of K out of M points is adopted throughout the paper in order to average the performance for a given constellation. In Fig. 4(b), the elements of $\mathbf{v}_k$ are depicted for $N_{\rm t}=5$, $N_{\rm r}=3$ and $N_{\rm a}=3$. From Figs. 4(a) and 4(b), we can easily see that the SCD forces irregular constellation points to be located at the corners of a hyper-rectangle. Since $K=2^{\lfloor\log_2\binom{5}{3}\rfloor}=8$ and $N_{\rm r}=3$, the 8-ary constellation could be mapped to the edges of a cube in $\mathbb{R}^3$. For the sake of clarity, a numerical example for the SCD is provided for $N_{\rm t}=5$, $N_{\rm r}=3$ and $N_{\rm a}=3$ in Table I.

TABLE I

TRANSMISSION VECTORS OF SCD BASED GSSK WITH $N_{\rm T}=5$, $N_{\rm R}=3$ AND $N_{\rm A}=3$

$\mathbf{b}=(b_1,b_2,b_3)$	$\mathcal{I}_k$	$\mathbf{v}_k=[v_{k,1},v_{k,2},v_{k,3}]^{\rm T}$
[0 0 0]	$(\mathcal{I}_{1,1},\mathcal{I}_{1,2},\mathcal{I}_{1,3})$	$\mathbf{v}_1=[v_{1,1},v_{1,2},v_{1,3}]^{\rm T}$
[0 0 1]	$(\mathcal{I}_{2,1},\mathcal{I}_{2,2},\mathcal{I}_{2,5})$	$\mathbf{v}_2=[v_{2,1},v_{2,2},v_{2,3}]^{\rm T}$
[0 1 0]	$(\mathcal{I}_{3,1},\mathcal{I}_{3,3},\mathcal{I}_{3,4})$	$\mathbf{v}_3=[v_{3,1},v_{3,2},v_{3,3}]^{\rm T}$
[0 1 1]	$(\mathcal{I}_{4,1},\mathcal{I}_{4,3},\mathcal{I}_{4,5})$	$\mathbf{v}_4=[v_{4,1},v_{4,2},v_{4,3}]^{\rm T}$
[1 0 0]	$(\mathcal{I}_{5,1},\mathcal{I}_{5,4},\mathcal{I}_{5,5})$	$\mathbf{v}_5=[v_{5,1},v_{5,2},v_{5,3}]^{\rm T}$
[1 0 1]	$(\mathcal{I}_{6,2},\mathcal{I}_{6,3},\mathcal{I}_{6,4})$	$\mathbf{v}_6=[v_{6,1},v_{6,2},v_{6,3}]^{\rm T}$
[1 1 0]	$(\mathcal{I}_{7,2},\mathcal{I}_{7,4},\mathcal{I}_{7,5})$	$\mathbf{v}_7=[v_{7,1},v_{7,2},v_{7,3}]^{\rm T}$
[1 1 1]	$(\mathcal{I}_{8,3},\mathcal{I}_{8,4},\mathcal{I}_{8,5})$	$\mathbf{v}_8=[v_{8,1},v_{8,2},v_{8,3}]^{\rm T}$

B. Design of Zero Forcing Precoder

In this subsection, a ZFP is designed with the aid of Bob's CSIT to avoid the ICI. In order to observe the $\mathbf{v}_k$'s at Bob's side as given in (10), we design a ZFP which provides the energy leakage-free reception by utilizing the generalized left inverse of the channel matrix as follows:

$$\mathbf{P}_k^{+}=\left(\tilde{\mathbf{H}}_{k,\rm B}^{\rm T}\tilde{\mathbf{H}}_{k,\rm B}\right)^{-1}\tilde{\mathbf{H}}_{k,\rm B}^{\rm T} \quad \forall k, \tag{13}$$

where $\tilde{\mathbf{H}}_{k,\rm B}$ denotes Bob's effective channel matrix for the $k^{\rm th}$ transmit symbol. Thus, the precoder yields, $\tilde{\mathbf{H}}_{k,\rm B}\mathbf{P}_k^{+}=\mathbf{I}_{N_{\rm r}}$. It should be noted from (13) that as $N_{\rm a}\neq N_{\rm r}$ the matrix $\left(\tilde{\mathbf{H}}_{k,\rm B}^{\rm T}\tilde{\mathbf{H}}_{k,\rm B}\right)$ might not be invertible. It is also shown in [8], [47] that even though $N_{\rm a}=N_{\rm r}$, the square channel matrix might become singular due to the symmetry of the channel parameters. In OWC, unlike RF, geometry plays significant role on the channel elements. Hence, the perfectly symmetrical LED and PD configurations yield a linearly dependent row/column vectors in the channel matrix. In other words, geometrical symmetry causes rank deficient (singular) channel matrices. To avoid the mentioned problem, in this work, we will employ the standard trick of adding a slight perturbation to $\left(\tilde{\mathbf{H}}_{k,\rm B}^{\rm T}\tilde{\mathbf{H}}_{k,\rm B}\right)$ such that it becomes full rank. Consequently, the final form of the ZFP becomes

$$\mathbf{P}_k=\left(\tilde{\mathbf{H}}_{k,\rm B}^{\rm T}\tilde{\mathbf{H}}_{k,\rm B}+\epsilon\mathbf{I}_{N_{\rm a}}\right)^{-1}\tilde{\mathbf{H}}_{k,\rm B}^{\rm T} \quad \forall k, \tag{14}$$

where the addition of a very small identity matrix for $\epsilon\approx 0^{+}$ makes $\left(\tilde{\mathbf{H}}_{k,\rm B}^{\rm T}\tilde{\mathbf{H}}_{k,\rm B}\right)$ non-singular. Note that as a rule of thumb,

ϵ should be chosen to satisfy $\epsilon < \lambda_{\min}$, where $\lambda_{\min}$ is the smallest non-zero eigenvalue of the matrix $\left(\tilde{\mathbf{H}}_{k,\mathrm{B}}^{\mathrm{T}}\tilde{\mathbf{H}}_{k,\mathrm{B}}\right)$.

C. Scaling the Transmit Power

In this subsection, both ρ and B_{DC} will be calculated. Accordingly, the average power at the transmitter side is constrained due to the limited dynamic range of the LEDs and eye safety concerns. Therefore, after the SCD and precoding stages, the resultant signal should be fitted into the operating range of the LED by the appropriate selection of ρ and B_{DC}. The components of the designed signal $\tilde{\mathbf{s}}_k = \rho\mathbf{P}_k\mathbf{v}_k + B_{\mathrm{DC}}$ arriving at each LED must be positive valued and not exceed the minimum ($I_{\min}$) and maximum ($I_{\max}$) current limits. As $\mathrm{E}\{\tilde{\mathbf{s}}_k\} = B_{\mathrm{DC}}\ \forall k$, the value of the required bias becomes $B_{\mathrm{DC}} = (I_{\max} + I_{\min})/2$. Similarly, we know that the elements of the vector $\tilde{\mathbf{s}}_k$ takes values between $[-\tilde{s}_{k,\max},\ \tilde{s}_{k,\max}]$ for the k^{th} symbol. Hence, the power coefficient becomes, $\rho = I_{\max}/\max\{|\tilde{\mathbf{s}}_k|\},\ \forall k$. The upper bound for the term $\max\{|\tilde{\mathbf{s}}_k|\}$ is given by

$$\begin{aligned}\max\{|\tilde{\mathbf{s}}_k|\} &= \max\left\{\left|\left(\tilde{\mathbf{H}}_{k,\mathrm{B}}^{T}\tilde{\mathbf{H}}_{k,\mathrm{B}} + \epsilon\mathbf{I}_{N_{\mathrm{r}}}\right)^{-1}\tilde{\mathbf{H}}_{k,\mathrm{B}}^{T}\mathbf{v}_k\right|\right\} \\ &\preceq \max\{|\mathbf{P}_k|\}\max\{|\mathbf{v}_k|\} \equiv P_{\max}A_{\max}, \quad (15)\end{aligned}$$

where $P_{\max}$ and $A_{\max}$ represent the maximum value of the precoder and designed constellation vectors, respectively. The values of both $P_{\max}$ and $A_{\max}$ are calculated as follows:

$$P_{\max} = \max\{\mathbf{P}_k\}, \quad (16)$$

$$A_{\max} = (\sqrt[N_{\mathrm{r}}]{M} - 1)\alpha. \quad (17)$$

Finally, the received signals by Bob and Eve, after propagation through their respective channels are given by

$$\mathbf{y}_{\mathrm{B}} = \mathbf{s}_{\mathrm{B}} + B_{\mathrm{DC}}\tilde{\mathbf{H}}_{k,\mathrm{B}} + \mathbf{n}_{\mathrm{B}}, \quad (18)$$

$$\mathbf{y}_{\mathrm{E}} = \mathbf{s}_{\mathrm{E}} + B_{\mathrm{DC}}\tilde{\mathbf{H}}_{k,\mathrm{E}} + \mathbf{n}_{\mathrm{E}}, \quad (19)$$

where the transmit symbols observed by Bob ($\mathbf{s}_{\mathrm{B}}$) and Eve ($\mathbf{s}_{\mathrm{E}}$) are given as follows:

$$\begin{aligned}\mathbf{s}_{\mathrm{B}} &\triangleq \rho\tilde{\mathbf{H}}_{k,\mathrm{B}}\mathbf{P}_k\mathbf{v}_{k,\mathrm{B}} = \rho\mathbf{v}_{k,\mathrm{B}}, \\ \mathbf{s}_{\mathrm{E}} &\triangleq \rho\tilde{\mathbf{H}}_{k,\mathrm{E}}\mathbf{P}_k\mathbf{v}_{k,\mathrm{B}} \\ &= \rho\tilde{\mathbf{H}}_{k,\mathrm{E}}\left(\tilde{\mathbf{H}}_{k,\mathrm{B}}^{\mathrm{T}}\tilde{\mathbf{H}}_{k,\mathrm{B}} + \epsilon\mathbf{I}_{N_{\mathrm{r}}}\right)^{-1}\tilde{\mathbf{H}}_{k,\mathrm{B}}^{\mathrm{T}}\mathbf{v}_{k,\mathrm{B}},\end{aligned}$$

where $\tilde{\mathbf{H}}_{k,\mathrm{E}}$ is Eve's effective channel matrix which corresponds to the k^{th} transmit symbol. The AWGN noise components at Bob and Eve's sides, $\mathbf{n}_{\mathrm{B}}$ and $\mathbf{n}_{\mathrm{E}}$, are zero mean Gaussian random variables with variances, σ_{B}^2 and σ_{E}^2, respectively. The DC component B_{DC} can be suppressed before the detection process. Consequently, the received signals (18) and (19) can be re-expressed by

$$\mathbf{y}_{\mathrm{B}} = \mathbf{s}_{\mathrm{B}} + \mathbf{n}_{\mathrm{B}}, \quad (20)$$

$$\mathbf{y}_{\mathrm{E}} = \mathbf{s}_{\mathrm{B}} + \mathbf{J} + \mathbf{n}_{\mathrm{E}}, \quad (21)$$

where the natural jamming signal occurring at Eve's side is denoted by $\mathbf{J}$. It is important to note that both SCD and the precoding stages are tailored for Bob's CSIT and they will be serving as a natural jammer if Eve has different channel coefficients. In other words, the SCD maximizes the BER performance of Bob while it produces a jamming signal to all the other users. The expression for the jamming signal is given by

$$\mathbf{J} = \mathbf{s}_{\mathrm{E}} - \mathbf{s}_{\mathrm{B}} = \rho\left(\tilde{\mathbf{H}}_{k,\mathrm{E}} - \tilde{\mathbf{H}}_{k,\mathrm{B}}\right)\mathbf{P}_k\mathbf{v}_{k,\mathrm{B}}. \quad (22)$$

Note from (21) and (22) that the jamming signal naturally emerges in the proposed technique due to the SCD and ZFP. Therefore, the PLS is maintained whilst minimizing the BER performance of the legitimate user. Unlike in the conventional friendly jamming method, an additional computation to design a jamming signal is not required to hide spatial symbols. The jamming vector observed at the eavesdropper's side could be approximated as a Gaussian random vector with zero mean and covariance matrix $\mathbb{C}_{\mathbf{J}}$. From (21), $\mathbf{w} \triangleq \mathbf{J} + \mathbf{n}_{\mathrm{E}}$ is a colored zero-mean Gaussian vector with covariance matrix

$$\mathbb{C}_{\mathbf{w}} = \mathrm{E}\{\mathbf{w}\mathbf{w}^{\mathrm{T}}\} = \mathbb{C}_{\mathbf{J}} + \sigma_{\mathrm{E}}^2\mathbf{I}_{N_{\mathrm{r}}}. \quad (23)$$

If both sides of (21) is multiplied by $\mathbb{C}_{\mathbf{w}}^{-1/2}$ we obtain,

$$\mathbf{y}'_{\mathrm{E}} = \mathbb{C}_{\mathbf{w}}^{-1/2}\mathbf{y}_{\mathrm{E}} = \mathbf{s}'_{\mathrm{E}} + \mathbf{w}'_{\mathrm{E}}, \quad (24)$$

where $\mathbf{s}'_{\mathrm{E}} = \mathbb{C}_{\mathbf{w}}^{-1/2}\mathbf{s}_{\mathrm{B}}$ and $\mathbf{w}'_{\mathrm{E}} = \mathbb{C}_{\mathbf{w}}^{-1/2}\mathbf{w}$ becomes the standard white Gaussian vector with zero mean and unit covariance matrix. As described earlier, at both Bob's and Eve's sides, the detection of spatial information is implemented by the ML detector as

$$\begin{aligned}\widehat{\mathcal{I}}_{k,\mathrm{B}} &= \arg\max_{\mathcal{I}_k}\{\ \|\ \mathbf{y}_{\mathrm{B}} - \mathbf{s}_{\mathrm{B}}\ \|^2\}, \\ \widehat{\mathcal{I}}_{k,\mathrm{E}} &= \arg\max_{\mathcal{I}_k}\{\ \|\ \mathbf{y}'_{\mathrm{E}} - \mathbf{s}'_{\mathrm{E}}\ \|^2\}. \quad (25)\end{aligned}$$

IV. Achievable Secrecy Capacity of Optical MIMO-GSSK System

We now consider the secrecy capacity of the MIMO-OWC wiretap channel in the presence of a single eavesdropper as shown in Fig. 3. Different than the other work presented in the literature on this topic, as the input spatial symbols $\mathbf{s}_\chi$ are determined by the indices of randomly selected LEDs, the input probability distribution is discrete-valued with $P(\text{selecting the } i^{\text{th}} \text{ index}) = 1/N_{\mathrm{t}}$ and the output $\mathbf{y}_\chi$ is continuous random variable having a Gaussian mixture distribution, where χ represents the user such as $\chi \in \{\mathrm{B},\mathrm{E}\}$. The capacity of such discrete-continuous memoryless channels with the ML based spatial information detection, as considered in (25), can be expressed for Bob's and Eve's channels as [48]

$$\mathbb{C}_\chi = \log_2(K) - \frac{1}{K}\sum_{i=1}^{K}\mathrm{E}\{\mathbf{n}_\chi\}\log_2\left(\sum_{j=1}^{K}\exp\left(\mathbf{\Psi}_\chi(i,j)\right)\right), \quad (26)$$

where $\chi \in \{\mathrm{B},\mathrm{E}\}$ and $\mathbf{\Psi}_\chi(i,j)$ is given by

$$\mathbf{\Psi}_\chi(i,j) = -\frac{||\mathbf{s}_\chi(i) - \mathbf{s}_\chi(j) + \mathbf{n}_\chi||^2 + ||\mathbf{n}_\chi||^2}{\sigma_\chi^2}.$$

Consequently, the secrecy capacity of the optical GSSK can be determined as

$$\mathbb{C}_{\mathrm{GSSK}} = \mathbb{C}_{\mathrm{B}} - \mathbb{C}_{\mathrm{E}}. \quad (27)$$

Note that $\mathbb{C}_{\text{GSSK}}$ in (27) cannot be obtained analytically in a closed-form expression and it is implicitly relies on the ML based detection of (25), which has quite high computational complexity. On the other hand, reduced complexity channel capacities between Alice-Bob and Alice-Eve can be computed based on the per bit mutual information $\mathbb{I}_\chi(b;\hat{b}_\chi)$. The mutual information is measured for the proposed GSSK system between the input bits $b \in \{0,1\}$ and the corresponding demodulated output bits $\hat{b}_\chi \in \{0,1\}$. Hence, the resulting binary input-output channels between Alice-Bob, and Alice-Eve can be modelled as a binary symmetric channel (BSC) with crossover probabilities ϵ_{B} and ϵ_{E}, respectively. Both achieve equal input probabilities. That is $P(0) = P(1) = 1/2$. Therefore, both channels achieve the channel capacity exactly.

Computed with respect to this specific input distribution, the secrecy capacity of a optical MIMO-GSSK wiretap channel yields

$$\begin{aligned}\mathbb{C}_{\text{GSSK}} &= \mathbb{I}_{\text{B}}(b;\hat{b}_{\text{B}}) - \mathbb{I}_{\text{E}}(b;\hat{b}_{\text{E}}) \\ &= \mathbb{H}_{\text{B}}(b) - \mathbb{H}_{\text{B}}(b|\hat{b}_{\text{B}}) - \mathbb{H}_{\text{E}}(b) + \mathbb{H}_{\text{E}}(b|\hat{b}_{\text{E}}),\end{aligned} \quad (28)$$

where $\mathbb{H}_\chi(b) = -\sum_{m=0}^{1} P(m)\log_2 P(m)$ denotes the entropy of the input bits with respect to the input probabilities $P(m), m = 1, 2$. On the other hand, $\mathbb{H}_\chi(b|\hat{b}_\chi)$ represents conditional entropy and for a BSC it is given by

$$\mathbb{H}_\chi(b|\hat{b}_\chi) = -\epsilon_\chi \log_2 \epsilon_\chi - (1-\epsilon_\chi)\log_2(1-\epsilon_\chi). \quad (29)$$

Hence, by substituting (29) into (28), and exploiting $H_\chi(b) = 1$, since the input bits are equally likely, the exact achievable secrecy capacity for L, the number of bits transmitted per LEDs index, becomes

$$\begin{aligned}\mathbb{C}_{\text{GSSK}} = L\Big(&\epsilon_{\text{B}}\log_2\epsilon_{\text{B}} + (1-\epsilon_{\text{B}})\log_2(1-\epsilon_{\text{B}}) \\ &- \epsilon_{\text{E}}\log_2\epsilon_{\text{E}} - (1-\epsilon_{\text{E}})\log_2(1-\epsilon_{\text{E}})\Big).\end{aligned} \quad (30)$$

The crossover probabilities ϵ_χ in (30) correspond to the BER of the spatial symbol $\mathcal{I}$, due to detection of $\mathbf{y}_\chi$ in (20) and (21). The average BER is limited by the union bound as

$$\epsilon_\chi \leq \sum_{i=1}^{K-1}\sum_{i'=i+1}^{K} 2\frac{n_{i,i'}}{K}\text{Prob}\left(\mathcal{I}=i\rightarrow\widehat{\mathcal{I}}_\chi = i' \mid \mathbf{H}_\chi\right) \equiv \tilde{\epsilon}_\chi, \quad (31)$$

where $n_{i,i'}$ is the number of bits between the constellation vectors representing spatial symbols for $\mathcal{I} = i$, $\widehat{\mathcal{I}}_\chi = i'$. $\text{Prob}\left(\mathcal{I} = i \rightarrow \widehat{\mathcal{I}}_\chi = i'\right)$ denotes the average per symbol pairwise error probability (PEP) of deciding on $\widehat{\mathcal{I}}_\chi = i'$ when $\mathcal{I} = i$ is chosen for transmission and $\mathbf{H}_\chi$ represents a fixed channel matrix between source. The well-known conditional PEP (CPEP) expression for the observation models in (20)-(21) are given as

$$\begin{aligned}\text{Prob}\left(\mathcal{I}=i\rightarrow\widehat{\mathcal{I}}_{\text{B}}=i' \mid \mathbf{H}_{\text{B}}\right) &= Q\left(\sqrt{\frac{d^2_{\text{B}}(i,i')}{4\sigma^2_{\text{B}}}}\right), \\ \text{Prob}\left(\mathcal{I}=i\rightarrow\widehat{\mathcal{I}}_{\text{E}}=i' \mid \mathbf{H}_{\text{E}}\right) &= Q\left(\sqrt{\frac{d^2_{\text{E}}(i,i')}{4\sigma^2_{\text{E}}}}\right),\end{aligned} \quad (32)$$

where $d^2_{\text{B}}(i,i') \triangleq \rho^2 \parallel \mathbf{v}_{I=i} - \mathbf{v}_{I=i'} \parallel^2_F$ and $Q(x) \triangleq \int_x^\infty (1/\sqrt{2\pi})\exp(-t^2/2)dt$.

Finally, taking into account that $\epsilon_{\text{B}} = \tilde{\epsilon}_{\text{B}} + \delta_{\text{B}}$ and $\epsilon_{\text{E}} = \tilde{\epsilon}_{\text{E}} + \delta_{\text{E}}$, for some $\delta_{\text{B}}, \delta_{\text{E}} \ll 0.5$, the secrecy capacity in (28) can be expressed as

$$\begin{aligned}\mathbb{C}_{\text{GSSK}} \approx L\Big(&\tilde{\epsilon}_{\text{B}}\log_2\tilde{\epsilon}_{\text{B}} + (1-\tilde{\epsilon}_{\text{B}})\log_2(1-\tilde{\epsilon}_{\text{B}}) \\ &- \tilde{\epsilon}_{\text{E}}\log_2\tilde{\epsilon}_{\text{E}} - (1-\tilde{\epsilon}_{\text{E}})\log_2(1-\tilde{\epsilon}_{\text{E}})\Big).\end{aligned} \quad (33)$$

A. Bounds on the Achievable Secrecy Capacity

Since it is difficult to obtain closed-form solutions analytically for the channel capacities $\mathbb{C}_\chi$, when the ML detection scheme in (25) is used, as mentioned earlier, we now drive thigh upper and lower bounds for the achievable secrecy capacity for the optical physical layer security system based on GSSK modulation. From the observation equations (20)-(21), lower and upper bounds on the secrecy capacity of GSSK-OWC systems can be obtained as

$$C_{\text{GSSK}} \leq \frac{N_{\text{r}}}{2}\log_2\left(\frac{\det\left(\mathbb{C}_{\mathbf{w}}\right)^{(1/N_{\text{r}})}}{\sigma^2_{\text{B}}}\right) - \zeta_{\text{U}}, \quad (34)$$

$$C_{\text{GSSK}} \geq \frac{N_{\text{r}}}{2}\log_2\left(\frac{\det\left(\mathbb{C}_{\mathbf{w}}\right)^{(1/N_{\text{r}})}}{\sigma^2_{\text{B}}}\right) - \zeta_{\text{L}}, \quad (35)$$

where

$$\zeta_{\text{L}} = \frac{N_{\text{r}}}{2}\log_2\left(1 + \frac{\det\left(\mathbb{C}_{\mathbf{w}} - \sigma^2_{\text{B}}\mathbb{I}_{N_{\text{r}}}\right)^{(1/N_{\text{r}})}}{\sigma^2_{\text{B}}K^{(2/N_{\text{r}})}}\right), \quad (36)$$

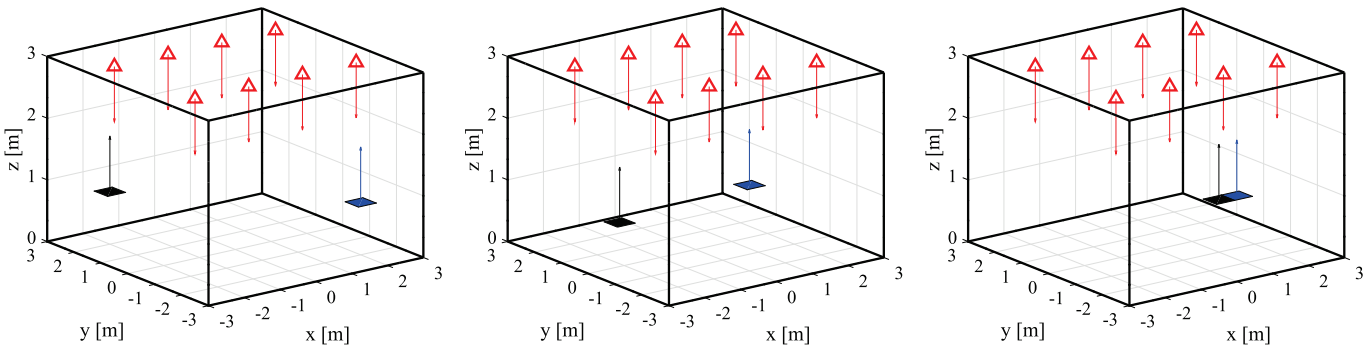
$$\begin{aligned}\zeta_{\text{U}} = &\frac{N_{\text{r}}}{2}\log_2\left(\frac{\exp(1)\det\left(\mathbb{D}_{\mathbf{w}}\right)^{(1/N_{\text{r}})}}{2\sigma^2_{\text{B}}}\right) - \log_2(K) \\ &+ \log_2\left(1 + (K-1)\exp\left(-\frac{\rho^2}{4\sigma^2_{\text{B}}}d^2_{\min}\right)\right),\end{aligned} \quad (37)$$

where $\mathbb{D}_{\mathbf{w}} = \text{diag}(\mathbb{C}_{\mathbf{w}})$. Derivations of the upper and lower bounds are provided in the Appendix.

V. Simulation Results

In this section, comparative secrecy performance evaluation for the proposed SCD based GSSK technique is provided in different indoor LiFi transmission scenarios. Accordingly, Monte-Carlo computer simulations for BER as a function of electrical SNR is provided under both legitimate user's and eavesdropper's mobility. In simulations, a typical 6 m × 6 m × 3 m room is considered with 8 LEDs which are located at the ceiling of the room. The LEDs are assumed to be uniformly distributed over the ceiling with their locations given by $\text{LED}_{\text{location}}$, as shown at the bottom of the next page.

It is assumed that each LED radiates 1 W of optical power and has the half-power semi-angle of $\Phi_{1/2} = 60^{\text{o}}$. The channel gain of users is obtained by (5) where the semi-angle of the FoV and the physical area of each PD are chosen as $\Psi_{1/2} = 70^{\text{o}}$ and $A_{\text{PD}} = 1\ \text{cm}^2$, respectively. Several simulation setups are considered to investigate the performance of different transmission techniques such as the proposed



(a) Bob: $[-2, 2, 0.85]$, Eve: $[2, -2, 0.85]$ (b) Bob: $[-2.5, -0.5, 0.85]$, Eve: $[1.5, 0, 0.85]$ (c) Bob: $[1, -1, 0.85]$, Eve: $[1.5, -1, 0.85]$

Fig. 5. Room layout and mobile user locations for (a) Scenario 1, (b) Scenario 2 and (c) Scenario 3. Red triangles represent location of the LEDss; black and blue squares are Bob and Eve's location, respectively. Orientation of objects is shown by the arrows.

GSSK versus SSK and the different locations of Bob and Eve, as depicted in Fig. 5. The idea of considering the different locations of Bob and Eve shown in Fig. 5, named scenario in this manuscript, can be explained as follows. In scenario 1, Bob and Eve are located at different corners of the room. Due to their location, it can be said that Bob and Eve will have spatially separated channel gains from the transmit elements and their channel gains will be different. In scenario 2, Bob is located around one edge of the room and slightly centred along the y-axis; and Eve is located at the centre of the y-axis. Therefore, it can be expected that Bob's channel coefficients will be slightly similar for spatially distributed transmitters and Eve's channel coefficients will have a spatial similarity for half of the transmitters, where half of the transmitters will have the same channel gain for Eve. However, as in scenario 1, Bob's and Eve's channels will not be similar to each other. In scenario 3, Bob and Eve are located 0.5 m away from each other. Thus, Bob and Eve will have similar channel gains. Also, due to their location which is off the centre of both x- and y-axes, the channel gain of the transmit elements will be spatially separated.

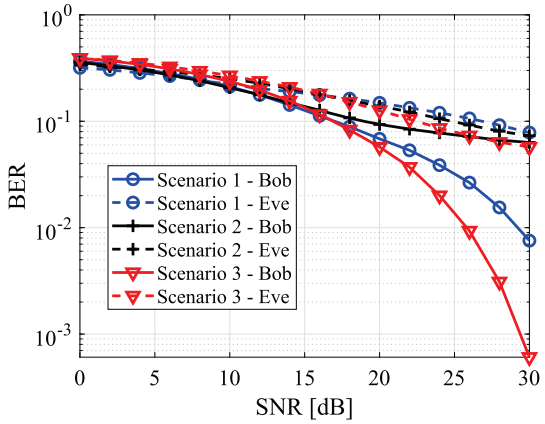


Fig. 6. BER performance of SSK transmission for Bob and Eve ($N_{\mathrm{t}} = 8$ and $N_{\mathrm{a}} = 1$).

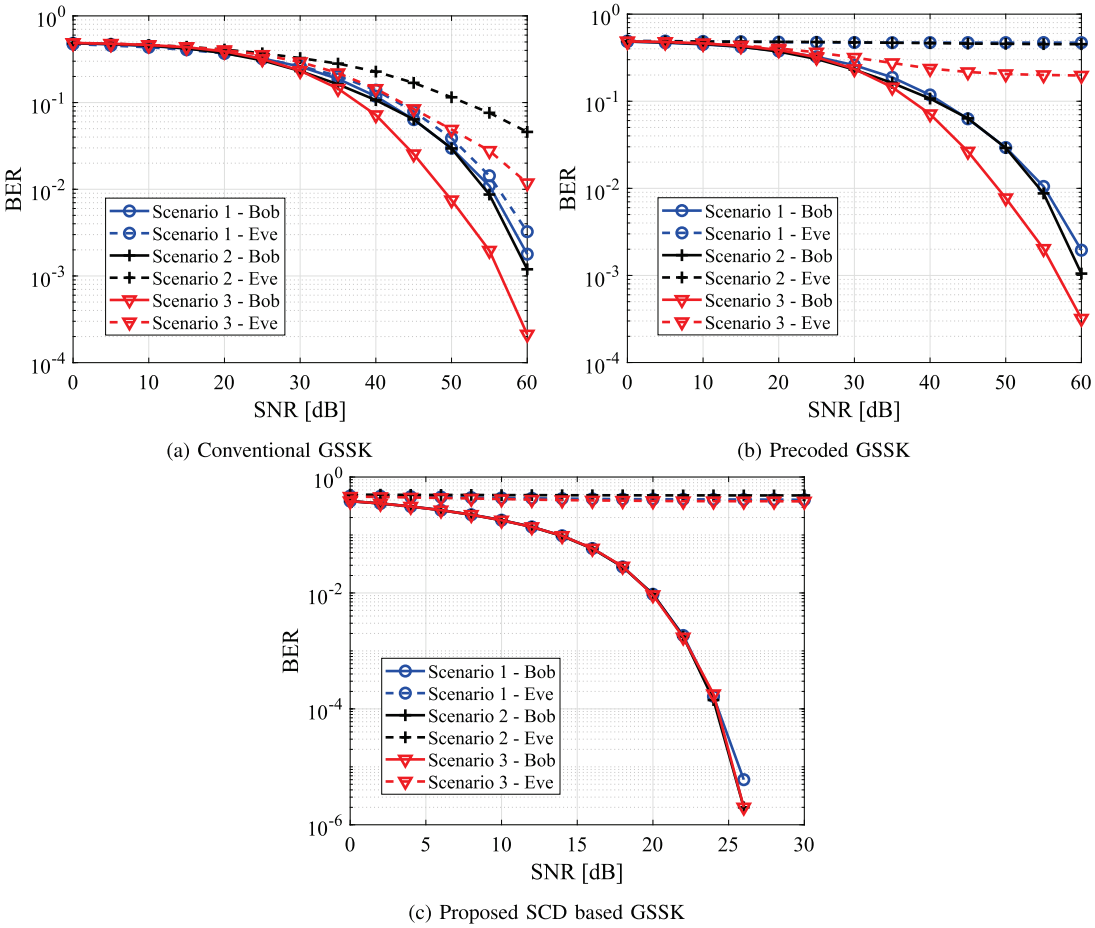
A. SSK With a Single PD

It is assumed that communication is realized by a conventional SSK scheme with $N_{\mathrm{a}} = 1$ and a single PD is employed at the receiver units. Different positions for the legitimate user and eavesdropper are considered, as shown in Fig. 5. The average BER performance of the scenarios is shown in Fig. 6. As it can be seen from the plots, the BER performance of the legitimate user outperforms the eavesdropper for scenarios 1 and 3. While the BER performance of Bob reaches 10^{-2} and 10^{-3} at an SNR value of 30 dB for scenarios 1 and 3, respectively, Eve's performance cannot exceed 8×10^{-2}. However, when scenario 2 is considered, the BER performance of the legitimate user and eavesdropper is around 7×10^{-2} for an SNR value of 30 dB. Due to the position of the users, the channel gain of half of the transmit elements is symmetric to the other half. Therefore, such a low BER performance is achieved for scenario 2 for both users.

B. GSSK With Multiple PDs ($N_{\mathrm{a}} > 1$)

It is assumed that the proposed GSSK scheme is used with $N_{\mathrm{t}} = 8$, $N_{\mathrm{a}} = 3$ and the receivers are equipped with 2 PDs ($N_{\mathrm{r}} = 2$) which are positioned at a height of 0.85 m and separated by a distance of 3 cm. The same scenarios depicted in Fig. 5 are considered for the different locations of Bob and Eve. Fig. 7 shows the BER performance of Bob and Eve for the conventional, precoded and proposed GSSK schemes. On the one hand, channel similarities among different transmit elements affect the BER performance of the conventional and precoded GSSK schemes as shown in Figs. 7(a) and 7(b). Moreover, the difference between the BER performance of the legitimate user and eavesdropper is explained by the channel similarities between Bob and Eve. For a 50 dB SNR,

$$\mathrm{LED}_{\mathrm{location}}\,(x, y) = \begin{bmatrix} -2.25 & -0.75 & 0.75 & 2.25 & -2.25 & -0.75 & 0.75 & 2.25 \\ 1.5 & 1.5 & 1.5 & 1.5 & -1.5 & -1.5 & -1.5 & -1.5 \end{bmatrix}^{\mathrm{T}}$$



(a) Conventional GSSK

(b) Precoded GSSK

(c) Proposed SCD based GSSK

Fig. 7. BER versus electrical SNR performance of Bob and Eve for the (a) conventional, (b) precoded and (c) proposed GSSK schemes under three considered scenarios ($N_{\mathrm{t}} = 8$, $N_{\mathrm{a}} = 3$ and $N_{\mathrm{r}} = 2$).

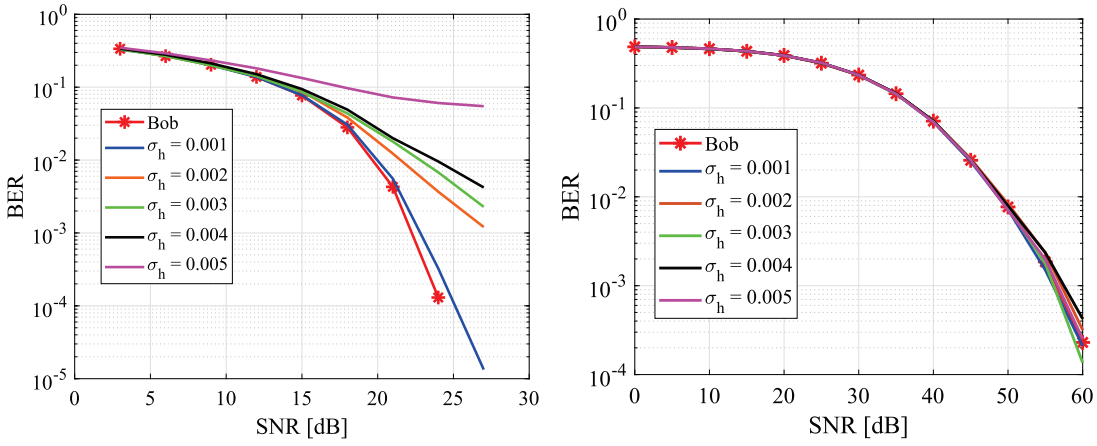
Bob and Eve achieve a BER of 5×10^{-3} and 2×10^{-2} for scenario 3, respectively. For the precoded GSSK scheme, although a similar BER performance of the legitimate user is observed for a 50 dB SNR, the BER performance of the eavesdropper is worsen, around 0.2 for scenario 3 and 0.5 for scenarios 1 and 2. On the other hand, as shown in Fig. 7(c), the proposed GSSK scheme achieves a BER of 10^{-3} at 22 dB SNR level for the legitimate user for all the considered locations, irrespective of channel similarities among different transmit elements. Whereas, the BER performance of the eavesdropper is around 0.5, irrespective of the considered SNR levels. In other words, even the eavesdropper has a spatially separated channel gain and/or a similar channel gain with Bob, he/she cannot obtain the information sent to Bob. Hence, it can be said that the proposed GSSK provides (i) a secure transmission to the legitimate user; and (ii) mitigates the effect of channel similarities on the BER performance.

In order to understand the effect of channel similarities of Bob and Eve on the BER performance of the proposed GSSK system, Eve's channel is generated as follows:

$$\mathbf{H}_{\mathrm{E}} = \mathbf{H}_{\mathrm{B}} + \mathbf{c} \circ \mathbf{H}_{\mathrm{B}}, \tag{38}$$

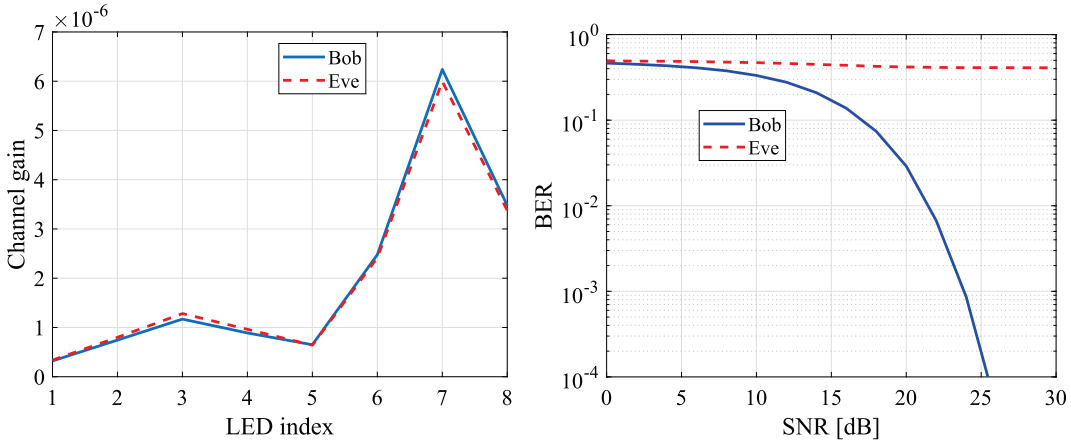
where $\mathbf{c} \in \mathbb{R}^{N_{\mathrm{a}} \times 1}$ is a vector such that its elements are random variables with zero mean and σ_h standard deviation. In Fig. 8, the BER performances of Bob and Eve are given when different σ_h values are used to generate Eve's channel. When Bob and Eve have very similar channel gains, which is the case $\sigma_h = 0.001$, the BER performance of both users are similar for both the precoded and proposed GSSK schemes. This means that information sent to Bob can be understood by Eve. Therefore, the PLS of the system is low in this case. When the proposed GSSK scheme is used, a slight change in the channel gains of both users results in substantial BER performance differences as shown in Fig. 8(a). However, this is not the case for the precoded GSSK scheme as shown in Fig. 8(b).

In terms of physical location based channel similarities, Fig. 9 shows the channel gain and BER performance of Bob and Eve when they are located 10 cm apart. As it can be seen from Fig. 9(a), the channel gain of both users are almost the same. However, the BER performance of Eve is around 0.5 as shown in Fig. 9(b). In other words, Eve cannot understand what is sent to Bob for the given SNR range. In order to understand the BER performance of Eve throughout the room, Bob is located at point $[-1, 1, 0.85]$ and Eve is located on circles with different radius around Bob. As shown in Fig. 10,



(a) Proposed SCD based GSSK. (b) Precoded GSSK.

Fig. 8. The BER versus SNR performances of Bob and Eve for the (a) proposed and (b) precoded GSSK when the channel gains of Eve is obtained by (38).



(a) Channel gain. (b) BER performance.

Fig. 9. The (a) channel gain and (b) BER performance of the proposed GSSK for $N_t = 8$, $N_r = 3$, $N_a = 3$ when Bob is located at point $[-1.06, 0.95, 0.85]$ and Eve is located at point $[-0.96, 0.95, 0.85]$.

the BER of Eve is low when Eve's location is exactly the same as Bob's and the BER performance is around 0.5 at the rest of the room. Therefore, it can be said that the proposed GSSK scheme provides a robust PLS for LiFi systems.

In order to investigate the effect of Bob and Eve's mobility on the PLS, a 6 m $\times$ 6 m floor plane with $+0.85$ m offset in z-axis is divided into 601×601 uniformly separated square grid. Thus, 361201 different channel realizations are obtained with respect to the user locations. The overall BER versus SNR performance curves of both Bob and Eve for the proposed system are plotted by randomly chosen user locations within the given room in Fig. 11. As can be seen from the Fig. 11, the BER values of Bob and Eve are averaged over their random channel realizations which corresponds to their 2D locations. Thus, the average secrecy performance of the proposed system under the user mobility model is obtained.

Fig. 12 shows upper and lower bounds on the achievable secrecy capacity computed from equations (34) and (35), as well as the exact secrecy capacity obtained analytically from (33). Scenario 3 given in Fig. 5 is considered for the location of Bob and Eve. As can be seen from Fig. 12, the bounds are quite tight, especially at the low SNR region.

In Fig. 13, the proposed GSSK scheme is compared with an M-ary PAM signalling. M-ary PAM signals are superimposed over a DC bias so that transmission of positive-valued light intensity is satisfied and the required illumination level is achieved. In each signalling interval, an LED at the transmitter is randomly chosen from the set of available light fixtures and a M-PAM symbol transmitted by this LED to Bob and Eve carrying $\log_2(M)$ bits/symbol. A target value of 4 bits/sec/Hz transmission, $N_t = 8$, $N_r = 2$ and $N_a = 2$ is considered. Hence, the proposed GSSK system generates the effective channel column vectors of Bob's channel, $\tilde{\mathbf{H}}_{k,\mathrm{B}}$, which are on the corners of an 16-ary extended signal constellation, carrying 4 bits/symbol. Gray mapping is employed for both constellations. $M = 16$ is also chosen for the M-PAM constellation to have the same spectral efficiency of 4 bits/sec/Hz. At the receivers of Bob and Eve, the ML is applied to detect M-PAM and GSSK modulated data. The plots in Fig. 13 show that using the M-PAM signalling scheme is not suitable to achieve

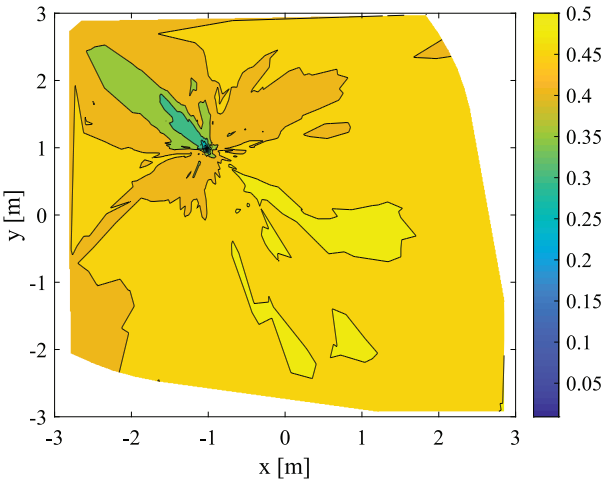


Fig. 10. BER performance of the proposed GSSK while Eve is mobile within the room and Bob is located at point $(-1, 1, 0.85)$. Eve is located on circles with different radius around Bob and Eve's location is not considered in white areas in the figure.

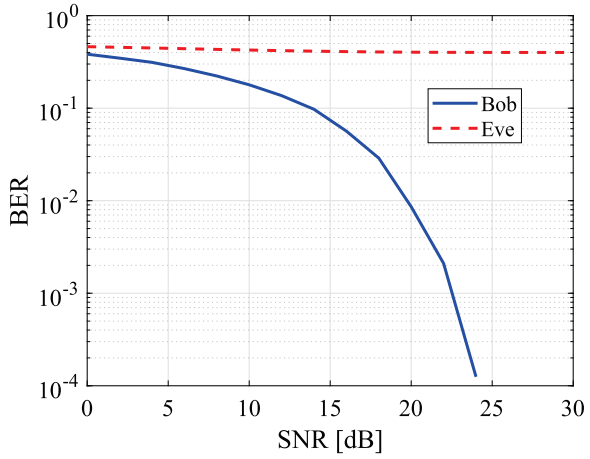


Fig. 11. Average BER performance of Bob and Eve when they are located randomly in the room.

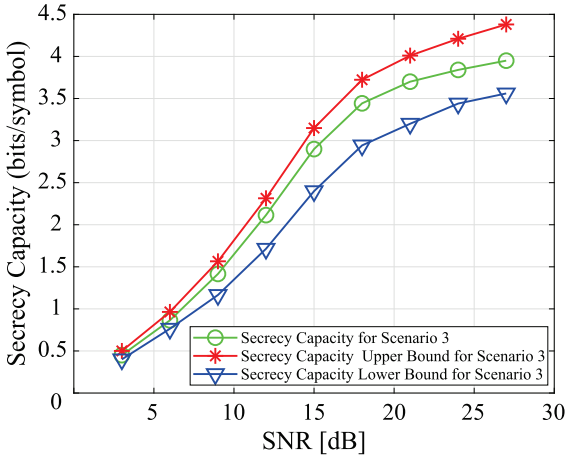


Fig. 12. Secrecy capacity of the proposed GSSK scheme.

PLS in LiFi systems. The BER performance of Bob and Eve is comparable to each other unless additional precautions, such as utilizing beam-forming by Bob and/or jamming Eve's reception by a jamming signal, are taken.

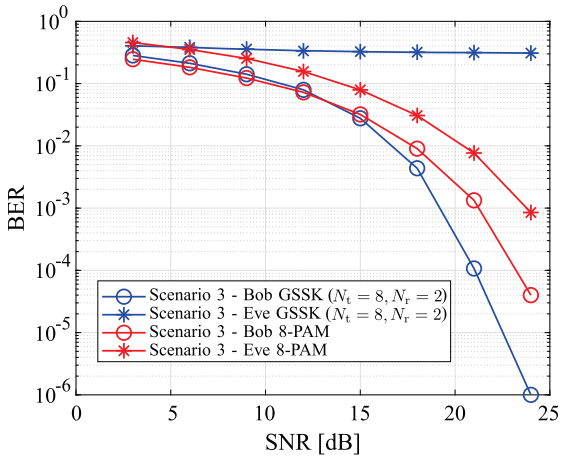


Fig. 13. Performance comparison of the proposed GSSK and PAM signalling schemes.

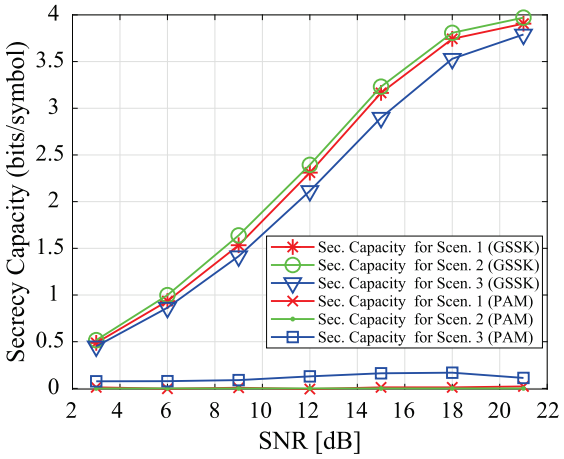


Fig. 14. Secrecy capacity performance of the proposed GSSK and M-PAM schemes.

In order to support the noted observations, the achieved secrecy capacity is also obtained for GSSK and M-PAM schemes. As can be seen from Fig. 14, the secrecy capacity of the proposed GSSK scheme for each scenario given in Fig. 5 reaches the maximum achievable capacity of 4 bits/symbol. However, the secrecy capacity of the M-PAM scheme is almost zero and hence it is not desirable for PLS.

VI. Conclusion

In this paper, a novel physical security technique has been proposed for indoor LiFi systems. The proposed MIMO-GSSK based technique designs spatial constellations to maximize the minimum Euclidean distance of the transmit symbol set with the aid of CSIT of the legitimate user. The proposed technique also employs ZFP to mitigate ICI such that the transmit symbol set becomes the received symbol set for the legitimate user, whereas for an eavesdropper, the proposed technique introduces a natural jamming signal. It has been shown by computer simulations that the proposed technique effectively provides secure information transmission to the legitimate user and prohibits the successful reception of the same information by an eavesdropper in a reliable way. Closed

form expressions for upper and lower bounds as well as an approximate expression on the proposed GSSK secrecy capacity have been derived.

APPENDIX
DERIVATIONS OF UPPER AND LOWER BOUNDS

A. Derivation of Upper Bound

The secrecy capacity of the MIMO wiretap channel of the GSSK scheme in (20) and (21) is achieved when the discrete input random variable $\mathcal{I}$, taking values in $\{1, 2, \cdots, K\}$, is equally likely. Thus, the secrecy capacity can be found from

$$\begin{aligned} C_{\text{GSSK}} &= \mathbb{I}\left(\mathbf{s}_{\text{B}}; \mathbf{y}_{\text{B}}\right) - \mathbb{I}\left(\mathbf{s}_{\text{B}}; \mathbf{y}_{\text{E}}\right) \\ &= \mathbb{H}\left(\mathbf{y}_{\text{B}}\right) - \mathbb{H}\left(\mathbf{y}_{\text{B}}|\mathbf{s}_{\text{B}}\right) - \left(\mathbb{H}\left(\mathbf{y}_{\text{E}}\right) - \mathbb{H}\left(\mathbf{y}_{\text{E}}|\mathbf{s}_{\text{B}}\right)\right) \\ &= \frac{N_{\text{r}}}{2}\log_2\left(\frac{|\mathbb{C}_{\mathbf{w}}|^{1/N_{\text{r}}}}{\sigma_{\text{B}}^2}\right) - \left(\mathbb{H}\left(\mathbf{y}_{\text{E}}\right) - \mathbb{H}(\mathbf{y}_{\text{B}})\right), \end{aligned} \tag{39}$$

where $\mathbb{H}(\cdot)$ and $\mathbb{H}(\cdot|\cdot)$ represent the differential and conditional entropy, respectively. We can now apply the entropy power inequality (EPI) to $\mathbb{H}\left(\mathbf{y}_{\text{E}}\right)$ as follows. Since Bob's channel is less noisy than Eve's channel, Eve's noise vector $\mathbf{w}$ in (23) can be expressed as $\mathbf{w} = \mathbf{w}_{\text{B}} + \mathbf{n}$, for some zero-mean Gaussian vector $\mathbf{n}$ with covariance matrix $\mathbb{C}_{\mathbf{n}} = \mathbb{C}_{\mathbf{w}} - \sigma_{\text{B}}^2\mathbf{I}_{N_{\text{r}}}$. Then, by the EPI for $\mathbf{y}_{\text{B}}$ yields

$$\begin{aligned} &\mathbb{H}\left(\mathbf{y}_{\text{E}}\right) - \mathbb{H}\left(\mathbf{y}_{\text{B}}\right) = \mathbb{H}\left(\mathbf{y}_{\text{B}} + \mathbf{n}\right) - \mathbb{H}\left(\mathbf{y}_{\text{B}}\right) \\ &\quad\geq \frac{N_{\text{r}}}{2}\log_2\left(2^{(2/N_{\text{r}})\mathbb{H}(\mathbf{n})} + 2^{(2/N_{\text{r}})\mathbb{H}(\mathbf{y}_{\text{B}})}\right) - \mathbb{H}\left(\mathbf{y}_{\text{B}}\right) \\ &\quad= \frac{N_r}{2}\log_2\left(2\pi e|\mathbb{C}_n|^{1/N_{\text{r}}} + 2^{(2/N_{\text{r}})\mathbb{H}(\mathbf{y}_{\text{B}})}\right) - \mathbb{H}\left(\mathbf{y}_{\text{B}}\right). \end{aligned}$$

Please note that $f(u) = \frac{1}{2}\log_2(A + 2^{(2/N_{\text{r}})u}) - u$ is monotonically decreasing function of u [49] for $A \geq 0$, and

$$\begin{aligned} \mathbb{H}\left(\mathbf{y}_{\text{B}}\right) &\leq \log_2(K) + \frac{N_{\text{r}}}{2}\log_2\left(2\pi e\sigma_{\text{B}}^2\right) \\ &= \frac{N_{\text{r}}}{2}\log_2\left(2\pi e\sigma_{\text{B}}^2 K^{2/N_{\text{r}}}\right). \end{aligned}$$

Thus, the final upper bound is obtained as

$$C_{\text{GSSK}} \leq \frac{N_{\text{r}}}{2}\log_2\left(\frac{|\mathbb{C}_{\mathbf{w}}|^{1/N_{\text{r}}}}{\sigma_{\text{B}}^2}\right) - \zeta_{\text{L}},$$

where

$$\zeta_{\text{L}} = \frac{N_r}{2}\log_2\left(1 + \frac{|\mathbb{C}_{\mathbf{n}}|^{1/N_r}}{\sigma_{\text{B}}^2 K^{2/N_r}}\right).$$

B. Derivation of Lower Bound

The secrecy capacity of the MIMO wiretap channel of the GSSK scheme in (20) and (21) can be lower bounded as follow: From (39) it follows that

$$C_{\text{GSSK}} \geq \frac{N_{\text{r}}}{2}\log_2\left(\frac{|\mathbb{C}_{\mathbf{w}}|^{1/N_{\text{r}}}}{\sigma_{\text{B}}^2}\right) - \left(\mathbb{H}_{\text{U}}\left(\mathbf{y}_{\text{E}}\right) - \mathbb{H}_{\text{L}}(\mathbf{y}_{\text{B}})\right), \tag{40}$$

where $\mathbb{H}\left(\mathbf{y}_{\text{E}}\right) \leq \mathbb{H}_{\text{U}}\left(\mathbf{y}_{\text{E}}\right)$ and $\mathbb{H}\left(\mathbf{y}_{\text{B}}\right) \geq \mathbb{H}_{\text{L}}\left(\mathbf{y}_{\text{B}}\right)$.

By the entropy properties that translation does not change the entropy and that a continuous Gaussian random vector with independent components yields maximum entropy, it follows from (20) that

$$\mathbb{H}\left(\mathbf{y}_{\text{E}}\right) \leq \mathbb{H}_{\text{U}}\left(\mathbf{y}_{\text{E}}\right) = \frac{N_{\text{r}}}{2}\log_2\left(2\pi e|\mathbb{D}_{\mathbf{w}}|^{1/N_{\text{r}}}\right), \tag{41}$$

where $\mathbb{D}_{\mathbf{w}} = \text{diag}\left(\mathbb{C}_{\mathbf{w}}\right)$.

On the other hand, by using Jensen's inequality $\mathbb{E}\{-\log p(U)\} \geq -\log\left(\mathbb{E}\{p(U)\}\right)$, the differential entropy $\mathbb{H}\left(\mathbf{y}_{\text{B}}\right)$ can be lower bounded as

$$\mathbb{H}\left(\mathbf{y}_{\text{B}}\right) \geq \mathbb{H}_{\text{L}}\left(\mathbf{y}_{\text{B}}\right) = -\log_2\int p^2\left(\mathbf{y}_{\text{B}}\right)d\mathbf{y}_{\text{B}}. \tag{42}$$

Since the discrete LED indexes are selected equally likely with the probability $1/K$, the probability density function (PDF) of $\mathbf{y}_{\text{B}}$ is a Gaussian mixture given by

$$\begin{aligned} p(\mathbf{y}_{\text{B}}) &= \sum_{i=1}^{K} p(\mathbf{y}_{\text{B}}|\mathcal{I}=i)P(\mathcal{I}=i) \\ &= \frac{1}{K}\sum_{i=1}^{K}\frac{1}{(2\pi\sigma_{\text{B}}^2)^{2/N_{\text{r}}}}\exp\left(-\frac{1}{2\sigma_{\text{B}}^2}||(\mathbf{y}_{\text{B}} - \mathbf{s}_{\text{B}}(i)||^2\right), \end{aligned} \tag{43}$$

where $\mathbf{s}_{\text{B}}(i) = \rho\mathbf{v}_i$. Performing the integration in (42) after substituting (43) yields,

$$\begin{aligned} &\mathbb{H}_{\text{L}}\left(\mathbf{y}_{\text{B}}\right) \\ &= \log_2(K) + \frac{N_r}{2}\log_2(4\pi\sigma_{\text{B}}^2) \\ &\quad - \log_2\left(1 + \frac{1}{K}\sum_{i=1}^{K}\sum_{\substack{i'=1\\ i'\neq i}}^{K}\exp\left(-\frac{1}{4\sigma_{\text{B}}^2}\parallel \mathbf{s}_{\text{B}}(i) - \mathbf{s}_{\text{B}}(i')\parallel^2\right)\right) \\ &= \log_2(K) + \frac{N_{\text{r}}}{2}\log_2(4\pi\sigma_{\text{B}}^2) \\ &\quad - \log_2\left(1 + \frac{1}{K}\sum_{i=1}^{K}\sum_{\substack{i'=1\\ i'\neq i}}^{K}\exp\left(-\frac{\rho^2}{4\sigma_{\text{B}}^2}\parallel d(i,i')\parallel^2\right)\right) \\ &\geq \log_2(K) + \frac{N_{\text{r}}}{2}\log_2(4\pi\sigma_{\text{B}}^2) \\ &\quad - \log_2\left(1 + (K-1)\exp\left(-\frac{\rho^2}{4\sigma_{\text{B}}^2}d_{\min}^2\right)\right). \end{aligned} \tag{44}$$

Note that, $d(i,i')$ in the fourth line of the equation above is the Euclidean distance between any two distinct points in the constellation points having minimum distance $d_{\min}$. The inequality above follows since $d_{\min} \leq d(i,i')$, for all i and i', $(i \neq i')$.

Finally, by substituting (41) and (44) in (40), we obtain the lower bound as

$$C_{\text{GSSK}} \geq \frac{N_{\text{r}}}{2}\log_2\left(\frac{|\mathbb{C}_{\mathbf{w}}|^{1/N_{\text{r}}}}{\sigma_{\text{B}}^2}\right) - \zeta_{\text{U}},$$

where

$$\begin{aligned} \zeta_{\text{U}} = &\frac{N_{\text{r}}}{2}\log_2\left(\frac{\exp(1)\,|\mathbb{D}_{\mathbf{w}}|^{1/N_{\text{r}}}}{2\sigma_{\text{B}}^2}\right) \\ &- \log_2(K) + \log_2\left(1 + (K-1)\exp\left(-\frac{\rho^2}{4\sigma_{\text{B}}^2}d_{\min}^2\right)\right). \end{aligned}$$

REFERENCES

[1] I. Stefan, H. Burchardt, and H. Haas, "Area spectral efficiency performance comparison between VLC and RF femtocell networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 3825–3829.

[2] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?" *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, Mar. 15, 2016.

[3] S. Cho, G. Chen, and J. P. Coon, "Physical layer security in visible light communication systems with randomly located colluding eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 768–771, Oct. 2018.

[4] A. Arafa, E. Panayirci, and H. V. Poor, "Relay-aided secure broadcasting for visible light communications," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 4227–4239, Jun. 2019.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[7] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] A. Nuwanpriya, S.-W. Ho, and C. S. Chen, "Indoor MIMO visible light communications: Novel angle diversity receivers for mobile users," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1780–1792, Sep. 2015.

[9] S. Sugiura and H. Iizuka, "Element-by-element full-rank optical wireless MIMO systems using narrow-window angular filter designed based on one-dimensional photonic crystal," *J. Lightw. Technol.*, vol. 34, no. 24, pp. 5601–5609, Dec. 15, 2016.

[10] R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2228–2241, Jul. 2008.

[11] M. Di Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, "Spatial modulation for generalized MIMO: Challenges, opportunities, and implementation," *Proc. IEEE*, vol. 102, no. 1, pp. 56–103, Jan. 2014.

[12] Y. A. Chau and S.-H. Yu, "Space modulation on wireless fading channels," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Atlantic City, NJ, USA, vol. 3, Oct. 2001, pp. 1668–1671.

[13] H. Haas, E. Costa, and E. Schulz, "Increasing spectral efficiency by data multiplexing using antenna arrays," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, vol. 2. Lisboa, Portugal: Pavilhao Altantico, Sep. 2002, pp. 610–613.

[14] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Generalized space shift keying modulation for MIMO channels," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Cannes, France, Sep. 2008, pp. 1–5.

[15] L. Yang, "Transmitter preprocessing aided spatial modulation for multiple-input multiple-output systems," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, May 2011, pp. 1–5.

[16] A. Stavridis, S. Sinanovic, M. Di Renzo, and H. Haas, "Transmit precoding for receive spatial modulation using imperfect channel knowledge," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, May 2012, pp. 1–5.

[17] X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2012, pp. 1–4.

[18] R. Zhang, L.-L. Yang, and L. Hanzo, "Generalised pre-coding aided spatial modulation," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5434–5443, Nov. 2013.

[19] X. Guan, Y. Cai, and W. Yang, "On the mutual information and precoding for spatial modulation with finite alphabet," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 383–386, Aug. 2013.

[20] A. Stavridis, D. Basnayaka, S. Sinanovic, M. Di Renzo, and H. Haas, "A virtual MIMO dual-hop architecture based on hybrid spatial modulation," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3161–3179, Sep. 2014.

[21] 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, Apr. 2016.

[22] Y. Chen, L. Wang, Z. Zhao, M. Ma, and B. Jiao, "Secure multiuser MIMO downlink transmission via precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1116–1119, Jun. 2016.

[23] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[24] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1351–1354, Aug. 2015.

[25] Y. Wei, L. Wang, and T. Svensson, "Analysis of secrecy rate against eavesdroppers in MIMO modulation systems," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2015, pp. 1–5.

[26] C. Liu, L.-L. Yang, and W. Wang, "Secure spatial modulation with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 838–841, Dec. 2017.

[27] Z. Huang, Z. Gao, and L. Sun, "Anti-eavesdropping scheme based on quadrature spatial modulation," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 532–535, Mar. 2017.

[28] 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, Sep. 2018.

[29] F. Wang, R. Li, J. Zhang, S. Shi, and C. Liu, "Enhancing the secrecy performance of the spatial modulation aided VLC systems with optical jamming," *Signal Process.*, vol. 157, pp. 288–302, Apr. 2019.

[30] X. Wang, X. Wang, and L. Sun, "Spatial modulation aided physical layer security enhancement for fading wiretap channels," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2016, pp. 1–5.

[31] S. R. Aghdam and T. M. Duman, "Secure space shift keying transmission using dynamic antenna index assignment," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[32] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 877–889, Apr. 2018.

[33] X.-Q. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-enhancing scheme for spatial modulation," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 550–553, Mar. 2018.

[34] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[35] F. Wang *et al.*, "Secrecy analysis of generalized space-shift keying aided visible light communication," *IEEE Access*, vol. 6, pp. 18310–18324, 2018.

[36] J.-Y. Wang, H. Ge, M. Lin, J.-B. Wang, J. Dai, and M.-S. Alouini, "On the secrecy rate of spatial modulation-based indoor visible light communications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 9, pp. 2087–2101, Sep. 2019.

[37] G. Xia, F. Shu, Y. Zhang, J. Wang, S. Ten Brink, and J. Speidel, "Antenna selection method of maximizing secrecy rate for green secure spatial modulation," *IEEE Trans. Green Commun. Netw.*, vol. 3, no. 2, pp. 288–301, Jun. 2019.

[38] F. Wu, C. Dong, L. Yang, and W. Wang, "Secure wireless transmission based on precoding-aided spatial modulation," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[39] F. Wu, L.-L. Yang, W. Wang, and Z. Kong, "Secret precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1544–1547, Sep. 2015.

[40] F. Wu, W. Wang, C. Dong, and L.-L. Yang, "Performance analysis of secret precoding-aided spatial modulation with finite-alphabet signaling," *IEEE Access*, vol. 6, pp. 29366–29381, 2018.

[41] F. Shu, Z. Wang, R. Chen, Y. Wu, and J. Wang, "Two high-performance schemes of transmit antenna selection for secure spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8969–8973, Sep. 2018.

[42] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 2918–2931, May 2018.

[43] C. Chen, D. A. Basnayaka, and H. Haas, "Downlink performance of optical attocell networks," *J. Lightw. Technol.*, vol. 34, no. 1, pp. 137–156, Jan. 1, 2016.

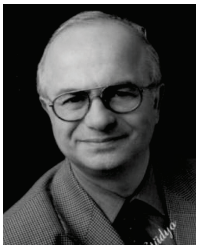
[44] J. M. Kahn and J. R. Barry, "Wireless infrared communications," *Proc. IEEE*, vol. 85, no. 2, pp. 265–298, Feb. 1997.

[45] O. Hassan, E. Panayirci, H. V. Poor, and H. Haas, "Physical-layer security for indoor visible light communications with space shift keying modulation," in *Proc. IEEE Global Telecomm. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[46] A. Yesilkaya, T. Cogalan, E. Panayirci, H. Haas, and H. V. Poor, "Achieving minimum error in MISO optical spatial modulation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[47] T. Q. Wang, R. J. Green, and J. Armstrong, "MIMO optical wireless communications using ACO-OFDM and a prism-array receiver," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1959–1971, Sep. 2015.

[48] R. Zhang, L.-L. Yang, and L. Hanzo, "Error probability and capacity analysis of generalised pre-coding aided spatial modulation," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 364–375, Jan. 2015.
[49] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.

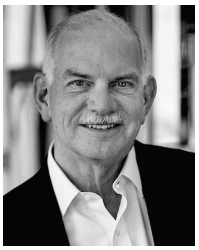


Erdal Panayirci (Life Fellow, IEEE) received the Diploma Engineering degree in electrical engineering from Istanbul Technical University, Istanbul, Turkey, in 1964, and the Ph.D. degree in electrical engineering and system science from Michigan State University, East Lansing, MI, USA, in 1971. From 2008 to 2009 and from 2017 to 2018, he was with the Department of Electrical Engineering, Princeton University. He is currently a Professor of electrical engineering and the Head of the Electrical and Electronics Engineering Department, Kadir Has University, Istanbul, Turkey, and a Visiting Research Collaborator with the Department of Electrical Engineering, Princeton, NJ, USA. He has published extensively in leading scientific journals and international conference and co-authored the book *Principles of Integrated Maritime Surveillance Systems* (Kluwer Academic, 2000). His research interests include communication theory, synchronization, advanced signal processing techniques and their applications to wireless electrical, underwater, and optical communications.

Dr. Panayirci was an Editor of IEEE TRANSACTIONS ON COMMUNICATIONS in the areas of Synchronization and Equalization from 1995 to 2000. He served and is currently serving as a member for IEEE Fellow Committee from 2005 to 2008 and from 2018 to 2020, respectively. He is currently a member of the IEEE GLOBECOM/ICC Management and Strategy Standing Committee. He was the Technical Program Co-Chair of the IEEE International Conference on Communications (ICC2006) and the Technical Program Chair of the IEEE PIMRC, both held in Istanbul in 2006 and 2010, respectively. He was the Executive Vice Chairman of the IEEE Wireless Communications and Networking Conference, Istanbul, Turkey, in April 2014. He was the General Co-Chair of the IEEE PIMRC, Istanbul, Turkey, in September 2019.

Anil Yesilkaya (Student Member, IEEE) received the B.Sc. (Hons.) and M.Sc. degrees in electronics engineering from Kadir Has University, Istanbul, Turkey, in 2014 and 2016, respectively. He is currently pursuing the Ph.D. degree in digital communications with The University of Edinburgh. His research interests include multiple-input multiple-output optical wireless communications (MIMO-OWC) and LiFi-based in-flight connectivity. He was a recipient of the Best Paper Award at the IEEE International Conference on Communications (ICC) in 2018.

Tezcan Cogalan (Member, IEEE) received the B.Sc. and M.Sc. degrees in electronics engineering from Kadir Has University (KHU), Istanbul, Turkey, in 2011 and 2013, respectively, and the Ph.D. degree in digital communications from The University of Edinburgh, U.K., in 2018. He is currently a Post-Doctoral Research Associate with the LiFi Research and Development Centre, The University of Edinburgh. His research interests include interference analysis, radio resource management and optimization of wireless communication (both radio frequency and optical) systems for user dense environments. He was a co-recipient of the recent Best Paper Award at ICC 2018.



H. Vincent Poor (Life Fellow, IEEE) received the Ph.D. degree in electrical engineering and computer science from Princeton University in 1977. From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana–Champaign. Since 1990, he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor of Electrical Engineering. During 2006 to 2016, he served as the Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other institutions, most recently at Berkeley and Cambridge. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a Foreign Member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, the 2019 ASEE Benjamin Garver Lamme Award, a D.Sc. *honoris causa* from Syracuse University, conferred in 2017, and a D. Eng. *honoris causa* from the University of Waterloo, conferred in 2019.

Harald Haas (Fellow, IEEE) received the Ph.D. degree from The University of Edinburgh in 2001. He is currently the Chair of mobile communications with The University of Edinburgh. He is also the Initiator, a Co-Founder, and a Chief Scientific Officer of pureLiFi Ltd., and the Director of the LiFi Research and Development Centre, The University of Edinburgh. He has authored 500 conference and journal articles. His main research interests are in optical wireless communications, hybrid optical wireless and RF communications, spatial modulation, and interference coordination in wireless networks.

Dr. Haas gave two TED Global talks "Wireless Data From Every light Bulb" and "Forget Wi-Fi: Meet the New Li-Fi Internet" which together have been downloaded more than 5.5 million times. He is a fellow of the Royal Academy of Engineering. In 2012 and 2017, he was a recipient of the prestigious Established Career Fellowship from the Engineering and Physical Sciences Research Council (EPSRC) in the U.K. In 2014, he was selected by EPSRC as one of ten Recognizing Inspirational Scientists and Engineers Leaders in the U.K. He was a co-recipient of the EURASIP Best Paper Award for the *Journal on Wireless Communications and Networking* in 2015 and the Jack Neubauer Memorial Award of the IEEE Vehicular Technology Society. In 2016, he received the Outstanding Achievement Award from the International Solid State Lighting Alliance. He was a co-recipient of recent best paper awards at VTC-Fall, 2013, VTC-Spring 2015, ICC 2016, ICC 2017, and ICC 2018. In 2019, he received the James Evans Avant Garde Award of the IEEE Vehicular Technology Society. He is an Associate Editor of the IEEE JOURNAL OF LIGHTWAVE TECHNOLOGIES.