Secrecy Analysis of Generalized Space-Shift Keying Aided Visible Light Communication

Fasong Wang, Chaowen Liu, Qi Wang, Jiankang Zhang, Rong Zhang, *Senior Member, IEEE*, Lie-Liang Yang, *Fellow, IEEE*, and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—This paper investigates the physical layer security (PLS) problem of visible light communication (VLC) systems relying on generalized space-shift keying (GSSK) termed as GSSK-VLC. The GSSK-VLC system considered is assumed to be comprised of three nodes: a transmitter equipped with multiple light-emitting diodes (LEDs), a legitimate receiver as well as a passive eavesdropper. Each of them is equipped with a single photo-detector (PD). Specifically, the average mutual information (AMI) of a GSSK-VLC system is derived. We also obtain both a lower bound and an accurate closed-form expression of the approximate AMI, which can be employed for efficiently estimating the achievable secrecy rate of GSSK-VLC systems. Furthermore, the pairwise error probability (PEP) and bit error rate (BER) of GSSK-VLC systems are analyzed, and again some closed-form expressions are obtained. Additionally, in order to enhance the secrecy performance of the GSSK-VLC system, an optimal LED pattern selection algorithm is proposed under the minimax criterion. We show that the proposed LED pattern selection algorithm is capable of enhancing both the AMI between the transmitter and legitimate user as well as the achievable secrecy rate of the GSSK-VLC system.**

***Index Terms*—Generalized space-shift keying (GSSK), visible light communication (VLC), physical layer security (PLS), secrecy rate analysis, optimal LED pattern selection.**

I. Introduction

A. Background

As a promising wireless transmission technique, visible light communication (VLC) relying on high-brightness light-emitting diodes (LEDs) both for illumination and for data communications has attracted wide interest. By exploiting the unlicensed visible light spectrum, VLC is capable of alleviating the spectral congestion of the radio frequency (RF) band [1]–[6]. VLC offers some unique advantages over RF communications, since it does not interfere with sensitive electromagnetic systems. However, similarly to RF-based transmission, VLC is inherently vulnerable to eavesdropping owing to its broadcast nature. Therefore, similar to its RF counterpart, information privacy and confidentiality constitute critical issues, in particular, when the VLC nodes are deployed in public train stations, libraries, offices, shopping malls, just to name a few.

By introducing physical layer security (PLS) techniques, secrecy in wireless communication systems can be readily enhanced [7]. PLS has first been studied from an information theoretic perspective in the context of a wiretap channel by Wyner for a point-to-point communication system [8], which has later been extended by Csiszár and Körner to RF broadcast channels [9]. PLS has been investigated from diverse perspectives in the context of [5], [6], [7], [10].

However, in contrast to RF systems, in many VLC schemes, the information is conveyed by intensity modulation and direct detection (IM/DD) techniques, real-valued and non-negative signals are transmitted. Secondly, in RF systems, the transmitter usually operates both under average and peak electrical power constraints. By contrast, the VLC signals are subject to both peak optical power, as well as to average optical power and electrical power constraints, owing to the dynamic range of typical LEDs and to the practical illumination requirements [11], [12]. Given these differences, the PLS techniques of RF systems cannot be directly applied in VLC systems.

B. State-of-the-art

The secrecy capacity and secrecy rate quantify the reliability and secrecy performance. Given the peak optical power, average optical power or the electrical power constraint, the upper and lower capacity bounds of IM/DD modulated single-input single-output (SISO) VLC channels have been investigated in [11]–[14]. In [15], the lower and upper bounds of the multiple-input multiple-output (MIMO) VLC system capacity have been derived under the assumption that the channel state information (CSI) is known to the transmitter.

PLS-aided VLC systems have also been investigated in the context of both SISO and multiple-input single-output (MISO) Gaussian wiretap channels and sophisticated beamforming schemes have been proposed in [16]–[18]. Specifically, the authors of [16] have derived the lower and upper bounds of the

F. Wang is with the School of Information Engineering, Zhengzhou University, Zhengzhou, 450001, Henan, China. (E-mail: iefswang@zzu.edu.cn)

C. Liu is with the Ministry of Education Key Laboratory for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an, 710049, Shaanxi, China. (E-mail: liucwhb@gmail.com)

Q. Wang, R. Zhang, L.-L. Yang and L. Hanzo are with Southampton Wireless, School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK. (E-mail: qw1e16@soton.ac.uk; jz09v@ecs.soton.ac.uk; rz@ecs.soton.ac.uk; lly@ecs.soton.ac.uk; lh@ecs.soton.ac.uk, http://www-mobile.ecs.soton.ac.uk)

J. Zhang is with the Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, U.K, also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China as well as with the School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China. (jz09v@ecs.soton.ac.uk)

This work is supported by the National Natural Science Foundation of China under grants 61401401 and 61571401, the China Postdoctoral Science Foundation Project under Grant 2015T80779, the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University under grant 2016D02, Innovative Talent of Colleges and University of Henan Province under grant 18HASTIT021, the Outstanding Young Talent Research Fund of Zhengzhou University under grant 1521318001 and the ERC's Advanced Fellow Grant Beam-Me-Up.

SISO Gaussian wiretap channel's capacity by assuming that the input signal is continuous and has a limited amplitude. Furthermore, when assuming that the eavesdropper's channel is perfectly known to the transmitter, the closed-form secrecy rate expressions of zero-forcing beamforming have been derived. Then, both the optimal and robust secrecy beamformers have been designed for MISO VLC systems under the idealized assumption that the CSI of the eavesdropper is perfectly known to the transmitter [17] or that some imperfect CSI knowledge is available [18]. As a more realistic scenario assuming that the eavesdropper's instantaneous CSI is not known by the transmitter, a friendly jammer strategy has been introduced in [19] for transmitting jamming signals with the objective of maximizing the secrecy rate.

A common assumption used in the above-mensioned contributions is that the distributions of both the information signals and of the jamming signals are continuous. Specifically, continuous uniform signal distribution has been considered in [16]–[18]. By contrast, having a truncated Gaussian signal distribution has been assumed in [20], in order to increase the secrecy rate under the constraint of a certain maximum input signal magnitude. In RF-based wireless communications it was found that under magnitude and power constraints imposed on the input signal of the SISO Gaussian wiretap channel, the optimal input distribution capable of achieving the secrecy capacity is a finite-cardinality discrete set [21]. However, under magnitude and power constraints, there are no corresponding results for the optimal input distribution of the MISO Gaussian wiretap channels capable of achieving their secrecy capacity.

To elaborate a little further, generalized space-shift keying (GSSK) has also been extensively studied in the context of VLC [22], [23]. In practice, given the limited luminous flux of an individual LED and the size of a typical room, usually multiple LEDs are used for achieving adequate illumination. When several LEDs are activated to transmit information, these spatially distributed LEDs can be naturally viewed as spatial constellation points, which can be exploited for implicitly conveying information. Therefore, the GSSK scheme is also suitable for VLC systems. In this case, the LEDs are utilized not only for lighting, but also for data transmission [24]. However, apart from the constraints imposed on the average power, as well as on the peak power relying on non-negative signalling, the input signals of GSSK-VLC systems are discrete, which makes the conventional Gaussian or uniform distribution based secrecy analysis infeasible. To the best of our knowledge, there are no research results in the open literature on the comprehensive secrecy performance analysis of GSSK-VLC systems relying on realistic discrete channel inputs, which inspired this treatise.

C. Contributions

Motivated by the aforementioned issues, in this paper, we propose and study the PLS issues in GSSK-VLC systems. In particular, we analyze the secrecy performance of GSSK-VLC systems, and propose an optimal LED pattern selection scheme for enhancing the secrecy performance of GSSK-VLC systems. The contributions of this paper can be summarized as follows:

- *The secrecy performance of a GSSK-VLC system is analyzed for the first time, when the channel inputs obey the finite discrete distributions, subject to certain constraints.* The performance metrics studied include the average mutual information (AMI), as well as the lower-bound of AMI and the achievable secrecy rate. Furthermore, an accurate closed-form expression is derived for the approximate AMI and the achievable secrecy rate. Additionally, the pairwise error probability (PEP) and bit error ratio (BER) of the proposed GSSK-VLC system are derived.
- *An optimal LED pattern selection algorithm is designed* for maximizing the AMI between the transmitter and legitimate user, when assuming that there is no *a priori* information regarding to the location of eavesdropper Eve. Furthermore, the secrecy performance of GSSK-VLC systems is improved by the optimal LED-pattern selection over that of the random LED selection.

D. Organization and Notation

Organization: The remainder of this paper is organized as follows. The system's description and the channel models are detailed in Section II. In Section III, we analyze the secrecy performance of the GSSK-VLC systems. Based on the minimax criterion, an optimal LED pattern selection algorithm is proposed in Section IV. Our performance results and the related discussions are provided in Section V. Finally, we conclude in Section VI.

Notation: Matrices (vectors) are denoted by boldface uppercase (lowercase) letters. The set of N-dimensional real-valued (non-negative) numbers is denoted by $\mathcal{R}^N(\mathcal{R}_+^N)$. $(\cdot)^{\mathrm{T}}$, $|\cdot|$, $\|\cdot\|$, $\lfloor\cdot\rfloor$, $\odot$, $\mathbb{E}\{\cdot\}$, $\mathbb{I}(\cdot;\cdot)$, $\binom{\cdot}{\cdot}$, $\approx$ denote transposition, absolute value, Euclidean norm, floor operation, Hadamard product, expected value, mutual information, binomial coefficient and approximately equal, respectively. Superscript $[x]^+$ denotes $\max\{x, 0\}$. The transmitter is denoted as Alice. Legitimate user and illegitimate user are denoted as Bob and Eve, respectively. We use $\mathbf{I}_N$ to denote the N-dimensional identity matrix, the subscripts $(\cdot)_{\mathrm{B}}$ and $(\cdot)_{\mathrm{E}}$ to denote relevance to Bob and Eve, respectively.

II. System and Signals Models

In this section, the GSSK-VLC system is described. Firstly, the channel gains and the Gaussian wiretap channel model are characterized, followed by our signal model.

A. Description of VLC Channel and Wiretap VLC Channel Models

Again, we consider a VLC system utilizing IM/DD, where confidential information is transmitted from a transmitter (Alice) to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). We assume that the transmitter is equipped with N_t down-facing LEDs installed on the ceiling, which are used for privately communicating with Bob, who has only a single upward facing photo-detector (PD). We assume that Eve is also equipped with a single PD and attempts to intercept the confidential information sent from Alice to

Bob. For simplicity, the PD of Eve is also assumed to face upwards, although this is not necessary [16]. Furthermore, all the LEDs and PDs are assumed to have the same parameters.

The transmit LEDs are driven by an identical bias current, denoted by $I_{\text{DC}} \in \mathcal{R}_+$, which is utilized to adjust the illumination level of the LEDs [16]. The information-bearing signals $\mathbf{x}(k) = [x_1(k), x_2(k), \cdots, x_{N_t}(k)]^{\text{T}} \in \mathcal{R}^{N_t}, k = 1, 2, \cdots$, are modulated by the LEDs, which are assumed to be zero-mean signals superimposed on I_{DC}. It should be noted that, since $\mathbb{E}\{x_i(k)\} = 0, i = 1, \cdots, N_t$, the information-bearing signals do not change the average optical intensity and, therefore, they do not affect the illumination of the LEDs [16], [18]. For the sake of safety and also for maintaining linear current conversion, so as to avoid clipping distortion and to conserve power, we restrict the total current of $I_{\text{DC}} + x_i(k)$ to the range of $[(1-\alpha)I_{\text{DC}}, (1+\alpha)I_{\text{DC}}]$, where $\alpha \in [0, 1]$ is the modulation index [11], [16]. As a result, the information-bearing signal $x_i(k)$ has to satisfy the peak amplitude constraint of $|x_i(k)| \leq A, \forall i, k$ with $A = \alpha I_{\text{DC}} \in \mathcal{R}_+$.

After electro-optical conversion, the instantaneous optical intensity can be modelled as $P_{\text{T}i}(k) = \eta[I_{\text{DC}} + x_i(k)]$, where η is the LEDs' current-to-light conversion efficiency. At the receiver, the optical power received from the i-th LED is expressed as $P_{\text{R}i}(k) = G_i P_{\text{T}i}(k)$, where G_i is the path gain between the i-th LED and the receiver, where $i = 1, 2, \cdots, N_t$. As shown in [16], [25], when a generalized Lambertian emission pattern is considered, the path gain G_i is expressed as

$$G_i = \begin{cases} \frac{1}{2\pi d_i^2}(m+1)A_{\text{R}} \cos^m(\phi_i)\cos\psi_i, & |\psi_i| \leq \Psi_{\text{FoV}}, \\ 0, & |\psi_i| > \Psi_{\text{FoV}}, \end{cases} \tag{1}$$

where d_i is the line of sight (LoS) distance between the i-th LED and the receiver's PD, A_{R} is the effective detection area of the PD, $\phi_i = \phi$ is the angle of irradiance from the LED, which is measured with respect to (w.r.t.) the LED axis and assumed to be the same for all the transmit LEDs. Still referring to (1), ψ_i is the angle of incidence of the i-th optical link, $m = -1/\log_2\left(\cos\Phi_{1/2}\right)$ is the Lambertian emission order, $\Phi_{1/2}$ is the half irradiance angle, and finally, Ψ_{FoV} is the receiver's field-of-view (FoV) semi-angle. According to [25], the detection area of the PD is given by

$$A_{\text{R}} = \frac{\beta^2}{\sin^2(\Psi_{\text{FoV}})} A_{\text{PD}}, \tag{2}$$

where β denotes the refractive index of the optical concentrator and A_{PD} is the PDs' area.

Given a responsivity R for the PD, the incident optical power is converted into a current of $RP_{\text{R}i}(k)$. After removing the DC bias I_{DC}, the received signal is amplified by a transimpedance amplifier with a gain of T, to produce a voltage of $q(k) \in \mathcal{R}$, which is a scaled combination of the transmitted signals in $\mathbf{x}(k)$ contaminated by the noise [16]. In summary, the input-output relationship of the VLC channel between the N_t LEDs and a PD can be modelled as

$$q(k) = \sum_{i=1}^{N_t} h_i x_i(k) + w(k), k = 1, 2, \cdots \tag{3}$$

where $h_i = TRG_i\eta$ is the channel gain and $w(k) \sim \mathcal{N}(0, \sigma^2)$ is the Gaussian noise. We considered three components of the noise [11], which are the thermal noise, intensity-dependent noise and the shot noise caused by the ambient light. The sum of these noise components can be modelled by the zero-mean additive white Gaussian noise (AWGN) [16].

Note furthermore that the VLC channel gain depends on the specific location of both the transmit LED and of the receive PD. If a receive PD and the associated transmit LED are not in each others' FoV, we have $h_i = 0$. Furthermore, if light reflections are encountered, an accurate VLC channel should include both the LoS link and the non-LoS links. However, the power conveyed by the non-LoS components is in general significantly lower than that conveyed by the LoS component [16]. Consequently, the channel model of (3) can readily neglect the non-LoS components for simplifying our analysis.

Given the above assumptions, our system constitutes a typical multi-input single-output single-Eve (MISOSE) Gaussian wiretap scenario. Therefore, following the VLC channel model of (3), the observations obtained by Bob and Eve can be expressed, respectively, as

$$y(k) = \mathbf{h}_{\text{B}}^{\text{T}}\mathbf{x}(k) + w_{\text{B}}(k), \tag{4}$$

$$z(k) = \mathbf{h}_{\text{E}}^{\text{T}}\mathbf{x}(k) + w_{\text{E}}(k), \tag{5}$$

where, by definition, we have $\mathbf{h}_{\text{B}} = [h_{\text{B},1}, h_{\text{B},2}, \cdots, h_{\text{B},N_t}]^{\text{T}} \in \mathcal{R}_+^{N_t}$ and $\mathbf{h}_{\text{E}} = [h_{\text{E},1}, h_{\text{E},2}, \cdots, h_{\text{E},N_t}]^{\text{T}} \in \mathcal{R}_+^{N_t}$, which are referred to as the MISO channel vectors of the Alice-to-Bob and Alice-to-Eve links, respectively. In this paper, we assume that Alice has perfect knowledge of $\mathbf{h}_{\text{B}}$ but no knowledge of $\mathbf{h}_{\text{E}}$. Eve is capable of estimating its own channel vector $\mathbf{h}_{\text{E}}$. We assume that $w_{\text{B}} \sim \mathcal{N}(0, \sigma_{\text{B}}^2)$ and $w_{\text{E}} \sim \mathcal{N}(0, \sigma_{\text{E}}^2)$ are independent and identically distributed (i.i.d.) AWGN processes, hence $\sigma_{\text{B}}^2 = \sigma_{\text{E}}^2$.

B. GSSK-VLC System Model

Let us assume that there are N LEDs in the service area considered. For the proposed GSSK-VLC system, we assume that from the N LEDs, only $N_t \leq N$ LEDs are utilized for GSSK modulation. Based on the N_t transmit LEDs selected, during a symbol duration, n_t $(1 \leq n_t < N_t)$ LEDs are activated to simultaneously transmit their information, while the remaining $(N_t - n_t)$ LEDs are only employed for illumination. Hence, there are in total $M' = \binom{N_t}{n_t}$ possible combinations, where $M = 2^m$ associated with $m = \lfloor \log_2 M' \rfloor = \lfloor \log_2 \binom{N_t}{n_t} \rfloor$ are actually used for information transmission. Therefore, the number of bits per GSSK symbol is m. In our ensuring discussions, we explicitly select the first M combinations for conveying information.

Let us assume that an i.i.d. random bit sequence $\{\cdots, b_1, b_2, \cdots, b_l, \cdots\}$ is entered into the GSSK mapper, where the bit sequence is partitioned into blocks of $m = \log_2(M)$ bits that are mapped into GSSK symbols $\mathbf{x}(k), \mathbf{x}(k) \in \mathcal{X}$, where $\mathcal{X}$ is the set of M GSSK symbols. Based on $\mathbf{x}(k)$, n_t LEDs are selected for transmission, with each having a constant intensity of $I = s/\sqrt{n_t}$, where the factor of $1/\sqrt{n_t}$ is used for satisfying the power constraint.

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/ACCESS.2018.2799658, IEEE Access

Consequently, the transmitted signal vector $\mathbf{x}(k)$ can be expressed as

$$\begin{aligned}\mathbf{x}(k) &= \frac{s}{\sqrt{n_t}}\sum_{i=1}^{n_t}\mathbf{e}_{\omega_i} \\ &= \frac{s}{\sqrt{n_t}}\underbrace{[\ \cdots\ 0\ 1\ 0\ \cdots\ 1\cdots]^{\mathrm{T}}}_{n_t \text{ non-zero values in } N_t} \\ &= \frac{s}{\sqrt{n_t}}\mathbf{e}_{\omega(k)}, \end{aligned} \tag{6}$$

where $\mathbf{e}_{\omega_i}$, $\omega_i \in \{1, 2, \cdots, N_t\}$, represents a single column of an identity matrix $\mathbf{I}_{N_t}$, determined by the index of the i-th activated LED, while $\mathbf{e}_{\omega(k)} = \sum_{i=1}^{n_t}\mathbf{e}_{\omega_i}$ is a N_t-length vector with its non-zero elements corresponding to the n_t activated LEDs, $\omega(k) \in \Omega = \{1, 2, \cdots, M\}$. Without loss of generality, we assume that the average intensity of $\mathbf{x}(k)$ is normalized to $\mathbb{E}\{\|\mathbf{x}(k)\|^2\} = 1$. Hence, we also have $s^2 = 1$.

Note that, the above-mentioned GSSK-VLC system becomes an SSK-VLC system, when $n_t = 1$. In other words, the SSK-VLC system is a special case of our GSSK-VLC system. Hence, all the following analytical results and the LED selection methods can be straightforwardly applied to SSK-VLC systems by letting $n_t = 1$.

When the signal of (6) is transmitted over the VLC wiretap channel, following (4) and (5), we have

$$\begin{aligned} y(k) &= \mathbf{h}_{\mathrm{B},\omega(k)}^{\mathrm{T}}\mathbf{x}(k) + w_{\mathrm{B}}(k) \\ &= \frac{s}{\sqrt{n_t}}\mathbf{h}_{\mathrm{B},\omega(k)}^{\mathrm{T}}\mathbf{e}_{\omega(k)} + w_{\mathrm{B}}(k) \\ &= h_{\mathrm{B}(\omega(k))}s + w_{\mathrm{B}}(k), \end{aligned} \tag{7}$$

$$\begin{aligned} z(k) &= \mathbf{h}_{\mathrm{E},\omega(k)}^{\mathrm{T}}\mathbf{x}(k) + w_{\mathrm{E}}(k) \\ &= \frac{s}{\sqrt{n_t}}\mathbf{h}_{\mathrm{E},\omega(k)}^{\mathrm{T}}\mathbf{e}_{\omega(k)} + w_{\mathrm{E}}(k) \\ &= h_{\mathrm{E}(\omega(k))}s + w_{\mathrm{E}}(k), \end{aligned} \tag{8}$$

where by definition, $\mathbf{h}_{\mathrm{B},\omega(k)} = \mathbf{h}_{\mathrm{B}} \odot \mathbf{e}_{\omega(k)}$, $\mathbf{h}_{\mathrm{E},\omega(k)} = \mathbf{h}_{\mathrm{E}} \odot \mathbf{e}_{\omega(k)}$, $h_{\mathrm{B}(\omega(k))} = \frac{\mathbf{h}_{\mathrm{B},\omega(k)}^{\mathrm{T}}\mathbf{e}_{\omega(k)}}{\sqrt{n_t}} \in \mathcal{H}_{\mathrm{B}(\omega)}$ and $h_{\mathrm{E}(\omega(k))} = \frac{\mathbf{h}_{\mathrm{E},\omega(k)}^{\mathrm{T}}\mathbf{e}_{\omega(k)}}{\sqrt{n_t}} \in \mathcal{H}_{\mathrm{E}(\omega)}$, $\mathcal{H}_{\mathrm{B}(\omega)}$ and $\mathcal{H}_{\mathrm{E}(\omega)}$ are the two sets collecting all the M possible channel states observed at Bob and Eve, respectively. In summary, the system model of the GSSK-VLC wiretap channel is illustrated by Fig. 1.

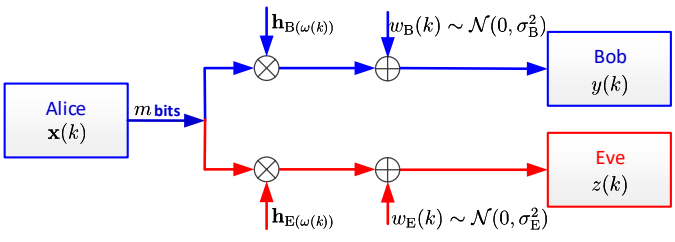


Fig. 1. System model of GSSK-VLC MISO wiretap channel.

III. Performance Analysis for GSSK-VLC Systems

In this section, we first derive both the AMI, as well as its lower-bound and the achievable secrecy rate. Then, a closed-form expression of the approximate AMI is derived. Finally, the PEP and BER of the GSSK-VLC system are analyzed.

Observe from (7) and (8) that the GSSK-VLC system may be modelled by a typical *discrete input memoryless* wiretap channel. In this paper, similar to many existing studies, such as [17], [18], a lower-bound of the achievable secrecy rate is considered for characterizing the secrecy behaviour of the GSSK-VLC system, which can be expressed as

$$R_{\text{sec}} = \left[\mathbb{I}(h_{\mathrm{B}}; Y) - \mathbb{I}(h_{\mathrm{E}}; Z)\right]^{+}, \tag{9}$$

where $\mathbb{I}(h_{\mathrm{B}}; Y)$ and $\mathbb{I}(h_{\mathrm{E}}; Z)$ denote the mutual information between Alice and Bob, as well as between Alice and Eve , respectively. Below we first analyze these mutual information expressions.

A. Average Mutual Information

Explicitly, given $\mathbf{h}_{\mathrm{B},\omega(k)}$ and $\mathbf{h}_{\mathrm{E},\omega(k)}$, the observations (7) and (8) by Bob and Eve obey the Gaussian distributions, with the probability density functions (PDFs) expressed as

$$p_{Y|h_{\mathrm{B}}}(y|h_{\mathrm{B}} = h_{\mathrm{B}(\omega(k))}) = \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{B}}}\exp\left(-\frac{(y - h_{\mathrm{B}(\omega(k))}s)^2}{2\sigma_{\mathrm{B}}^2}\right), \tag{10}$$

$$p_{Z|h_{\mathrm{E}}}(z|h_{\mathrm{E}} = h_{\mathrm{E}(\omega(k))}) = \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}}\exp\left(-\frac{(z - h_{\mathrm{E}(\omega(k))}s)^2}{2\sigma_{\mathrm{E}}^2}\right). \tag{11}$$

Furthermore, as the transmitted information is i.i.d., we can express the unconditional PDFs of Y and Z as

$$\begin{aligned} p_Y(y) &= \sum_{\omega(k)\in\Omega} p_{Y|h_{\mathrm{B}}}(y|h_{\mathrm{B}(\omega(k))})P_{h_{\mathrm{B}}}(h_{\mathrm{B}(\omega(k))}) \\ &= \sum_{\omega(k)\in\Omega}\frac{1}{\sqrt{2\pi}\sigma_{\mathrm{B}}M}\exp\left(-\frac{(y - h_{\mathrm{B}(\omega(k))}s)^2}{2\sigma_{\mathrm{B}}^2}\right), \end{aligned} \tag{12}$$

$$\begin{aligned} p_Z(z) &= \sum_{\omega(k)\in\Omega} p_{Z|h_{\mathrm{E}}}(z|h_{\mathrm{E}(\omega(k))})P_{h_{\mathrm{E}}}(h_{\mathrm{E}(\omega(k))}) \\ &= \sum_{\omega(k)\in\Omega}\frac{1}{\sqrt{2\pi}\sigma_{\mathrm{E}}M}\exp\left(-\frac{(z - h_{\mathrm{E}(\omega(k))}s)^2}{2\sigma_{\mathrm{E}}^2}\right). \end{aligned} \tag{13}$$

For the following analysis, we define $\varrho_{\mathrm{B}} = 1/\sigma_{\mathrm{B}}^2$ and $\varrho_{\mathrm{E}} = 1/\sigma_{\mathrm{E}}^2$ as the average signal-to-noise ratios (SNRs) at Bob and Eve, respectively. Furthermore, for simplicity, we omit all the time indices k. With the aid of the PDF expressions in (10) - (13), we can derive the AMIs of both the Alice-to-Bob link and of the Alice-to-Eve link, which are stated as follows.

Theorem 1: For the GSSK-VLC system having finite discrete inputs, the AMI between the input signal of Alice and the output signal of Bob can be written as

$$\begin{aligned} \mathbb{I}(h_{\mathrm{B}}; Y) = \log_2 M - \frac{1}{M}\times \\ \sum_{\omega=1}^{M}\mathbb{E}_{w_{\mathrm{B}}}\left[\log_2\sum_{\varpi=1}^{M}\exp\left(\frac{1}{2}\varrho_{\mathrm{B}}\left(w_{\mathrm{B}}^2 - (w_{\mathrm{B}} + \zeta_{\omega,\varpi}s)^2\right)\right)\right], \end{aligned} \tag{14}$$

where $\zeta_{\omega,\varpi} = h_{\mathrm{B}(\omega)} - h_{\mathrm{B}(\varpi)}$. Similarly, the AMI between the input signal of Alice and the output signal of Eve can be expressed as

$$\mathbb{I}(h_{\mathrm{E}}; Z) = \log_2 M - \frac{1}{M} \times \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{E}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(\frac{1}{2} \varrho_{\mathrm{E}} \left(w_{\mathrm{E}}^2 - (w_{\mathrm{E}} + \xi_{\omega,\varpi} s)^2 \right) \right) \right], \tag{15}$$

where $\xi_{\omega,\varpi} = h_{\mathrm{E}(\omega)} - h_{\mathrm{E}(\varpi)}$.

Proof: Please refer to Appendix A. ∎

Upon substituting (14) and (15) into (9), the achievable secrecy rate of the GSSK-VLC system can be expressed as

$$\begin{aligned} R_{\mathrm{sec}} &= \left[\mathbb{I}(h_{\mathrm{B}}; Y) - \mathbb{I}(h_{\mathrm{E}}; Z) \right]^+ \\ &= \left[-\frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(\Theta_1 \right) \right] \right. \\ &\quad \left. + \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{E}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(\Theta_2 \right) \right] \right]^+ . \end{aligned} \tag{16}$$

where we defined the short-hand of $\Theta_1 = \frac{1}{2} \varrho_{\mathrm{B}} \left(w_{\mathrm{B}}^2 - (w_{\mathrm{B}} + \zeta_{\omega,\varpi} s)^2 \right)$ and $\Theta_2 = \frac{1}{2} \varrho_{\mathrm{E}} \left(w_{\mathrm{E}}^2 - (w_{\mathrm{E}} + \xi_{\omega,\varpi} s)^2 \right)$.

B. Lower-Bound for AMI

In general, deriving a closed-form expection w.r.t. w_{B} or w_{E} in (14) or (15) is not an easy task. Therefore, below we derive the lower-bounds for the AMI of both the Alice-to-Bob link and of the Alice-to-Eve link, which are detailed in the following theorem.

Theorem 2: The AMI between the input signal of Alice and the output signal of Bob can be lower-bounded as

$$\mathbb{I}_L(h_{\mathrm{B}}; Y) = \log_2 M - \frac{1}{2} \left(\log_2 e - 1 \right) - \frac{1}{M} \sum_{\omega=1}^{M} \log_2 \sum_{\varpi=1}^{M} \exp\left(-\frac{\varrho_{\mathrm{B}} \left(\zeta_{\omega,\varpi} s \right)^2}{4} \right). \tag{17}$$

Similarly, the AMI between the input signal of Alice and the output signal of Eve can be lower-bounded as

$$\mathbb{I}_L(h_{\mathrm{E}}; Z) = \log_2 M - \frac{1}{2} \left(\log_2 e - 1 \right) - \frac{1}{M} \sum_{\omega=1}^{M} \log_2 \sum_{\varpi=1}^{M} \exp\left(-\frac{\varrho_{\mathrm{E}} \left(\xi_{\omega,\varpi} s \right)^2}{4} \right). \tag{18}$$

Proof: Please refer to Appendix B. ∎

C. Approximation for AMI

Furthermore, for Theorem 2, below we derive approximations for $\mathbb{I}(h_{\mathrm{B}}; Y)$ and $\mathbb{I}(h_{\mathrm{E}}; Z)$, respectively. As stated in Theorem 1, the AMI achieved by Bob can be expressed as in (14). Accordingly, letting $\varrho_{\mathrm{B}} \to \infty$ and $\varrho_{\mathrm{B}} \to 0$, we can derive the limits of $\mathbb{I}(h_{\mathrm{B}}; Y)$, which are given by

$$\begin{aligned} \lim_{\varrho_{\mathrm{B}} \to \infty} \mathbb{I}(h_{\mathrm{B}}; Y) &= \log_2 M, \\ \lim_{\varrho_{\mathrm{B}} \to 0} \mathbb{I}(h_{\mathrm{B}}; Y) &= 0. \end{aligned} \tag{19}$$

Similarly, from (17) we can obtain the limits of $\mathbb{I}_L(h_{\mathrm{B}}; Y)$ as

$$\begin{aligned} \lim_{\varrho_{\mathrm{B}} \to \infty} \mathbb{I}_L(h_{\mathrm{B}}; Y) &= \log_2 M - \frac{1}{2} (\log_2 e - 1), \\ \lim_{\varrho_{\mathrm{B}} \to 0} \mathbb{I}_L(h_{\mathrm{B}}; Y) &= -\frac{1}{2} (\log_2 e - 1). \end{aligned} \tag{20}$$

Observe by comparing (19) and (20) that there is a constant difference between the AMI and its lower bound at both high and low SNRs, which is $\frac{1}{2}(\log_2 e - 1)$. Moreover, it can be shown that both $\mathbb{I}(h_{\mathrm{B}}; Y)$ and $\mathbb{I}_L(h_{\mathrm{B}}; Y)$ are monotonically increasing functions w.r.t. ϱ_{B}. Hence we infer that for any given SNR, especially for relatively high or low SNRs, the difference between $\mathbb{I}(h_{\mathrm{B}}; Y)$ and $\mathbb{I}_L(h_{\mathrm{B}}; Y)$ can be approximated by a constant of $\frac{1}{2}(\log_2 e - 1)$. Similarly, same is true for the difference between $\mathbb{I}(h_{\mathrm{E}}; Z)$ and $\mathbb{I}_L(h_{\mathrm{E}}; Z)$.

Based on the above observations, we can hence propose an approximation for $\mathbb{I}(h_{\mathrm{B}}; Y)$ as

$$\mathbb{I}(h_{\mathrm{B}}; Y) \approx \mathbb{I}_L(h_{\mathrm{B}}; Y) + \frac{1}{2} (\log_2 e - 1). \tag{21}$$

Substituting this result into (17) of Theorem 2, $\mathbb{I}(h_{\mathrm{B}}; Y)$ can be approximated as

$$\mathbb{I}_A(h_{\mathrm{B}}; Y) \approx \log_2 M - \frac{1}{M} \sum_{\omega=1}^{M} \log_2 \sum_{\varpi=1}^{M} \exp\left(-\frac{\varrho_{\mathrm{B}} \left(\zeta_{\omega,\varpi} s \right)^2}{4} \right). \tag{22}$$

Following a similar procedure, we can approximate $\mathbb{I}(\mathbf{h}_{\mathrm{E}}; Z)$ as

$$\mathbb{I}_A(h_{\mathrm{E}}; Z) \approx \log_2 M - \frac{1}{M} \sum_{\omega=1}^{M} \log_2 \sum_{\varpi=1}^{M} \exp\left(-\frac{\varrho_{\mathrm{E}} \left(\xi_{\omega,\varpi} s \right)^2}{4} \right). \tag{23}$$

Consequently, upon substituting (22) and (23) into (9), the approximate secrecy rate of the GSSK-VLC system can be expressed as

$$\begin{aligned} R_{A,\mathrm{sec}} &= \left[\mathbb{I}_A(h_{\mathrm{B}}; Y) - \mathbb{I}_A(h_{\mathrm{E}}; Z) \right]^+ \\ &= \left[\frac{1}{M} \sum_{\omega=1}^{M} \log_2 \left[\frac{\sum_{\varpi=1}^{M} \exp\left(-\Phi \right)}{\sum_{\varpi=1}^{M} \exp\left(-\Psi \right)} \right] \right]^+ , \end{aligned} \tag{24}$$

where we defined the short-hand of $\Phi = \frac{\varrho_{\mathrm{B}} (\xi_{\omega,\varpi} s)^2}{4}$ and $\Psi = \frac{\varrho_{\mathrm{E}} (\zeta_{\omega,\varpi} s)^2}{4}$.

D. Error Ratio Analysis

In the GSSK-VLC system, the task of detection at both Bob and Eve is to determine the indices of the activated LEDs by Alice. Since the LEDs are activated based on a uniform distribution, the optimal detectors employed by Bob and Eve

follow the principles of maximum likelihood (ML) detection, expressed as

$$\hat{\omega}_{\mathrm{B}} = \arg \min_{\omega \in \{1,\cdots,M\}} |y - h_{\mathrm{B}(\omega)} s|^2, \tag{25}$$

$$\hat{\omega}_{\mathrm{E}} = \arg \min_{\omega \in \{1,\cdots,M\}} |z - h_{\mathrm{E}(\omega)} s|^2, \tag{26}$$

respectively. Below, we analyze the error probability of Bob and Eve based on (25) and (26).

To begin with, let us derive the PEP of the detection at Bob, which is the probability of detecting the LED set ϖ, while the LED set ω are the actually activated LEDs, which can be expressed as

$$\begin{aligned} \mathrm{P}(\omega \mapsto \varpi | h_{\mathrm{B}}) &= \mathrm{P}\left(|y - h_{\mathrm{B}(\varpi)} s|^2 > |y - h_{\mathrm{B}(\omega)} s|^2\right) \\ &= \mathrm{P}\Big(\left(h_{\mathrm{B}(\varpi)} s + w_{\mathrm{B}} - h_{\mathrm{B}(\varpi)} s\right)^2 \\ &\qquad > \left(h_{\mathrm{B}(\varpi)} s + w_{\mathrm{B}} - h_{\mathrm{B}(\omega)} s\right)^2\Big) \\ &= \mathrm{P}\left(2\zeta_{\omega,\varpi} s w_{\mathrm{B}} > \zeta_{\omega,\varpi}^2 s^2\right) \\ &= Q\left(\frac{|\zeta_{\omega,\varpi}| s}{2\sigma_{\mathrm{B}}}\right), \end{aligned} \tag{27}$$

where $Q(\cdot)$ is the Gaussian Q-function defined as $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{t^2}{2}\right) dt$. Note that the third equation holds, since $2\zeta_{\omega,\varpi} s w_{\mathrm{B}}$ is a random variable obeying the Gaussian distribution of $2\zeta_{\omega,\varpi} s w_{\mathrm{B}} \sim \mathcal{N}(0, 4\zeta_{\omega,\varpi}^2 s^2 \sigma^2)$.

Consequently, we can express the upper-bound BER at Bob with the aid of the union-bound approach [26] as

$$\begin{aligned} \mathrm{P}_{\mathrm{B,bit}} &\leq \frac{1}{mM} \sum_{\omega=1}^{M} \sum_{\varpi=1}^{M} H_d(\omega \mapsto \varpi)\, \mathrm{P}(\omega \mapsto \varpi | h_{\mathrm{B}}) \\ &= \frac{1}{mM} \sum_{\omega=1}^{M} \sum_{\varpi=1}^{M} H_d(\omega \mapsto \varpi)\, Q\left(\frac{|\zeta_{\omega,\varpi}| s}{2\sigma_{\mathrm{B}}}\right), \end{aligned} \tag{28}$$

where $H_d(\omega \mapsto \varpi)$ is the Hamming distance between the binary representations of ω and ϖ. Similarly, the upper-bounded BER at Eve is expressed as

$$\mathrm{P}_{\mathrm{E,bit}} \leq \frac{1}{mM} \sum_{\omega=1}^{M} \sum_{\varpi=1}^{M} H_d(\omega \mapsto \varpi)\, Q\left(\frac{|\xi_{\omega,\varpi}| s}{2\sigma_{\mathrm{E}}}\right). \tag{29}$$

In order to further simplify the computations, we may exploit the tight upper bound for the Q function [27], which is given by $Q(x) \leq \sum_{n=1}^{3} a_n \exp(-b_n x^2)$, where $a_1 = \frac{1}{6}, a_2 = \frac{1}{12}, a_3 = \frac{1}{4}$, $b_1 = 2, b_2 = 1, b_3 = \frac{1}{2}$. As a result, the PEP of the detection at Bob can be expressed as

$$\begin{aligned} \mathrm{P}(\omega \mapsto \varpi | h_{\mathrm{B}}) \leq \frac{1}{6} \exp\left(-\frac{(\zeta_{\omega,\varpi})^2 s^2}{2\sigma_{\mathrm{B}}^2}\right) + \\ \frac{1}{12} \exp\left(-\frac{(\zeta_{\omega,\varpi})^2 s^2}{4\sigma_{\mathrm{B}}^2}\right) + \frac{1}{4} \exp\left(-\frac{(\zeta_{\omega,\varpi})^2 s^2}{8\sigma_{\mathrm{B}}^2}\right). \end{aligned} \tag{30}$$

The BER expression of Eve can be obtained similarly.

Observe from (28) that the BER depends both on the SNR, and on the Euclidean distance or diversity order $|\zeta_{\omega,\varpi}|$ between any two LED sets. In other words, the performance of the GSSK-VLC system depends on the diversity gain of the channels determined by two LED sets. Therefore, maximizing the diversity order $|\zeta_{\omega,\varpi}|$ may enhance the performance of GSSK-VLC system, which is hence studied below in the next section.

IV. Secrecy Enhancement by Optimal LED Pattern Selection

As shown in (1), there is a direct relationship between the channel gains and the relative positions of LEDs. When the positions of LEDs are fixed, some symmetric regions exist in the coverage area, as shown in Fig. 3, where the AMI of both $\mathbb{I}(h_{\mathrm{B}}; Y)$ and $\mathbb{I}(h_{\mathrm{E}}; Z)$ is relatively low. If Bob is located in these symmetric regions, the achievable secrecy rate will be low. In this section, we exploit these characteristics and propose an optimal LED pattern selection algorithm for the secrecy enhancement of GSSK-VLC systems.

Let us assume that all the LED parameters are fixed. Then, an optimal LED pattern selection seeks the minimax solution of a given objective function, as detailed below. We also assume that the Alice-Bob channel is known to Alice, but the Alice-Eve channel is unknown to Alice, since Eve is a passive eavesdropper. Then, as shown in (22), $\mathbb{I}_A(h_{\mathrm{B}}; Y)$ is mainly determined by $\zeta_{\omega,\varpi}$. Hence, we may select the LED activation pattern by solving the following optimization problem,

$$\begin{aligned} \zeta^\star &= \max_{h_{\mathrm{B}(\omega)} \in \mathcal{H}_{\mathrm{B}(\omega)},\, h_{\mathrm{B}(\varpi)} \in \mathcal{H}_{\mathrm{B}(\omega)}} \min |\zeta_{\omega,\varpi}| \\ &= \max_{h_{\mathrm{B}(\omega)} \in \mathcal{H}_{\mathrm{B}(\omega)},\, h_{\mathrm{B}(\varpi)} \in \mathcal{H}_{\mathrm{B}(\omega)}} \min |h_{\mathrm{B}(\omega)} - h_{\mathrm{B}(\varpi)}|. \end{aligned} \tag{31}$$

Given this optimal $\zeta^\star$, we can determine the optimum LED set $N_t^\star$. In order to solve this optimization problem, we propose Algorithm 1. If we have served optimal LED patterns $\zeta_{\min}^{(i)} = \zeta^\star$, we can randomly select one of them.

Algorithm 1: Optimal LED Pattern Selection

Step 1: Given $N > N_t$ LEDs, choose N_t LEDs from the N LEDs to form a LED set for GSSK. Hence, there are in total $\binom{N}{N_t}$ selections, forming a set $\mathcal{F} = \{\mathcal{F}_1, \mathcal{F}_2, \cdots, \mathcal{F}_{\binom{N}{N_t}}\}$;

Step 2: For each element of $\mathcal{F}$, choose n_t LEDs from the N_t LEDs for the GSSK modulation. There are in total $\binom{N_t}{n_t}$ selections, collected to a set $\mathcal{N}_t^{(i)} = \{\omega_1^{(i)}, \omega_2^{(i)}, \cdots, \omega_{\binom{N_t}{n_t}}^{(i)}\}, i = 1, 2, \cdots, \binom{N}{N_t}$;

Step 3: For each set $\mathcal{N}_t^{(i)}$, compute $\zeta_{\min}^{(i)} = \min\{|h_{\omega_k^{(i)}} - h_{\omega_l^{(i)}}|, \omega_k^{(i)}, \omega_l^{(i)} \in \mathcal{N}_t^{(i)}, \omega_k^{(i)} \neq \omega_l^{(i)}\}, i = 1, 2, \cdots, \binom{N}{N_t}$;

Step 4: Find the maximum value $\zeta^\star$ as $\zeta^\star = \max\{\zeta_{\min}^{(1)}, \zeta_{\min}^{(2)}, \cdots, \zeta_{\min}^{(\binom{N}{N_t})}\}$, from which the optimum LED pattern is determined.

Let us now consider the complexity of the proposed LED pattern selection algorithm. Firstly, choosing N_t LEDs out of the N LEDs requires a number of operations on the order of $\binom{N}{N_t}$. Secondly, it can be shown that for a given set in $\mathcal{F}$, the number of operation is $\frac{\binom{N_t}{n_t}\left[\binom{N_t}{n_t}-1\right]}{2}$. Hence, the total number

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/ACCESS.2018.2799658, IEEE Access

TABLE I
SIMULATION PARAMETERS

Simulation setup parameters	
Room size ($L \times W \times H$)	$5 \times 5 \times 3$ m^3
Number of LEDs	$2, 4, 8, 9$
LEDs (Alice) height	3 m
Receivers (Bob and Eve) height	0.85 m
Transmitter parameters	
Semi-angle at half power ($\Phi_{1/2}$)	60°
Optical power/ electric conversion efficiency (η)	813.6 μW/mA
Modulation index (α)	0.1
Receivers parameters	
Refractive index (β)	1.5
Physical area of a PD (A_{PD})	1.0 cm^2
Receiver FoV semi-angle (Ψ_{FoV})	60°
PD responsivity (R)	100 μA/mW/cm^2

TABLE II
THE DISTRIBUTIONS OF THE LEDS' LOCATIONS

2 LEDs		8 LEDs	
LED	(O_X, O_Y, O_Z)	1	$(1.25, 0.63, 3.0)$ m
1	$(1.25, 2.50, 3.0)$ m	2	$(3.75, 0.63, 3.0)$ m
2	$(3.75, 2.50, 3.0)$ m	3	$(1.25, 1.88, 3.0)$ m
4 LEDs		4	$(3.75, 1.88, 3.0)$ m
1	$(1.25, 1.25, 3.0)$ m	5	$(1.25, 3.13, 3.0)$ m
2	$(3.75, 1.25, 3.0)$ m	6	$(3.75, 3.13, 3.0)$ m
3	$(1.25, 3.75, 3.0)$ m	7	$(1.25, 4.38, 3.0)$ m
4	$(3.75, 3.75, 3.0)$ m	8	$(3.75, 4.38, 3.0)$ m

of operations required for determining the optimum LED pattern is $\binom{N}{N_t}\binom{N_t}{n_t}\left[\binom{N_t}{n_t}-1\right]/2$, which quantifies the complexity of the algorithm as $\mathcal{O}\left(N^{\min\{N_t, N-N_t\}} \cdot N_t^{2\min\{n_t, N_t-n_t\}}\right)$.

V. SIMULATION AND NUMERICAL RESULTS

In order to characterize the performance of the proposed GSSK-VLC system, and to validate the analytical expressions derived, we consider an indoor VLC environment having the dimensions of $5 \times 5 \times 3$ m^3, which is represented in a 3-dimensional (3-D) Cartesian coordinate system with the origin being one corner of the room. Again, the transmit LEDs are assumed to radiate perpendicularly from to the ceiling to the floor. The receivers of Bob and Eve are located on their desks at 0.85 m from the floor. The receivers are also assumed to be perpendicularly oriented from the desk to the ceiling. The half-illuminance semi-angle $\Phi_{1/2}$ of the LED is set to 60°, which is a typical value for commercially-available high-brightness LEDs [16][1]. For convenience, all the parameters involved in our simulations are summarized in Table I.

A. Performance of GSSK-VLC Systems without LEDs Selection

Firstly, we validate the analytical results without considering the LED selections. Unless specially noted, we assume that the positions of LEDs are those presented in Table II. We assume that Bob's receiver is located at $(2.15, 1.28, 0.85)$ m, while Eve's receiver is located randomly on a desk with the height of 0.85 m from the floor.

Fig. 2 visualizes the AMI calculated from (14), as well as the lower bound of the AMI computed from (17) and the approximated AMI of (22). In order to evaluate these formulas, 10^4 realizations are used for each SNR $= 1/\sigma^2$. In Fig. 2, we assumed that $N_t = 2, 4, 8$ and only a single LED is activated for transmission, forming the SSK-VLC system. Furthermore, for the case of $N_t = 8$ LEDs, we also consider the GSSK-VLC using $n_t = 2$. Additionally, the total number of bits conveyed per symbol in these cases are $m = 1, 2, 3$ and 4 bits, respectively. As shown in Fig. 2, the AMI increases upon increasing of the SNR, and also with the number of LEDs N_t. The difference between $\mathbb{I}(h_{\text{B}}; Y)$ and the lower bound $\mathbb{I}_L(h_{\text{B}}; Y)$ is approximately $\frac{1}{2}(\log_2 e - 1)$ at both low and high SNRs, which coincides with the theoretical analysis of Section III-C. As shown in Fig. 2, the approximation of $\mathbb{I}_A(h_{\text{B}}; Y)$ in (22) by (14) is tight, especially when the SNR is either low or high. For the SSK-VLC system employing 2 LEDs, $\mathbb{I}(h_{\text{B}}; Y)$ reaches the maximum of 1 bit/symbol, when the SNR is higher than 26 dB. For the SSK-VLC system using 8 LEDs, provided that the SNR is higher than 29 dB, $\mathbb{I}(h_{\text{B}}; Y)$ conveys the maximum of 3 bits/symbol. Similarly, for the GSSK-VLC system associated with $N_t = 8, n_t = 2$, $\mathbb{I}(h_{\text{B}}; Y)$ reaches its maximum of 4 bits/symbol, provided that the SNR is above 50 dB.

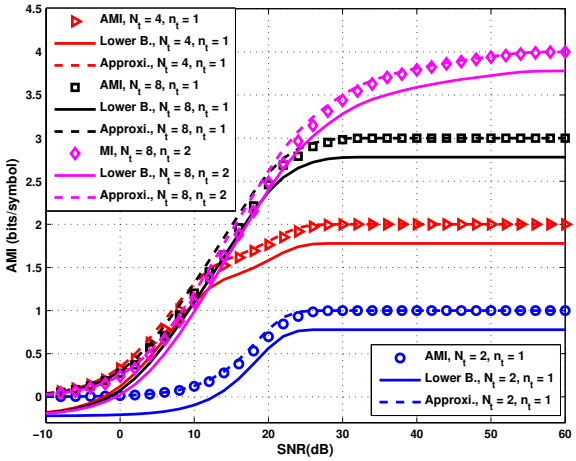


Fig. 2. Comparison of the AMI, AMI lower-bounds and AMI approximations of the Alice-to-Bob link with different setting of N_t and n_t, where $N_t = 2, 4, 8, n_t = 1$ for SSK and $N_t = 8, n_t = 2$ for GSSK. The results were calculated from (14), (17) and (22).

In Fig. 3(a) and 3(b), 3-D mesh and 2-dimensional (2-D) contour plots are provided for the AMI of $\mathbb{I}(h_{\text{B}}; Y)$ as the functions of Bob's position, when there are 4 LEDs with one activated for information transmission. By contrast, Fig. 3(c) and 3(d) demonstrate the AMI of $\mathbb{I}(h_{\text{B}}; Y)$ as the functions of Bob's position when the GSSK-VLC system using $N_t = 8, n_t = 2$ is considered. From these figures, it becomes clear that the AMI of $\mathbb{I}(h_{\text{B}}; Y)$ decreases significantly, when Bob is located in the symmetric projection areas of the 4

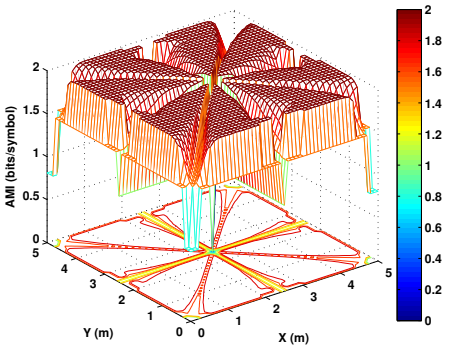
[1]Note that the BER and achievable secrecy rate are both influenced by $\Phi_{1/2}$, and they can achieve better performance with smaller $\Phi_{1/2}$. The two main reasons behind can be clarified as follows. Firstly, according to the expression of the order of Lambertian emission, the channel gain increases as $\Phi_{1/2}$ decreases, when all the other parameters are fixed. Secondly, the channel correlation decreases as $\Phi_{1/2}$ decreases.

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/ACCESS.2018.2799658, IEEE Access

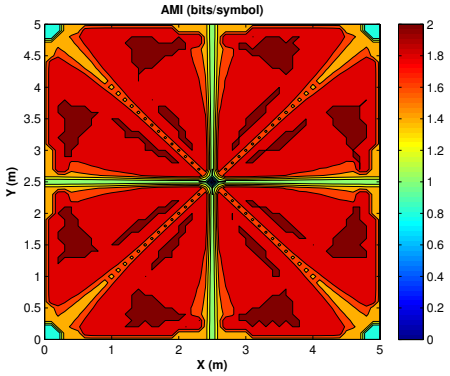
LEDs ($N_t = 4$). Specifically, when Bob is located in the symmetric area of the 4 LEDs, i.e. at the centre of the room, the AMI reaches its minimum. There are eight other symmetric regions at the coordinates formed by $x = 2.5$ m, $y = 2.5$ m, $y = x$ and $y = 5 - x$, respectively, as shown in Fig. 3(a) and 3(b), which also result in a reduced AMI. These symmetric regions are the result of the strong channel correlation between Alice and Bob. Hence future counter-measures have to be found to avoid these symmetrical areas in order to guarantee a reliable communication performance. A simple solution may be to have random LED positions. One may design the positions and parameters of the LEDs to ensure that Eve experiences the effect of symmetrical regions. Consequently, the secrecy performance may be improved. We may also reduce the number of symmetric areas by carefully arranging the LED patterns as well as beneficially configuring the transmit signalling scheme. As seen in Figs. 3(c) and 3(d), when $n_t = 2$ is used instead of $n_t = 1$ (in Figs. 3(a) and 3(b)), the symmetric areas are reduced. Furthermore, for the sake of enhancing the secrecy performance, we can activate more LEDs of the set of available LEDs.

Fig. 4 illustrates the AMI between Alice and Bob as well as that between Alice and Eve. Furthermore, the achievable secrecy rate between Alice and Bob in the SSK-VLC system associated with $N_t = 2, 4, 8$ LEDs and the GSSK-VLC system with $N_t = 8$ and $n_t = 2$ is also portrayed. We assume that Bob is located at $(2.15, 1.28, 0.85)$ m and Eve $(2.60, 0.88, 0.85)$ m. As shown in the figure, when the SNR is sufficiently high, the achievable secrecy rate approaches zero for all the four scenarios. In fact, this phenomenon always occurs regardless of where Bob and Eve are located. This is because when the SNR is sufficiently high, Eve can always intercept the confidential information sent by Alice to Bob. Although in the SNR region of $10 - 40$ dB, non-zero secrecy rate can be achieved, the secrecy rate is in general low, with the case of $N_t = 2$ and $n_t = 1$ capable of achieving the highest secrecy rate, which is slightly below 1 bit/symbol. As shown in the figure, the plots of $N_t = 4, n_t = 1$ are different from the other ones. The reason behind this lies in the following two facts. Firstly, the SSK-VLC system associated with $N_t = 4, n_t = 1$ has more symmetric regions than the other three cases, as demonstrated in Fig. 3(a)-3(d). Secondly, the secrecy performance is dependent on the positions of Bob and Eve. From the results we observe that the secrecy performance may be improved by carefully configuring the LED pattern based on our secrecy strategies.

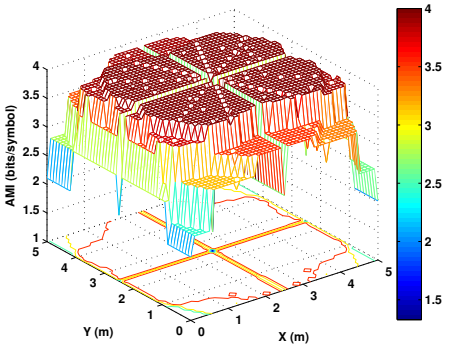
Fig. 5 shows the 3-D mesh and 2-D contour plots of the achievable secrecy rate between Alice and Bob for a SSK-VLC system associated with $N_t = 8, n_t = 1$, when Eve is located at different positions of the room. As shown in the figures, the achievable secrecy rate between Alice and Bob is nearly zero in most areas. When comparing Figs. 5(a)-5(b) with 5(c)-5(d), the near-zero secrecy rate region increases as the SNR is increased from 26 dB to 36 dB. As shown in the figure, there are some areas for Eve, where the achievable secrecy rate does not approach zero. This is because these areas belong to the symmetric areas of Eve, which result in near-zero AMI between Alice and Eve. However, these areas



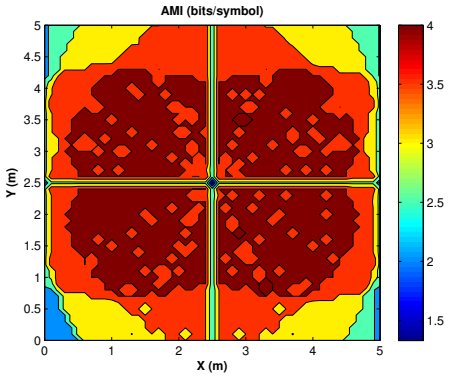
(a) $N_t = 4, n_t = 1$, 3-D mesh



(b) $N_t = 4, n_t = 1$, 2-D contour



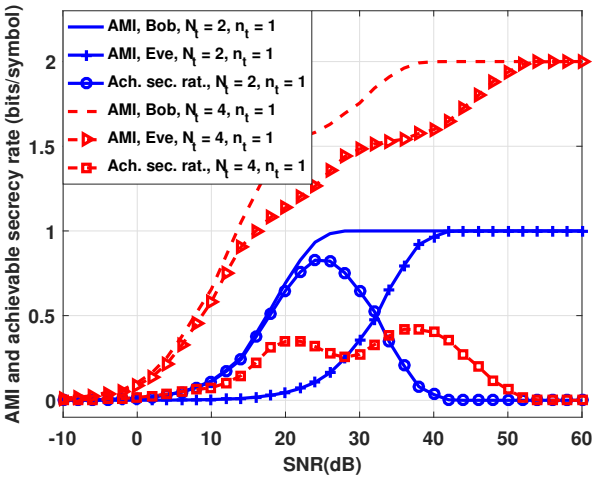
(c) $N_t = 8, n_t = 2$, 3-D mesh



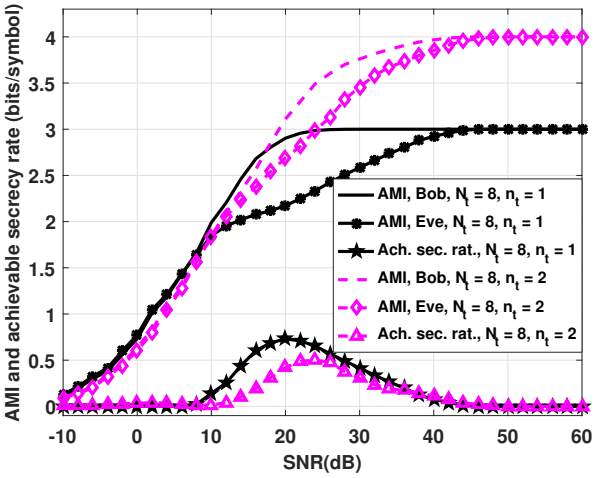
(d) $N_t = 8, n_t = 2$, 2-D contour

Fig. 3. AMI versus the location of Bob. When the LED's location are given in Table II. (a) and (b) $N_t = 4, n_t = 1$, SNR = 30 dB; (c) and (d) $N_t = 8, n_t = 2$, SNR = 60 dB. The results were calculated from (24).

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/ACCESS.2018.2799658, IEEE Access



(a)

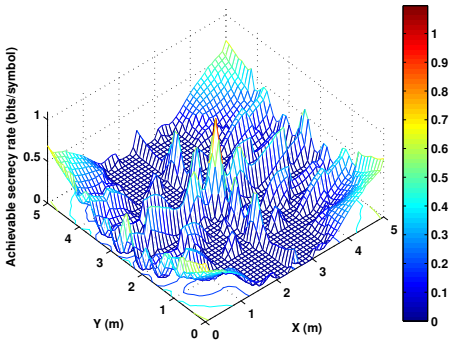


(b)

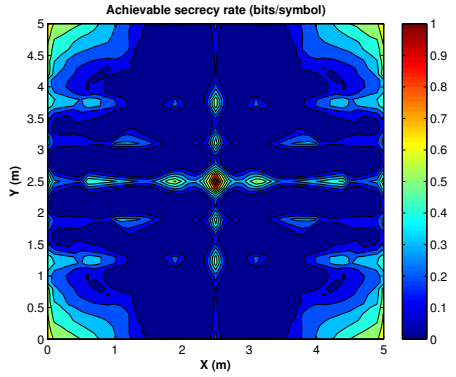
Fig. 4. AMI and achievable secrecy rate versus SNR performance of the SSK-VLC and GSSK-VLC systems. The results were calculated from (14), (15) and (24).

are not the symmetric areas of Bob. Hence, the AMI between Alice and Bob is a non-zero. Consequently, the achievable secrecy rate is positive in these areas.

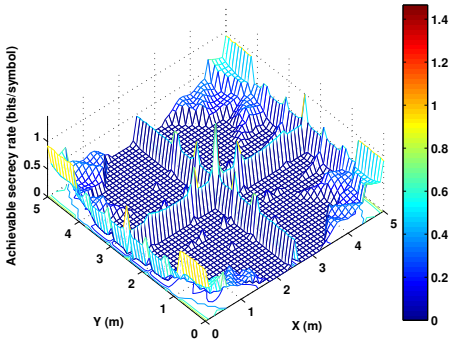
Fig. 6 compares the theoretical upper bound of (28) and the simulated BER of Bob in the GSSK-VLC systems, when ML detection is assumed, and when the locations of the LEDs are given in Table II. Observe from the plots in Fig. 6 that the BER upper bound of (28) is tight in the moderate to high SNR regions, which hence validates our theoretical analysis. As shown in the figure, the SSK system associated with $N_t = 4, n_t = 1$ slightly outperforms the GSSK system using $N_t = 4, n_t = 2$, although both of them transmit 2 bits per symbol. This is because the GSSK system suffers from higher interference due to having more activated LEDs than the SSK system, and the LED selections are fixed in the GSSK system. In practice, we will recommend $N_t = 4, n_t = 2$, if we only want to transmit 2 bits per symbol. Furthermore, if we use $N_t = 4$ and $n_t = 2$, we may exploit the redundancy



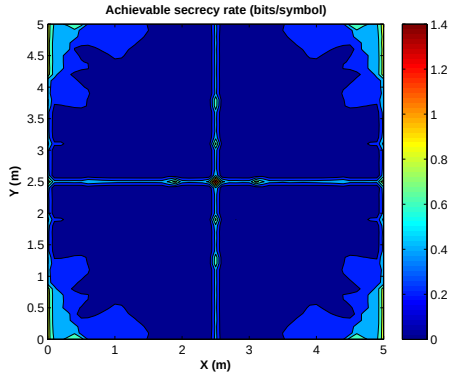
(a) SNR = 26 dB, 3-D mesh



(b) SNR = 26 dB, 2-D contour



(c) SNR = 36 dB, 3-D mesh



(d) SNR = 36 dB, 2-D contour

Fig. 5. Achievable secrecy rate versus Eve's location in a SSK-VLC system with $N_t = 8, n_t = 1$, where Bob is located at $(2.15, 1.28, 0.85)$ m. The results were calculated from (24).

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/ACCESS.2018.2799658, IEEE Access

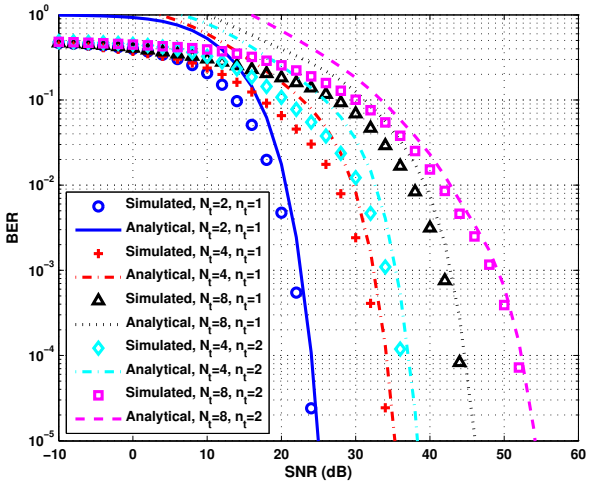


Fig. 6. Comparison of the analytical upper-bound and simulated bit error probability of Bob in the GSSK-VLC systems employing ML detection. The results were calculated from (28).

for performance enhancement. We note that in the GSSK-VLC system considered, the BER of Eve is the same as that of Bob, if Eve is at the same location as Bob. Therefore, we omit the corresponding figures for saving space.

B. Secrecy Performance Enhancement Evaluation with Optimal Selection of LEDs

Let us now turn our attention to the secrecy performance of the GSSK-VLC system relying on the proposed optimal LED pattern selection. We assume that the room is equipped with $3 \times 3 = 9$ LEDs, which are distributed on the ceiling, as depicted in Fig. 7(a). Again, the parameters of the LEDs are provided in Table I.

Firstly, we demonstrate the efficiency of the proposed optimal LED selection approach. We assume that Bob is located at $(2.15, 1.28, 0.85)$ m, and that the GSSK-VLC systems have the settings of: a) $N_t = 4, n_t = 1$; b) $N_t = 6, n_t = 1$; c) $N_t = 8, n_t = 1$; d) $N_t = 4, n_t = 2$; e) $N_t = 6, n_t = 2$; f) $N_t = 8, n_t = 2$; g) $N_t = 6, n_t = 3$; h) $N_t = 8, n_t = 3$, respectively. Then, given the proposed LED pattern selection algorithm, the optimum LED patterns of these GSSK-VLC systems are shown in Fig. 7(b) - Fig. 7(i), respectively. Correspondingly, the values of $\zeta^\star$ given in (31) can be found, as shown in Table III. In practice, these selected LED patterns can be constructed as a list for later activation. However, we should note that the optimum LED patterns are different for the different locations of Bob.

Let us now demonstrate the efficiency of the LED pattern selection, based on the optimal LED patterns of Fig. 7 for the eight GSSK-VLC systems considered. Correspondingly, the AMI between Alice and Bob is depicted in Fig. 8, along with the AMI between Alice and Bob, when random LED selections are employed. Note that, in the random selection cases, the results were obtained from 100 realizations of random selections. Observe from the results shown in Fig. 8 that when an appropriate LED pattern is chosen from the 3×3 grid, the AMI can be beneficially enhanced in the medium SNR region, in particular, when N_t is small relative to N. By contrast, when N_t is close to N, such as $N_t = 8$, the AMI difference between the optimum and random selections is negligible. As shown in the figures, when the SNR is sufficiently high, the maximum attainable rate can indeed be achieved, regardless of using random or optimum selections. It is worthwhile to note that, while the proposed LEDs pattern selection approach works well for the medium SNRs, when SNRs are higher than some thresholds for different schemes, just like systems with optimum LEDs pattern, the one with randomly selected LEDs pattern can also approach the limit of AMI. As a suggestion in applications, we can arrange as much as possible LEDs in the service environment in one hand to enhance N and consequently to guarantee the security of the system, on the other hand, N_t can be chosen to ensure the difference between N and N_t as large as possible.

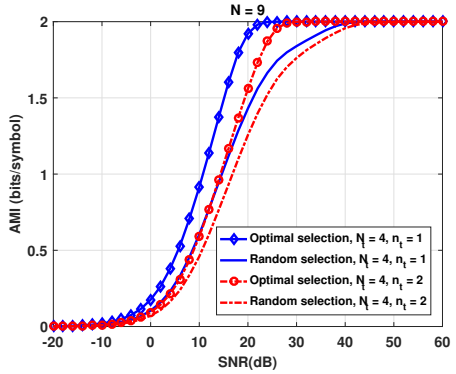
TABLE III
CONFIGURATIONS OF DIFFERENT GSSK-VLC SYSTEMS AND THE CORRESPONDING $\zeta^\star$, BOB LOCATES AT $(2.1516, 1.2768, 0.85)$ M.

GSSK-VLC systems	Configurations	$\zeta^\star$
a	$N_t = 4, n_t = 1, m = 2$	4.67×10^{-6}
b	$N_t = 6, n_t = 1, m = 2$	2.70×10^{-6}
c	$N_t = 8, n_t = 1, m = 3$	6.20×10^{-7}
d	$N_t = 4, n_t = 2, m = 2$	3.60×10^{-6}
e	$N_t = 6, n_t = 2, m = 3$	8.10×10^{-7}
f	$N_t = 8, n_t = 2, m = 4$	1.90×10^{-7}
g	$N_t = 6, n_t = 3, m = 4$	8.10×10^{-7}
h	$N_t = 8, n_t = 3, m = 5$	3.69×10^{-8}

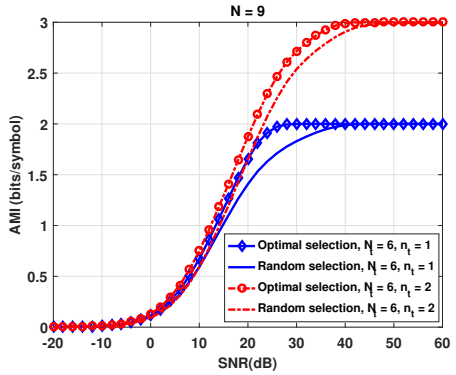
Finally, in Fig. 9 we compare the secrecy performance of the GSSK-VLC systems relying on both the optimal and on the random LED pattern selections, when the optimal patterns are shown in Fig.7, with the results presented in Table III. In the experiments, we assume that Bob and Eve are located at $(2.15, 1.28, 0.85)$ m and $(3.60, 3.90, 0.85)$ m, respectively. It can be observed from Fig. 9 that the proposed optimal LED selection scheme is indeed efficient in all the cases. The achievable secrecy rate of the optimal LED pattern selection is always higher than that of the random LED pattern selection. Furthermore, upon increasing N_t, the secrecy rate benefit of LED selection decreases, in line with the observations drawn from Fig. 8. Additionally, the achievable secrecy rate decreases, when the SNR is increased in order to exceed some thresholds, which approaches zero, when the SNR is sufficiently high.

As shown in Fig. 8 and Fig. 9, for certain available N LEDs, when $N_t \geq \frac{2}{3}N$, the Bob's AMI difference between random selections and optimal selections are negligible no matter the values of SNRs, such as in Fig. 8 (c) and Fig. 8 (d) (for the case of $N_t = 8$). Similarly, in Fig. 9 (d), the enhancement of achievable secrecy rate by the proposed optimal selections is also very limited for certain medium SNRs. Hence, in practice in order to increase the secrecy of the considered GSSK-VLC systems, we can arrange as much as possible LEDs in the service area to satisfy the requirement of $N_t \leq \frac{2}{3}N$, and simultaneously at certain SNR ranges, such as 15 dB $\sim$ 40 dB. Actually, in application environments, in order to

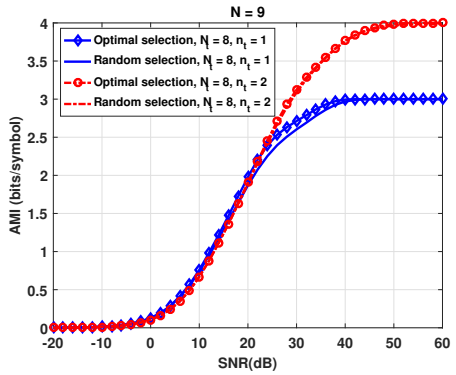
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2799658, IEEE Access



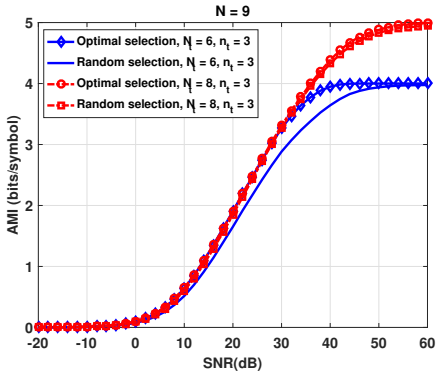
(a) System (a) and (d) in Table III



(b) System (b) and (e) in Table III



(c) System (c) and (f) in Table III



(d) System (g) and (h) in Table III

Fig. 8. Comparison of AMI achieved by the GSSK-VLC systems with optimal and random LED pattern selection, when Bob is located at $(2.15, 1.28, 0.85)$ m. The results were calculated from (14).

guarantee the adequate illumination, there are many LEDs equipped on the ceiling of the service environment, making that N is very large. In this case, N_t can be chosen with more freedom to ensure the difference between N and N_t as large as possible. Furthermore, we can conclude that when the difference between the number of available LEDs N and N_t is large enough, i.e., $N \geq \frac{3}{2}N_t$, the optimal selection method proposed in this paper can provide an enhance secrecy of the GSSK-VLC systems, while the SNRs lies in some medium regions simultaneously, such as 15 dB $\sim$ 40 dB.

VI. Conclusions

By exploiting the distinguishing features of GSSK-VLC systems, we considered their PLS issues and quantified the secrecy performance as well as its potential enhancement. Firstly, we used the finite discrete distributions subject to amplitude constraints and analyzed the secrecy performance of the proposed GSSK-VLC systems. We observed that without using extra secrecy enhancement strategies, Eve is capable of intercepting the confidential signals at high SNR, even if the channel condition are worse than those of Bob, hence resulting in a poor secrecy performance. Moreover, if the Alice-to-Bob channel is degraded, the system is unable to support confidential communication. Then, an optimal LED pattern selection algorithm was proposed for enhancing the secrecy performance of GSSK-VLC systems, specifically in the medium SNR region. Our studies demonstrated that the proposed LED pattern selection algorithm is capable of improving the achievable secrecy rate of Bob. In this paper, a range of analytical results were obtained and all the analytic results were verified by computer simulations.

Appendix

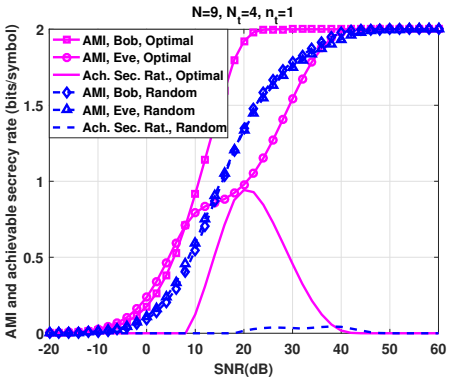
A. Proof of Theorem 1

Based on (10)-(13), $\mathbb{I}(h_{\mathrm{B}}; Y)$ can be derived as

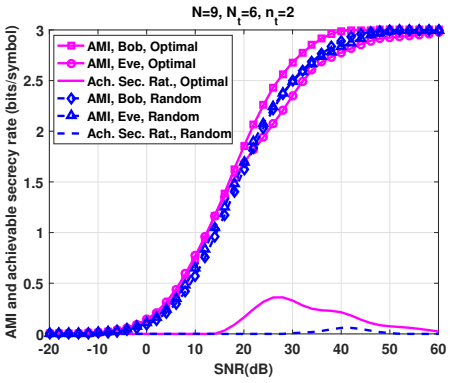
$$\begin{aligned}\mathbb{I}(h_{\mathrm{B}}; Y) &= \sum_{\omega=1}^{M} \int_{y} p_{Y,h_{\mathrm{B}}}(h = h_{\mathrm{B}(\omega)}, y) \\ &\qquad \times \log_2 \frac{p_{Y|h_{\mathrm{B}}}(y|h_{\mathrm{B}} = h_{\mathrm{B}(\omega)})}{p_Y(y)} dy \\ &= \log_2 M - \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(\Theta_3\right) \right],\end{aligned} \tag{32}$$

where we define $\Theta_3 = \frac{w_{\mathrm{B}}^2 - (w_{\mathrm{B}} + (h_{\mathrm{B}(\omega)} - h_{\mathrm{B}(\varpi)})s)^2}{2\sigma_{\mathrm{B}}^2}$. When denoting $\zeta_{\omega,\varpi} = h_{\mathrm{B}(\omega)} - h_{\mathrm{B}(\varpi)}$, the AMI between Alice and Bob in the GSSK-VLC systems having finite discrete inputs can be expressed as

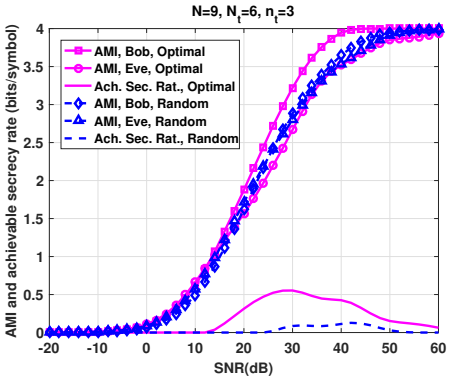
$$\begin{aligned}\mathbb{I}(h_{\mathrm{B}}; Y) &= \log_2 M \\ &\quad - \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(\frac{w_{\mathrm{B}}^2 - (w_{\mathrm{B}} + \zeta_{\omega,\varpi} s)^2}{2\sigma_{\mathrm{B}}^2} \right) \right] \\ &= \log_2 M - \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(\Theta_1\right) \right].\end{aligned} \tag{33}$$



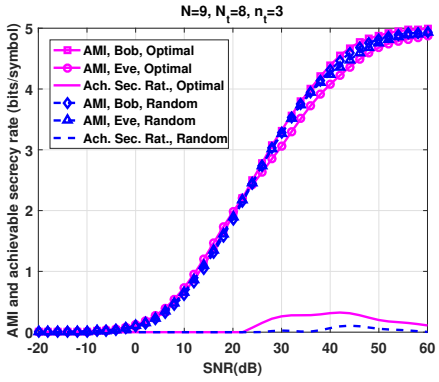
(a) System (a) in Table III



(b) System (e) in Table III



(c) System (g) in Table III



(d) System (h) in Table III

Fig. 9. Comparison of achievable secrecy performance of GSSK-VLC systems with respectively the optimal and random LED pattern selections. The results were calculated from (14), (15) and (24).

For a given $\zeta_{\omega,\varpi}$ and s, the AMI of (33) is a monotonically increasing function of the SNR ϱ_{B}. When $\varrho_{\mathrm{B}} \to \infty$, i.e., $\sigma_{\mathrm{B}}^2 = 0$, we have

$$\lim_{\varrho_{\mathrm{B}} \to \infty} \mathbb{I}(h_{\mathrm{B}}; Y) = \log_2 M, \tag{34}$$

which implies that the upper bound AMI of the Alice-to-Bob channel is $\log_2 M$.

In the same way, when denoting $\xi_{\omega,\varpi} = h_{\mathrm{E}(\omega)} - h_{\mathrm{E}(\varpi)}$, the AMI of the Alice-to-Eve channel can be expressed as

$$\mathbb{I}(h_{\mathrm{E}}; Z) = \log_2 M - \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{E}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(\Theta_2\right) \right]. \tag{35}$$

B. Proof of Theorem 2

From (33), we have

$$\begin{aligned}
\mathbb{I}(h_{\mathrm{B}}; Y) &= \log_2 M \\
&\quad - \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(\frac{w_{\mathrm{B}}^2}{2\sigma_{\mathrm{B}}^2} - \frac{\left(w_{\mathrm{B}} + \zeta_{\omega,\varpi} s\right)^2}{2\sigma_{\mathrm{B}}^2} \right) \right] \\
&= \log_2 M - \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\log_2 \exp\left(\frac{w_{\mathrm{B}}^2}{2\sigma_{\mathrm{B}}^2} \right) \right] \\
&\quad - \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\log_2 \sum_{\varpi=1}^{M} \exp\left(- \frac{\left(w_{\mathrm{B}} + \zeta_{\omega,\varpi} s\right)^2}{2\sigma_{\mathrm{B}}^2} \right) \right] \\
&= \log_2 M - I_1 - I_2.
\end{aligned} \tag{36}$$

In (36), the second term at the right-hand-side (RHS), respectively, I_1, can be simplified to

$$\begin{aligned}
I_1 &= \frac{1}{M} \sum_{\omega=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\log_2 \exp\left(\frac{w_{\mathrm{B}}^2}{2\sigma_{\mathrm{B}}^2} \right) \right] \\
&= \log_2 e \; \mathbb{E}_{w_{\mathrm{B}}} \left[\frac{w_{\mathrm{B}}^2}{2\sigma_{\mathrm{B}}^2} \right] \\
&= \frac{1}{2} \log_2 e.
\end{aligned} \tag{37}$$

With the aid of the concavity of $\log_2(\cdot)$, the third term at the RHS of (36), namely, I_2, can be upper bounded by applying Jensen's inequality as

$$\begin{aligned}
I_2 &\le \frac{1}{M} \sum_{\omega=1}^{M} \log_2 \sum_{\varpi=1}^{M} \mathbb{E}_{w_{\mathrm{B}}} \left[\exp\left(- \frac{\left(w_{\mathrm{B}} + \zeta_{\omega,\varpi} s\right)^2}{2\sigma_{\mathrm{B}}^2} \right) \right] \\
&= \frac{1}{M} \sum_{\omega=1}^{M} \log_2 \sum_{\varpi=1}^{M} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{B}}} \exp\left(- \frac{w_{\mathrm{B}}^2}{2\sigma_{\mathrm{B}}^2} \right) \\
&\qquad \times \exp\left(- \frac{\left(w_{\mathrm{B}} + \zeta_{\omega,\varpi} s\right)^2}{2\sigma_{\mathrm{B}}^2} \right) dw_{\mathrm{B}} \\
&= -\frac{1}{2} + \frac{1}{M} \sum_{\omega=1}^{M} \log_2 \sum_{\varpi=1}^{M} \exp\left(- \frac{\left(\zeta_{\omega,\varpi} s\right)^2}{4\sigma_{\mathrm{B}}^2} \right).
\end{aligned} \tag{38}$$

Consequently, upon substituting (37) and (38) into (36), we obtain

$$\begin{aligned}\mathbb{I}(h_{\mathrm{B}};Y) &= \log_2 M - I_1 - I_2 \\ &\geq \log_2 M - \frac{1}{2}(\log_2 e - 1) \\ &\quad - \frac{1}{M}\sum_{\omega=1}^{M}\log_2 \sum_{\varpi=1}^{M}\exp\left(-\frac{\varrho_{\mathrm{B}}(\zeta_{\omega,\varpi}s)^2}{4}\right). \quad (39)\end{aligned}$$

Similarly, by following the same procedure as that for deriving (17), we can derive the lower-bound of (18).

REFERENCES

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

[2] R. Zhang, J. Wang, Z. Wang, Z. Xu, C. Zhao, and L. Hanzo, "Visible light communications in heterogeneous networks: Paving the way for user-centric design," *IEEE Wireless Commun.*, vol. 22, no. 2, pp. 8–16, Apr. 2015.

[3] R. Zhang, H. Claussen, H. Haas, and L. Hanzo, "Energy efficient visible light communications relying on amorphous cells," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 894–906, Apr. 2016.

[4] R. D. Dupuis and M. R. Krames, "History, development, and applications of high-brightness visible light-emitting diodes," *J. Lightw. Technol.*, vol. 26, no. 9, pp. 1154–1171, May 2008.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[6] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 2017.

[7] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

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

[9] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2016.

[11] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4449–4461, Oct. 2009.

[12] A. Chaaban, J. M. Morvan, and M. S. Alouini, "Free-Space optical communications: Capacity bounds, approximations, and a new sphere-packing perspective," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1176–1191, Mar. 2016.

[13] R. Jiang, Z. Wang, Q. Wang, and L. Dai, "A tight upper bound on channel capacity for visible light communications," *IEEE Commun. Lett.*, vol. 20, no. 1, pp. 97–100, Jan. 2016.

[14] S. Ma, R. Yang, H. Li, Z. L. Dong, H. Gu, and S. Li, "Achievable rate with closed-form for SISO channel and broadcast channel in visible light communication networks," *J. Lightw. Technol.*, vol. 35, no. 14, pp. 2778–2787, Jul. 2017.

[15] A. Chaaban, Z. Rezki, and M. S. Alouini, "Fundamental limits of parallel optical wireless channels: Capacity results and outage formulation," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 296–311, Jan. 2017.

[16] A. Mostafa and L. Lampe, "Physical-Layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[17] S. Ma, Z. L. Dong, H. Li, Z. Lu, and S. Li, "Optimal and robust secure beamformer for indoor MISO visible light communication," *J. Lightw. Technol.*, vol. 34, no. 21, pp. 4988–4998, Nov. 2016.

[18] A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," *IEEE Trans. Signal Process.*, vol. 64, no. 24, pp. 6501–6516, Dec. 2016.

[19] ——, "Securing visible light communications via friendly jamming," in *Proc. IEEE Globecom Wkshps'2014*, Dec. 2014, pp. 524–529.

[20] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *Proc. IEEE GLOBECOM'2016*, Dec. 2016, pp. 1–7.

[21] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with amplitude and variance constraints," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5553–5563, Oct. 2015.

[22] W. O. Popoola, E. Poves, and H. Haas, "Error performance of generalised space shift keying for indoor visible light communications," *IEEE Trans. Commun.*, vol. 61, no. 5, pp. 1968–1976, May 2013.

[23] W. O. Popoola and H. Haas, "Demonstration of the merit and limitation of generalised space shift keying for indoor visible light communications," *J. Lightw. Technol.*, vol. 32, no. 10, pp. 1960–1965, May 2014.

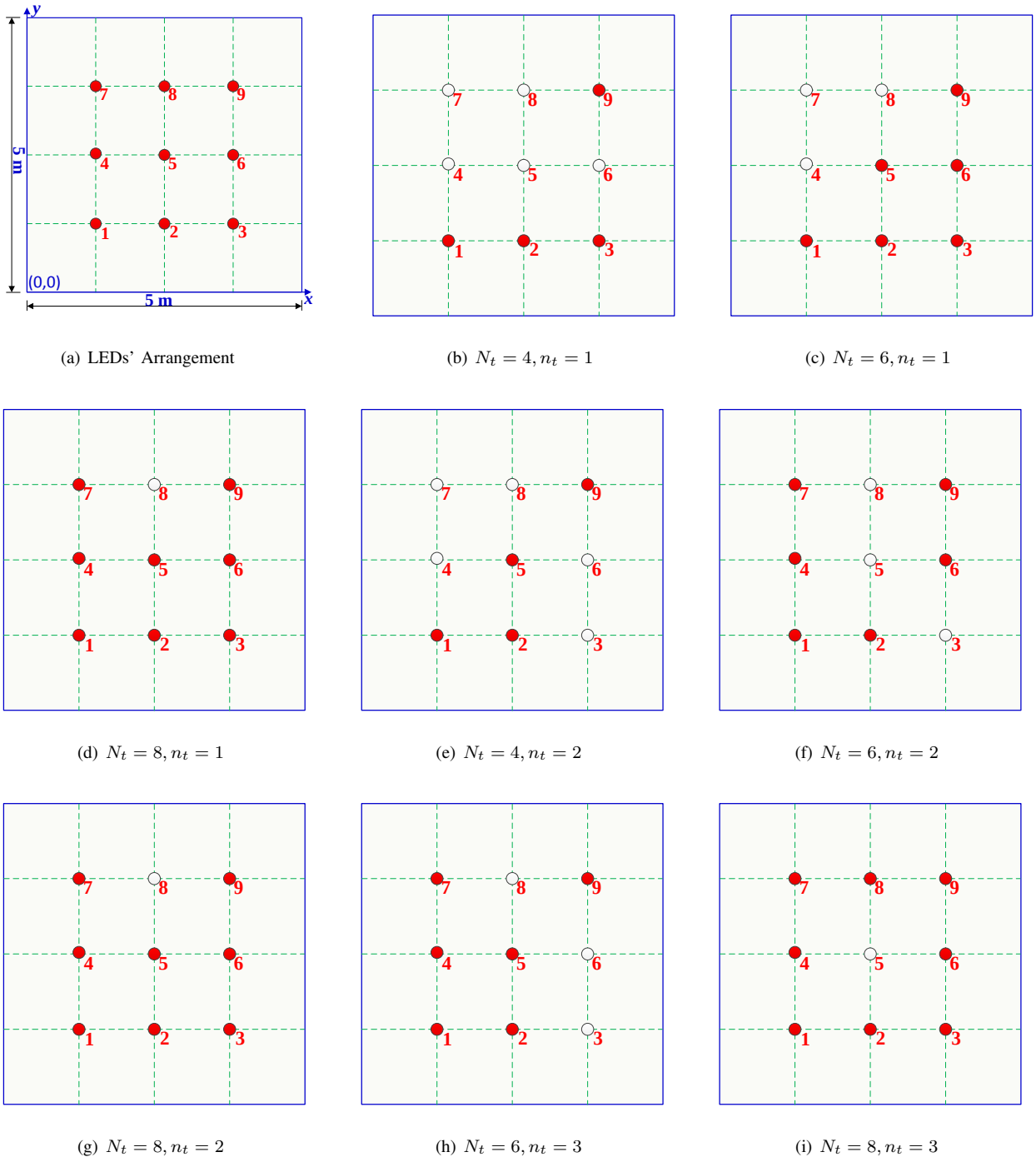
[24] T. Fath and H. Haas, "Performance comparison of MIMO techniques for optical wireless communications in indoor environments," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 733–742, Feb. 2013.

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

[26] J. G. Proakis and M. Salehi, *Digital communications*. New York, NY, USA: McGraw-Hill, 2008.

[27] M. Chiani, D. Dardari, and M. K. Simon, "New exponential bounds and approximations for the computation of error probability in fading channels," *IEEE Trans. Wireless Commun.*, vol. 2, no. 4, pp. 840–845, Jul. 2003.

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/ACCESS.2018.2799658, IEEE Access



(a) LEDs' Arrangement (b) $N_t = 4, n_t = 1$ (c) $N_t = 6, n_t = 1$

(d) $N_t = 8, n_t = 1$ (e) $N_t = 4, n_t = 2$ (f) $N_t = 6, n_t = 2$

(g) $N_t = 8, n_t = 2$ (h) $N_t = 6, n_t = 3$ (i) $N_t = 8, n_t = 3$

Fig. 7. Locations of $N = 9$ LEDs (a) on the ceiling and the optimum selected LED patterns for the N_t and n_t as specified, when Bob is located at $(2.15, 1.28, 0.85)$ m. In the figures, circles denote LEDs, filled circles represent the LEDs selected and blank ones indicate the LEDs not chosen. The number besides a circle represents the index of the LED.