Secrecy Sum-Rate of Multi-User MISO Visible Light Communication Systems with Confidential Messages

Thanh V. Pham and Anh T. Pham

Graduate Department of Computer and Information, The University of Aizu, Aizuwakamatsu, Japan.

Abstract

This paper studies the information theoretic secrecy sum-rate for multi-user multiple-input single-output (MU-MISO) visible light communication (VLC) systems with confidential messages. The well-known Zero-Forcing (ZF) precoding method is employed to ensure confidentiality among legitimate users and, at the same time, to prevent eavesdropper(s) from obtaining any information. Different from radio frequency (RF) counterpart wherein the average input power constraint is usually imposed on the derivation of channel capacity, the input data signal of VLC systems is amplitude constrained, leading to a peak input power constraint. The amplitude constraint gives rise to the complexity in obtaining an analytical expression for the capacity. In this paper, we analytically investigate a novel bound on the secrecy sum-rate of all legitimate users in MU-MISO VLC systems, which is valid in high signal-to-noise ratio (SNR) regime. The secrecy sum-rate performance is then derived for two scenarios: known and unknown eavesdropper's channel state information (CSI) at the transmitter.

Keywords: VLC, multi-user MISO, physical layer security, linear precoding.

1. Introduction

Over the past few years, it has been witnessed an explosion in research and development of visible light communication (VLC) technology in both academia and industry. As the demand for high data-rate wireless transmission continues to increase tremendously, VLC is indeed an attractive solution to cope with the problem. Operating at unregulated and free frequencies, VLC also effectively addresses the spectrum scarcity problem in radio frequency (RF) systems [1–4].

Thanks to the fact that LEDs are practically used for both illumination and communications purposes, the employment of multiple-input multiple-output (MIMO) technique is a logical solution to increase the data-rate and the coverage of VLC systems [3–6]. As a natural progression for the single-user MIMO configuration, MIMO VLC systems, especially its popular case of multi-input single-output (MISO) ones, supporting multiple users (MU) have recently received a great deal of attention. The popularity of MISO VLC systems is due to the fact that the single-output, i.e., only one photodiode (PD) is used at the receiver, is more practically feasible to be implemented on a mobile device, which is one of the main targets of the VLC technology. Our study in this paper therefore also focuses on this particular system. In previous studies on broadcast MU-MISO VLC systems, to improve the overall performance, two typical linear precoding techniques at the transmitter, namely: Zero-Forcing (ZF) [7–9] and Minimum Mean Square Error (MMSE) [10, 11], were investigated for different system configurations and performance measures.

Together with improving the performance, enhancing the security and privacy in VLC systems is another major concern as well. As a matter of fact, VLC systems have been considered offering higher security than RF systems due to light-of-sight (LOS) propagation and confinement of light signal by opaque surfaces. The threat of eavesdropping by malicious user is, nevertheless, still visible within the illuminated area, especially in the presence of multiple users. Besides traditional encryption techniques at the network layer, the interest in physical layer security (PLS) has been emerged drastically as a promising approach to further enhance user's confidentiality. The idea of PLS was initiated by Wyner [12]. In this work, Wyner introduced the *wiretap channel*, which consists of one transmitter, one legitimate user and one eavesdropper (unauthorized user). The *secrecy capacity* (or *secrecy rate*) was then defined as the maximum reliable rate between the transmitter and the legitimate user at which the transmitted message can not be decoded by the eavesdropper. In particular for the Gaussian channel, the secrecy capacity is the difference between the capacitity of the legitimate user and that of the eavesdropper's channels [13].

Compared to the extensive study on PLS in RF communications, there are only a few studies on PLS in VLC systems [14–21]. In [14, 15], the typical wiretap channel (i.e., one legitimate user and one eavesdropper) was examined in the context of VLC channels. These studies utilized linear precoding approach to improve the secrecy rate performance. Upper and lower bounds for the secrecy rate of single-input single-output (SISO) configuration were first derived as benchmarks. For MISO systems, ZF precoding was adopted to zero-force eavesdropper's reception and an achievable secrecy rate was obtained for both cases of perfect and imperfect channel state information (CSI). The authors in [16] consider a more general configuration by having an arbitrary number of eavesdroppers. The precoding strategy again was used. In addition to precoding technique, *artificial noise* is another method to increase security level. Jamming signal (i.e., artificial noise), which causes no interference to the legitimate user is added to the transmitted signal for degrading eavesdropper's reception, thus increasing the secrecy rate. It should be noted that input distribution of the jamming signal impacts considerably on the overall secrecy performance. Specifically, the uniform distribution was investigate in [17, 18]. On the other hand, the studies in [19, 20], respectively, showed that using the truncated Gaussian or the truncated generalized normal distribution for jamming signal can achieve better secrecy rate. For a scenario wherein a massive number (e.g., few thousands) of LEDs are deployed, an approach called *pattern synthesis* was proposed in [21]. By exploiting the excessive spatial degrees of freedom offered by the large number of LEDs and defining an insecurity zone, it is possible to shape a radiation pattern whose the main lobe is directed towards the legitimate user while achieving arbitrary small signal everywhere outside the insecurity zone. It should be noted that previous studies mainly focused on the scenario of single legitimate user. Only the study in [21] considered the MU VLC systems, however, with the aforementioned special LEDs setup, and the confidentiality among users was also ignored.

In this paper, we therefore focus on PLS issue in MU-MISO VLC systems with confidential messages, i.e., messages among users must be kept confidential from each other and also from the eavesdropper. To achieve the goal of confidentiality among users, ZF precoding technique is adopted due to its computational advantage and very good performance at high signal-to-noise ratio (SNR) region [22]. For this multiple legitimate user configuration, we are interested in characterizing the achievable secrecy sum-rate under the confidential message constraint. Specifically, we investigate lower bounds on the secrecy sum-rate of users for both cases of known and unknown eavesdropper's CSI at the transmitter. It is important to note that, unlike RF counterpart wherein the average input power constraint is usually imposed, the practical intensity modulating signal in VLC is inherently non-negative and has a limited linear range. This results in an amplitude constraint on the input data signal, which eventually leads to a peak input power constraint. The amplitude signal constraint gives rise to difficulty in obtaining an analytical expression for the capacity. As a matter of fact, Smith did show that the capacity-achieving distribution for an amplitude-constrained scalar Gaussian channel is discrete with a finite number of mass points [23]. From this result, a quite complicated numerical procedure was developed to compute the capacity. In this study, rather than relying on numerical algorithms, we provide a simple closed-form lower bound for the capacity, which is valid in high SNR regime (the condition that is usually available in VLC systems). Based on the bound, the maximum secrecy sum-rate problems are formulated as convex optimization problems, which can be solved efficiently by using standard optimization packages.

The rest of the paper is structured as follows. In Section II, the MU-MISO VLC system model with the ZF precoding technique are introduced. We revisit the capacity of amplitude-constrained scalar Gaussian channels and derive two lower bounds as benchmarks in Section III. Section IV investigates the secrecy sum-rate performance for two scenarios: known and unknown eavesdropper's CSI at the transmitter. Numerical results and discussions are presented in Section V. Finally, Section VI concludes the paper.

Notation: The following notations are used throughout the paper. Bold upper case letters represent matrices (e.g., $\mathbf{A}$). The transpose of matrix $\mathbf{A}$ is written as $\mathbf{A}^T$, while $[\mathbf{A}]_{k,:}$ denotes the $k-$th row of $\mathbf{A}$. $\|\cdot\|_1$ is the L_1 norm operator and $\mathbb{R}$ is the real number set. $\mathbb{I}(\cdot;\cdot)$ and $h(\cdot)$ represent the mutual information and the differential entropy in *nats*, respectively. Expected value is denoted by $\mathbb{E}[\cdot]$ and the natural logarithm $\log(\cdot)$ is used. Finally, $|\cdot|$ is the absolute value operator.

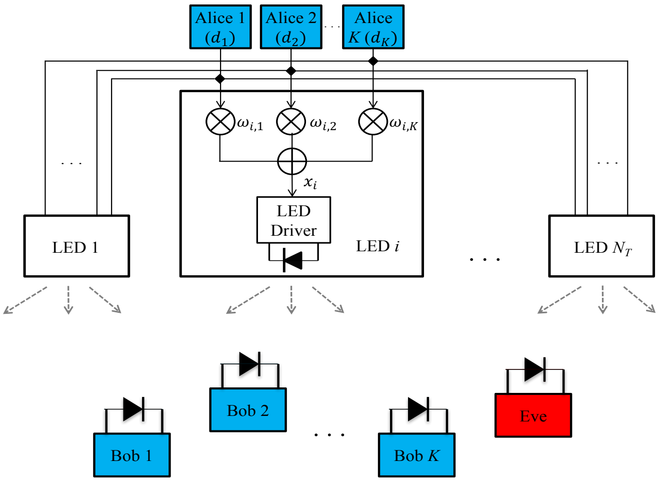

Fig. 1: MU-MISO VLC system with N_T LED arrays for K non-cooperative legitimate pairs of user (Alice and Bob) with mutual confidentiality, and one Eavesdropper (Eve).

2. MU-MISO VLC System Model

2.1. VLC Channel

Fig. 1 illustrates the schematic diagram of a MU-MISO VLC system with N_T LED arrays (transmitting units) for K non-cooperative legitimate pairs of user (Alice and Bob) with mutual confidentiality, and one Eavesdropper (Eve). We denote $\mathbf{H}_k \in \mathbb{R}^{1\times N_T}$ as the channel matrix between the LED arrays and the k-th user

$$\mathbf{H}_k = \begin{bmatrix} h_{k1} & h_{k2} & \cdots & h_{kN_T} \end{bmatrix}, \tag{1}$$

where h_{ki} represents the DC gain between the user and the $i-$th LED array. For indoor VLC systems, there are generally two main types of link model, which are the direct light-of-sight (LOS) and the non-direct line-of-sight (NLOS). In most cases, only LOS link is taken into account since it accounts for more than 95% of the total received optical power at the receiver [24]. For the sake of simplicity, we thus consider the LOS propagation path in this study. For the LOS link, h_{ki} is given by [24]

$$h_{ki} = \begin{cases} \frac{(l+1)D}{2\pi d_{ki}^2}\cos^l(\phi)T_s(\psi_{ki})g(\psi_{ki})\cos(\psi_{ki}) & , 0 \le \psi_{ki} \le \Psi_c, \\ 0 & , \psi_{ki} > \Psi_c, \end{cases} \tag{2}$$

where l is the order of Lambertian emission determined by the semi-angle for half illuminance of the LEDs $\Phi_{1/2}$ as $l = \frac{-\log(2)}{\log(\cos\Phi_{1/2})}$. D and d_{ki} are the active area of the PD and the distance from the LED array to the user, respectively. ψ_{ki} is the angle of incidence, $T_s(\psi_{ki})$ is the gain of optical filter and Ψ_c denotes the optical field of view (FOV) semi-angle of the PD. ϕ is the angle of irradiance with respect to the transmitter axis. $g(\psi_{ki})$ is the gain of optical concentrator, which is given by

$$g(\psi_{ki}) = \begin{cases} \frac{\kappa^2}{\sin^2 \Psi_c} & , 0 \leq \psi_{ki} \leq \Psi_c, \\ 0 & , \psi_{ki} > \Psi_c, \end{cases} \tag{3}$$

where κ is the refractive index of the concentrator.

2.2. Precoding Model and Broadcast Transmission

Let $d_i \in \mathbb{R}$ be the data symbol intended for the $i-$th user which must be kept secretly from other users and the eavesdropper. It is assumed that d_i is zero-mean and is normalized to the range of $[-1, 1]$. At the $k-$th LED array, d_i is multiplied by a well-designed precoder $w_{k,i} \in \mathbb{R}$. Therefore, the precoded data signal for the $k-$th LED array is given by

$$x_k = \sum_{i=1}^{K} w_{k,i} d_i. \tag{4}$$

It is noted that x_k can take on negative values which are not valid for the drive current of the LEDs. To generate a non-negative drive current, a DC bias current should be added to x_k, e.g.,

$$s_k = x_k + I_{\text{DC}}^k, \tag{5}$$

where I_{DC}^k denotes the DC bias current for the $k-$th LED array. Since $\mathbb{E}[d_k] = 0$, the signal x_k does not affect the average illumination level of the LEDs. Instead, it is uniquely determined by the DC bias current I_{DC}^k. The received optical signal at the $k-$th user can then be written as

$$P_r^k = \mathbf{H}_k \mathbf{P}_s, \tag{6}$$

where $\mathbf{P}_s = \begin{bmatrix} P_s^1 & P_s^2 & \dots & P_s^{N_T} \end{bmatrix}^T \in \mathbb{R}^{N_T \times 1}$ is the transmitted optical power vector of the LED arrays whose element $P_s^k = \eta s_k$ is the transmitted power of the $k-$th LED array with η is the LED conversion factor.

2.2.1. Legitimate Users

If we define $\mathbf{s} = \begin{bmatrix} s_1 & s_2 & \dots & s_K \end{bmatrix}^T \in \mathbb{R}^{K \times 1}$ as the transmitted signal vector and $\mathbf{I}_{\text{DC}} = \begin{bmatrix} I_{\text{DC}}^1 & I_{\text{DC}}^2 & \dots & I_{\text{DC}}^K \end{bmatrix}^T \in \mathbb{R}^{K \times 1}$ as the aggregate DC vector, the received signal at the $k-$th legitimate user after the optical-electrical conversion is given by

$$\begin{aligned} y_k &= \gamma P_r^k + n_k = \gamma\eta \mathbf{H}_k \mathbf{s} + n_k \\ &= \gamma\eta \left(\mathbf{H}_k \mathbf{W}_k d_k + \mathbf{H}_k \sum_{i=1, i \neq k}^{K} \mathbf{W}_i d_i + \mathbf{H}_k \mathbf{I}_{\text{DC}} \right) + n_k, \end{aligned} \tag{7}$$

where γ is the PD responsivity, $\mathbf{W}_k = \begin{bmatrix} w_{1,k} & w_{2,k} & \dots & w_{N_T,k} \end{bmatrix}^T \in \mathbb{R}^{N_T \times 1}$ is the precoder for the $k-$th user. If we write $\mathbf{W} = \begin{bmatrix} \mathbf{W}_1 & \mathbf{W}_2 & \dots \mathbf{W}_K \end{bmatrix} \in \mathbb{R}^{N_T \times K}$, $\mathbf{W}$ can also be represented as $\mathbf{W} = \begin{bmatrix} \overline{\mathbf{W}}_1 & \overline{\mathbf{W}}_2 & \dots & \overline{\mathbf{W}}_{N_T} \end{bmatrix}^T$ whose element $\overline{\mathbf{W}}_k = \begin{bmatrix} w_{k,1} & w_{k,2} & \dots & w_{k,K} \end{bmatrix} \in \mathbb{R}^{1 \times K}$ is the precoder for the $k-$th LED array. n_k denotes the receiver noise which is assumed to be additive white Gaussian noise (AWGN) with zero mean and variance σ_k^2 given by

$$\sigma_k^2 = 2e\overline{P_r^k}B + 4\pi e D \gamma \chi_{\text{amb}}(1 - \cos(\Psi_c))B + i_{\text{amb}}^2 B, \tag{8}$$

where e is the elementary charge, B denotes the system bandwidth and $\overline{P_k^r} = \mathbb{E}[P_r^k] = \eta \mathbf{H}_k \mathbf{I}_{\text{DC}}$ is the average received optical power at the $k-$ th user. i_{amp}^2 is the pre-amplifier noise current density, χ_{amp} is the ambient light photocurrent. After removing the DC current $\mathbf{H}_k \mathbf{I}_{\text{DC}}$ by AC coupling, the received signal can be written by

$$y_k = \gamma \eta \left(\mathbf{H}_k \mathbf{W}_k d_k + \mathbf{H}_k \sum_{i=1, i \neq k}^{K} \mathbf{W}_i d_i \right) + n_k. \tag{9}$$

The term $\mathbf{H}_k \sum_{i=1, i \neq k}^{K} \mathbf{W}_i d_i$ is the multi-user interference (MUI) which causes degradation in the overall performance of the system. Moreover, the MUI poses a risk of confidential compromise among users since each user can receive data symbols of other users. In order to ensure the confidentiality among users, zero-forcing (ZF) precoding technique is used to completely eliminate the MUI. To do so, the precoding matrix $\mathbf{W}_i$ of the $i-$th user is constructed to be orthogonal to the channel matrices of other users, i.e.,

$$\mathbf{H}_k \mathbf{W}_i = 0 \ \ \forall \ k \neq i. \tag{10}$$

As a result, the received signal at the $k-$th user can be rewritten as

$$y_k = \gamma \eta \mathbf{H}_k \mathbf{W}_k d_k + n_k. \tag{11}$$

2.2.2. Eavesdropper

Since ZF precoding matrices are designed for legitimate users, the received signal at the eavesdropper is expressed by

$$y_e = \gamma \eta \mathbf{H}_e \sum_{i=1}^{K} \mathbf{W}_i d_i + n_e, \tag{12}$$

where $\mathbf{H}_e$ and n_e are the channel matrix and the receiver noise of the eavesdropper, respectively.

2.3. Amplitude Constraint on VLC Signal

In this section, we briefly clarify practical constraints in VLC systems, which are fundamentally different from their RF counterpart. Firstly, as mentioned in

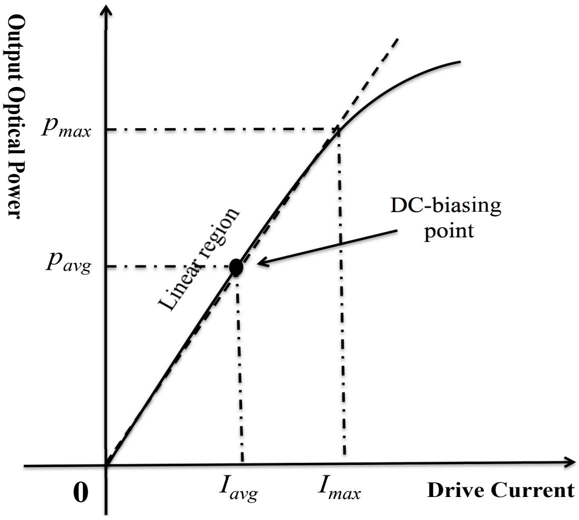

Fig. 2: Nonelinear LED transfer characteristic.

Eq. (5), the input current for LED chips must not be negative which results in an addition of a DC bias current. Secondly, as shown in Fig. 2, the LEDs exhibit a limited linear range, where the output optical power increases linearly from 0 to $p_{\max}$ corresponding to an input drive current from 0 to $I_{\max}$. Therefore, to guarantee a normal operation of the LEDs as well as to maintain a high energy efficiency, the drive current s_k should be constrained with the range of $[0, I_{\max}]$ as

$$0 \leq x_k + I_{\mathrm{DC}}^k \leq I_{\max}. \tag{13}$$

From Eq. (4) and since $|d_k| \leq 1$, we obtain

$$-\|\overline{\mathbf{W}}_k\|_1 \leq x_k \leq \|\overline{\mathbf{W}}_k\|_1. \tag{14}$$

To ensure both (13) and (14), the following constraint should be imposed

$$\|\overline{\mathbf{W}}_k\|_1 \leq \Delta_k, \tag{15}$$

where $\Delta_k = \min\left(I_{\mathrm{DC}}^k, I_{\max} - I_{\mathrm{DC}}^k\right)$. For convenience of the subsequent analysis, we can write the above constraint with respect to $\mathbf{W}_k$ as follows

$$\sum_{i=1}^{K} \left\|[\mathbf{W}_i]_{k,:}\right\|_1 \leq \Delta_k. \tag{16}$$

In the following part, the constraints in (10) and (16) are taken into account when designing the precoding matrices to maximize the achievable secrecy sum-rate for two different scenarios of known and unknown eavesdropper's CSI at the transmitter.

3. Bounds on Secrecy Sum-Rate

In this section, we derive lower bounds on the secrecy sum-rate performance of the considered system for two scenarios: known and unknown eavesdropper's CSI $\mathbf{H}_e$ at the transmitter. First, we define the secrecy sum-rate as a summation of the secrecy rates $C_{s,k}$ of all users, i.e.,

$$C_s \triangleq \sum_{i=1}^{K} C_{s,k} = \sum_{i=1}^{K} (C_k - C_{e,k}) = C_u - C_e, \tag{17}$$

where C_k is the rate of the $k-$th user and $C_{e,k}$ is the rate of the eavesdropper for the message d_k eavesdropping on this user. Therefore, $C_u = \sum_{i=1}^{K} C_k$ is the sum rate of legitimate users and $C_e = \sum_{i=1}^{K} C_{e,k}$ is the sum rate of eavesdropper for the messages eavesdropping on all users.

For the rates of legitimate users, let us define $r_k = \gamma\eta\mathbf{H}_k\mathbf{W}_k d_k$, then Eq. (11) is rewritten as

$$y_k = r_k + n_k, \tag{18}$$

where r_k is constrained within $[-\gamma\eta\mathbf{H}_k\mathbf{W}_k, \gamma\eta\mathbf{H}_k\mathbf{W}_k]$. It is seen that the channel in (18) is an amplitude-constrained scalar Gaussian. As shown in [23], the exact capacity of such channel can only be obtained numerically. In this work, instead of finding an exact solution for the sum secrecy-rate problem, we utilize a closed-form lower bound as a benchmark for further analysis. Using the Entropy Power Inequality (EPI) [29, 30], a lower bound for the data rate of the $k-$th user can be given by

$$\begin{aligned} C_k &= \mathbb{I}(r_k; y_k) = h(y_k) - h(y_k|r_k) \\ &= h(r_k + n_k) - h(n_k) \\ &\overset{\text{(EPI)}}{\geq} \frac{1}{2}\log\left(e^{2h(r_k)} + e^{2h(n_k)}\right) - h(n_k) \\ &= \frac{1}{2}\log\left(1 + \frac{e^{2h(r_k)}}{2\pi e\sigma_k^2}\right). \end{aligned} \tag{19}$$

To make this bound as tight as possible, the distribution of r_k is chosen in such a way that maximizes the differential entropy $h(r_k)$ under the amplitude constraint. It is well-known that the uniform distribution is the maximum entropy probability distribution for a random variable under no constraint other than it is contained in the distribution's support [31]. Therefore, assuming that r_k is uniformly distributed over $[-\gamma\eta\mathbf{H}_k\mathbf{W}_k, \gamma\eta\mathbf{H}_k\mathbf{W}_k]$, we obtain

$$C_k \geq \frac{1}{2}\log\left(1 + \frac{2(\gamma\eta)^2\mathbf{H}_k\mathbf{W}_k\mathbf{W}_k^T\mathbf{H}_k^T}{\pi e\sigma_k^2}\right). \tag{20}$$

The above lower bound, however, is not convenient for further analyses. To make a more tractable expression, we omit the quantity 1 inside the logarithm,

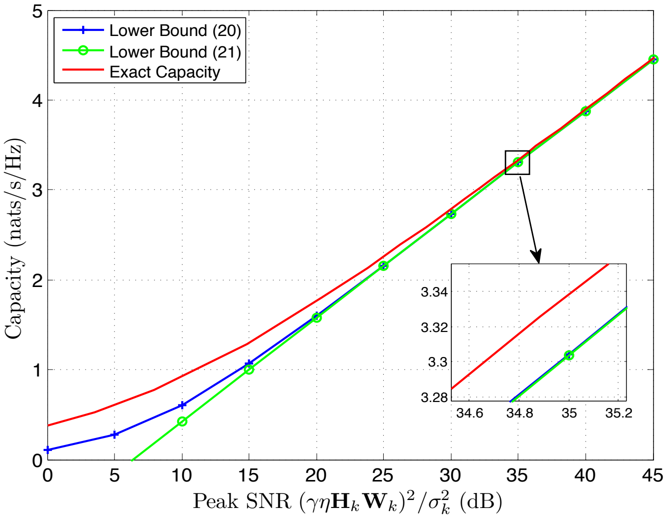

Fig. 3: Exact and lower bounds capacity of amplitude-constrained scalar Gaussian channels.

yields

$$C_k > \frac{1}{2}\log\left(\frac{2(\gamma\eta)^2\mathbf{H}_k\mathbf{W}_k\mathbf{W}_k^T\mathbf{H}_k^T}{\pi e\sigma_k^2}\right)$$
$$= \log\left(2\gamma\eta\mathbf{H}_k\mathbf{W}_k\right) - \log\left(\sqrt{2\pi e\sigma_k^2}\right). \tag{21}$$

We illustrate in Fig. 3 the tightness of the lower bound in (21) in comparisons with the bound in (20) and the exact capacity for amplitude-constrained Gaussian channels. We observed that at high peak SNR region (i.e., > 25 dB), the use of the bound in (21) is valid in characterizing the capacity of the channel since there is a negligible gap between the bound and the exact capacity.

3.1. $\mathbf{H}_e$ *Perfectly Known to the Transmitter*

It is generally unrealistic to assume that eavesdropper's CSI is known to the transmitter since the eavesdropper is usually a malicious user who does not register on the network. However, the assumption of known eavesdropper's CSI still needs to be taken into account as it provides an upper bound on the secrecy performance compared with more reasonable scenarios. If $\mathbf{H}_e$ is perfectly known to the transmitter, the ZF precoding can be applied to eliminate eavesdropper's reception. As a result, the communication between transmitter and legitimate users can be ensured to be completely secured. When the eavesdropper's reception is forced to zero (i.e., $C_e = 0$), any achievable rate of legitimate users is the secrecy rate of the system. In other words, the secrecy sum-rate in this case is the achievable sum-rate of all users.

Using the bound in (21), the maximum secrecy sum-rate problem is given by

$$\begin{aligned} \underset{\mathbf{W_k}}{\text{maximize}} \quad & \sum_{i=1}^{K} \log\left(2\gamma\eta\mathbf{H}_k\mathbf{W}_k\right) - \log\left(\sqrt{2\pi e\sigma_k^2}\right) \\ \text{subject to} \quad & \mathbf{H}_i\mathbf{W}_k = 0 \ \ \forall\, k \neq i, \\ & \mathbf{H}_e\mathbf{W}_k = 0 \ \ \forall\, k, \\ & \sum_{k=1}^{K} \left\|[\mathbf{W}_k]_{i,:}\right\|_1 \leq \Delta_k \ \ \forall\, i = 1, 2, ..., N_T. \end{aligned} \tag{22}$$

It can be seen that the above problem is a standard determinant maximization (MAXDET) program subject to linear matrix inequalities [32]. This problem is convex and thus can be solved efficiently using standard optimization packages [33], [34].

3.2. $\mathbf{H_e}$ *Unknown to the Transmitter*

In practical scenarios when $\mathbf{H}_e$ is completely unknown to the transmitter (e.g., passive eavesdropper), it is generally impossible to suppress eavesdropper's reception. Therefore, the ZF technique is utilized for legitimate users only to guarantee confidential message transmission and to increase the achievable sum-rate, thus enhance the secrecy sum-rate as well. The secrecy sum-rate is then derived from the difference between C_u and C_e as in Eq. (17)

Theorem 1: A lower bound on the secrecy sum-rate in this scenario is $\max(C_s, 0)$ where C_s is given by

$$C_s = C_u - C_e, \tag{23}$$

where C_u is the achievable sum-rate of legitimate users under ZF constraint, which is the solution to

$$\begin{aligned} \underset{\mathbf{W_k}}{\text{maximize}} \quad & \sum_{i=1}^{K} \log\left(2\gamma\eta\mathbf{H}_k\mathbf{W}_k\right) - \log\left(\sqrt{2\pi e\sigma_k^2}\right) \\ \text{subject to} \quad & \mathbf{H}_i\mathbf{W}_k = 0 \ \ \forall\, k \neq i, \\ & \sum_{k=1}^{K} \left\|[\mathbf{W}_k]_{i,:}\right\|_1 \leq \Delta_k \ \ \forall\, i = 1, 2, ..., N_T, \end{aligned} \tag{24}$$

and C_e is the maximum rate of the eavesdropper for the messages eavesdropping on legitimate users, which is given in Appendix A.

Proof: Refer to Appendix A.

Similar to the previous scenario, the optimization problem in (24) is a MAXDET program subject to linear matrix inequalities. Thus, optimization packages can be used to solve the problem.

Table 1: System Parameters

Parameter	**Value**
Room and LED configurations	
Room Dimension (Length × Width × Height)	5 (m) × 5 (m) × 3 (m)
Number of LED arrays, N_T	4
LED array size	0.1 (m) × 0.1 (m)
Number of LED chips per array	36
LED array positions	array 1: $[1.5, 1.5, 3]$ array 2: $[1.5, 3.5, 3]$ array 3: $[3.5, 1.5, 3]$ array 4: $[3.5, 3.5, 3]$
LED bandwidth, B	20 MHz
LED beam angle, ϕ (LED Lambertian order is 1)	120°
LED conversion factor, η	0.44 W/A
Users and eavesdropper photodiodes	
PD active area, D	1cm^2
PD responsivity, γ	0.53 A/W
PD field of view (FOV) semi-angle, Ψ_c	60°
Optical filter gain, $T_s(\psi)$	1
Refractive index of concentrator, κ	1.5
Other parameters	
Ambient light photocurrent, χ_{amb}	$10.93\ \text{A}/(\text{m}^2 \cdot \text{Sr})$
Pre-amplifier noise current density, i_{amb}	$5\ \text{pA}/\text{Hz}^{-1/2}$

4. Numerical Results and Discussions

In this section, representative numerical results are provided to demonstrate the secrecy sum-rate performance derived in Section 3. Fig. 4 shows the geometrical configuration of our considered MU-MISO VLC system with two legitimate users and one eavesdropper. We assume that users and eavesdropper are placed on the same receive plane, which is 0.5 m above the floor. Furthermore, a Cartesian coordinate system is set up for position specifications of LED arrays, legitimate users and the eavesdropper. For the sake of conciseness, all numerical

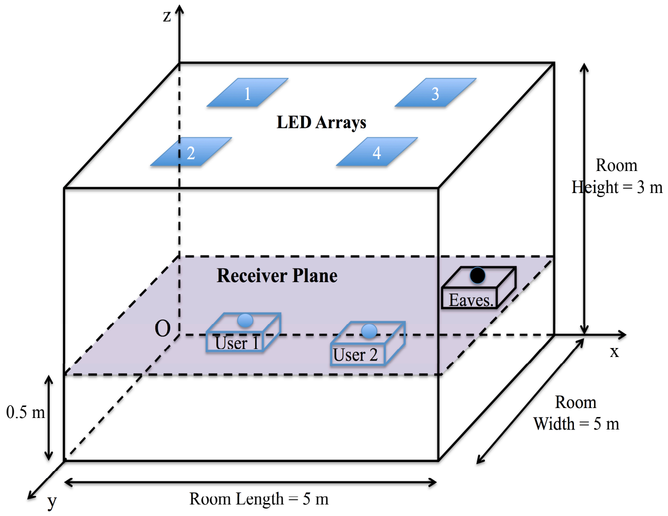

Fig. 4: Geometrical configuration of MU-MISO VLC wiretap channel.

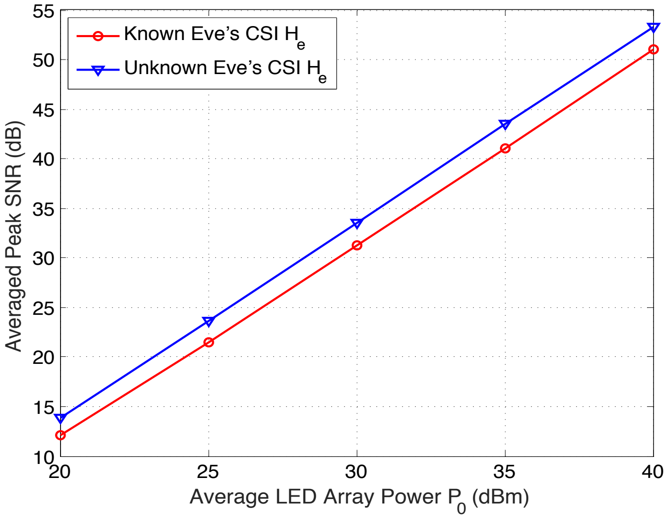

Fig. 5: Averaged peak SNR of legitimate users: known and unknown $\mathbf{H}_e$.

results are obtained for the case of 2 legitimate users. Unless otherwise noted, parameters of the room, the transmitter, legitimate users and the eavesdropper are given in Table 1.

First, Fig. 5 illustrates the average peak SNRs of legitimate users versus the average radiated power P_0 of LED arrays for both cases: known and unknown $\mathbf{H}_e$. The average radiated power ranges from 20 to 40 dBm, which corresponding

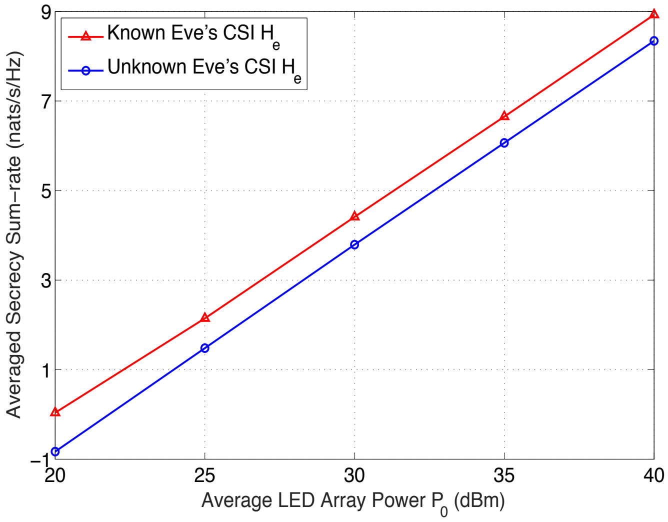

Fig. 6: Averaged secrecy sum-rate: known and unknown $\mathbf{H}_e$.

to 0.1 to 10 W. As will be shown later, the overall performance of the system depends on positions of the users and the eavesdropper. In this figure, we therefore average the results from $10,000$ different channel realizations, i.e., $10,000$ different positions of the users and the eavesdropper to evaluate the average performance. It is clearly shown that the average peak SNRs of higher than 25 dB can usually be achieved in both cases in practical VLC systems (i.e., when the transmit power of LED arrays is higher than 30 dBm corresponding to 1 W). This validates the use of the bound in (21) in evaluating the secrecy capacity performance. In the case of known $\mathbf{H}_e$, due to the additional ZF constraint for canceling eavesdropper's reception, i.e., the second constraint of problem (22), the degrees of freedom in designing the precoding matrix is lower than that in the case of unknown $\mathbf{H}_e$, i.e., the feasible space for searching the optimal $\mathbf{W}_k$ is smaller. As a result, the average user peak SNR in the scenario of unknown eavesdropper's CSI is better than that of the known one.

In Fig. 6, we show the average secrecy sum-rate performance versus the average radiated power P_0 by averaging $10,000$ different channel realizations as in the previous figure. Though the sum-rate of legitimate users C_u, in the case of unknown $\mathbf{H}_e$ is better (since the average peak SNR is better as shown in the previous figure), users must sacrifice a fraction of their communication rate C_e, which is considerable, to achieve perfectly secrecy. As a consequence, with the knowledge of $\mathbf{H}_e$ at the transmitter, zero-forcing eavesdropper's reception can improve the average secrecy sum-rate by around 0.6 *nats* in comparison with the case of unknown $\mathbf{H}_e$. In addition, it is found that positive secrecy sum-rate can be achieved in both scenarios for practical transmit power of LED arrays

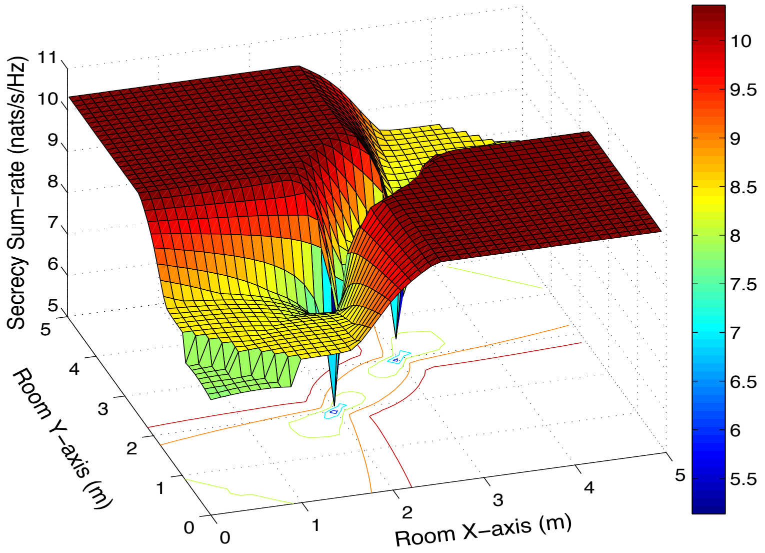

Fig. 7: Secrecy sum-rate for different positions of the eavesdropper: known $\mathbf{H}_e$.

(typically, $4-5$ W corresponding to around 35 dBm) . That demonstrates the benefit of using precoding technique in improving the secrecy performance in MU-MISO VLC systems.

Next, the distribution of the secrecy sum-rate with respect to eavesdropper's position when $\mathbf{H}_e$ is known to the transmitter is depicted in Fig. 7. It is assumed that User 1 and User 2 are placed at $[2, 2, 2.5]$ and $[3, 3, 2.5]$, respectively. The average LED array transmit power P_0 is set to 40 dBm. As clearly illustrated in the figure, we observed a significant variation on the secrecy sum-rate performance according to the location of the eavesdropper. In general, the secrecy performance when the eavesdropper locates in the area around the line connecting the two users is relatively poor. Especially, it drops severely in the area nearby one of the two users due to the lowest degrees of freedom in designing the precoding matrix, i.e., the CSI of the eavesdropper becomes more similar with those of legitimate users .

Finally, in Fig. 8, we investigate the secrecy sum-rate distribution in the case of unknown $\mathbf{H}_e$ at the transmitter. User's positions and LED power setup are the same as those in Fig. 7. Similar to the previous case, the secrecy sum-rate performance changes considerably in accordance to eavesdropper's position. However, because of the unawareness of the eavesdropper's channel, there is a large area of the receive plane where the system suffers poor performance compared with the case of known $\mathbf{H}_e$.

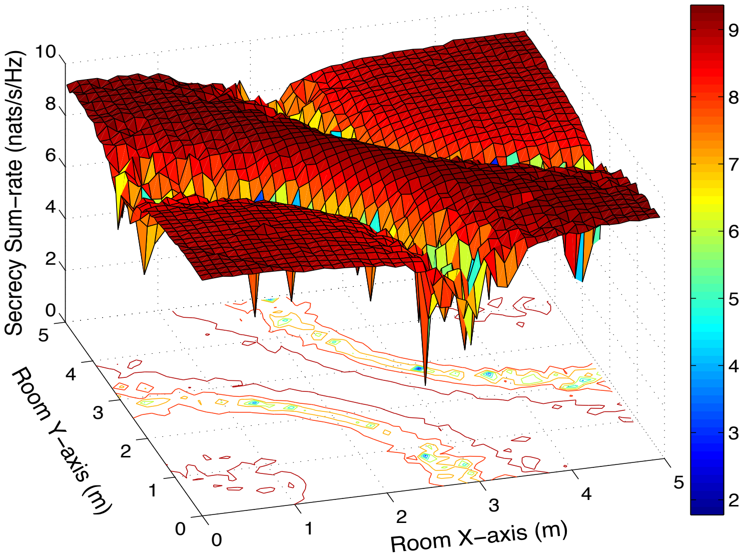

Fig. 8: Secrecy sum-rate for different positions of the eavesdropper: unknown $\mathbf{H}_e$.

5. Conclusions

This paper has analyzed the secrecy sum-rate of MU-MISO VLC broadcast systems with confidential messages. To ensure the confidentiality among users and to improve the secrecy performance, ZF precoding technique is adopted. The secrecy sum-rate was derived for two different scenarios: known and unknown eavesdropper's CSI at the transmitter. Numerical results have shown that performance in the known eavesdropper's CSI case is slightly better and positive secrecy performance can always be achieved for both scenarios. Additionally, it is seen that eavesdropper's position has a significant impact on the secrecy performance.

Appendices

A. Proof of Theorem 1

A.1. Differential Entropy of the Sum of Uniform Random Variables

Let $\{X_i\}_{i=1}^N$ be N independent uniform random variables and assume that the support of X_i is $[-A_i, A_i]$ for some $A_i > 0$. If we define a random variable

$Y = \sum_{i=1}^{N} X_i$, then the probability density function (PDF) of Y is given by [35]

$$f_Y^{(N)}(y) = U_n \left[\sum_{\overrightarrow{\epsilon} \in \{-1,1\}^N} \left(y + \sum_{i=1}^{N} \epsilon_i A_i \right)^{N-1} \times \text{sign} \left(y + \sum_{i=1}^{N} \epsilon_i A_i \right) \prod_{i=1}^{N} \epsilon_i \right], \tag{25}$$

where $U_n = \frac{1}{(N-1)!2^{N+1} \prod_{i=1}^{N} A_i}$. The summation is over all 2^N vectors of signs

$$\overrightarrow{\epsilon} = (\epsilon_1, \epsilon_2, ..., \epsilon_N) \in \{-1, 1\}^N \text{ where } \epsilon_i = \pm 1$$

and

$$\text{sign}(x) \triangleq \begin{cases} 1 & \text{if } x > 0, \\ 0 & \text{if } x = 0, \\ -1 & \text{if } x < 0. \end{cases}$$

Hence, the differential entropy of Y is written as

$$h(Y) = -\int f_Y^{(N)}(y) \log f_Y^{(N)}(y) \mathrm{d}y. \tag{26}$$

It is generally difficult to obtain a closed-form expression for $h(Y)$ due to the complexity of the PDF function in Eq. (25). However, for the simplest case when $N = 2$, $f_Y^{(N)}(y)$ can be expressed as

$$f_Y^{(N)}(y) = \begin{cases} \frac{y+A_1+A_2}{4A_1A_2} & -A1 - A2 \leq y \leq -|A_1 - A_2|, \\ \min\left(\frac{1}{2A_1}, \frac{1}{2A_2}\right) & -|A_1 - A_2| \leq y \leq |A_1 - A_2|, \\ \frac{-y+A_1+A_2}{4A_1A_2} & |A_1 - A_2| \leq y \leq A_1 + A_2, \\ 0 & \text{otherwise.} \end{cases}$$

The differential entropy $h(Y)$ is then given in closed-form as follows

$$h(Y) = \min\left(\log(2A_1) + \frac{A_2}{2A_1}, \log(2A_2) + \frac{A_1}{2A_2} \right). \tag{27}$$

A.2. Data Processing Inequality [31, Theorem 2.8.1]

Random variables X, Y, Z are said to form a Markov chain in that order (denoted by $X \to Y \to Z$) if the conditional distribution of Z depends only on Y and is conditionally independent of X, i.e.,

$$p(x, y, z) = p(x)p(y|x)p(z|y) \tag{28}$$

The *Data Processing Inequality* states that: if $X \to Y \to Z$, then $\mathbb{I}(X; Y) \geq \mathbb{I}(X; Z)$

A.3. Derivation of Eq. (23)

Let us define $r_{e,i} = \gamma\eta\mathbf{H}_e\mathbf{W}_i d_i$ where $\mathbf{W}_i$ is the solution to problem (24) and $r_e = \sum_{i=1}^{K} r_{e,i}$, respectively. Denoting that $A_i = \gamma\eta\mathbf{H}_e\mathbf{W}_i$, then $r_{e,i}$ is uniformly distributed over the interval $[-A_i, A_i]$. Hence, the sum rate for messages eavesdropping on legitimate users of the eavesdropper can be expressed by

$$C_e = \sum_{i=1}^{K} C_{e,i} = \sum_{i=1}^{K} \mathbb{I}(r_{e,1}; y_e). \tag{29}$$

By the definition, it is easy to prove that $r_{e,i} \to r_e \to y_e$. Following the *Data Processing Inequality*, we thus obtain

$$\begin{aligned} C_e &\leq \sum_{i=1}^{K} \mathbb{I}(r_{e,1}; r_e) = \sum_{i=1}^{K} \left(h(r_e) - h(r_{e,i}|r_e)\right) \\ &= K \times h(r_e) - \sum_{i=1}^{K} h(\overline{r_{e,i}}), \end{aligned} \tag{30}$$

where $\overline{r_{e,i}} = \sum_{j=1,j\neq i}^{K} r_{e,j}$ is the sum of $K-1$ independent uniform random variables. Therefore, using the results in Eqs. (25) and (26), C_e can be derived leading to a completion of the proof. Specifically for the case $K = 2$, C_e is given by

$$\begin{aligned} C_e &\leq 2\min\left(\log(2A_1) + \frac{A_2}{2A_1}, \log(2A_2) + \frac{A_1}{2A_2}\right) - \log(2A_1) - \log(2A_2) \\ &= \min\left(\log\left(\frac{A_1}{A_2}\right) + \frac{A_2}{A_1}, \log\left(\frac{A_2}{A_1}\right) + \frac{A_1}{A_2}\right). \end{aligned} \tag{31}$$

Acknowledgement

Portions of this work were presented at the conference CSNDSP 2016, paper *"On the secrecy sum-rate of MU-VLC broadcast systems with confidential messages"*.

References

[1] A. Jovicic, L. Junyi, T. Richardson, "Visible light communication: opportunities, challenges and the path to market," *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 26–32, Dec. 2013.

[2] A. C. Boucouvalas, P. Chatzimisios, Z. Ghassemlooy, M. Uysal, K. Yiannopoulos, "Standards for indoor Optical Wireless Communications," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 24–31, Mar. 2015.

[3] L. Zeng et al, “High data rate multiple input multiple output (MIMO) optical wireless communications using white LED lighting,” *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1654–1662, Dec. 2009.

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

[5] L. Wu, Z. Zhang, H. Liu, “MIMO-OFDM visible light communications system with low complexity”, in *Proc. IEEE International Conference Communications (ICC)*, pp. 3933 - 3937, 2013.

[6] A. H. Azhar et al, “A gigabit/s indoor wireless transmission using MIMO-OFDM visible-light communications”, *IEEE Photon. Technol. Lett.*, vol. 52, no. 2, pp. 171–174, 2013.

[7] Z. Yu, R. Baxley, G.T, Zhou, “Multi-user MISO broadcasting for indoor visible light communication”, *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 4849–4853, 2013.

[8] T. V. Pham, A . T .Pham, “Max-Min Fairness and Sum-Rate Maximization of MU-VLC Local Networks”, in *Proc. IEEE Global Communications Conference (GLOBECOM) Workshop - Optical Wireless Communications*, 2015.

[9] T. Cogalan, H. Haas, E. Panayirci, “Precoded single-cell multi-user MISO visible light communications”, in *Proc. European Wireless Conference*, pp. 1–6, 2015.

[10] H. Ma, L. Lampe, S. Hranilovic, “Coordinated broadcasting for multiuser indoor visible light communication systems,” *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3313–3324, Sept. 2015.

[11] B. Li, J. Wang, R. Zhang, H. Shen, C. Zhao, L. Hanzo, “Multiuser MISO transceiver design for indoor downlink visible light communication under per-LED optical power constraints,” *IEEE Photon. J.*, vol. 7, no. 4, Aug. 2015, Art. ID 7201415.

[12] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[13] S. Leung-Yan-Cheong, M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Info. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[14] A. Mostafa, L. Lampe, “Physical-layer security for MISO visible light communication channels,” *IEEE J. Sel. Areas Commun.*, no. 9, vol. 33, pp. 1806–1818, 2015.

[15] ———, “Optimal and Robust Beamforming for Secure Transmission in MISO Visible-Light Communication Links,” *IEEE Trans. Signal Process.*, vol. 64, no. 24, pp. 6501–6516, 2016.

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

[17] ———, “Physical-layer security for indoor visible light communications,” in *Proc. IEEE International Conference Communications (ICC)*, pp. 3342–3347, 2014.

[18] ———, “Securing visible light communications via friendly jamming,” in *Proc. IEEE Global Communications Conference (GLOBECOM) Workshop- Optical Wireless Communications*, pp. 524–529, 2014.

[19] H. Zaid, Z. Rezki, A. Chaaban, M. S. Alouini, “Improved achievable secrecy rate of visible light communication with cooperative jamming,” in *Proc. Symposium on Signal Processing for Optical Wireless Communications,* pp. 1165–1169, 2015.

[20] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, M. S. Alouini, “On the secrecy capacity of MISO visible light communication channels,” in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2017.

[21] A. Mostafa, L. Lampe, “Pattern synthesis of massive LED arrays for secure visible light communication links,” in *Proc. IEEE International Conference Communications (ICC) Workshop - Visible Light Communications and Networking*, pp. 1350–1355, 2015.

[22] G. Caire, S. Shamai (Shitz), “On the achievable throughput of a multiantenna Gaussian broadcast channel,” *IEEE Trans. Info. Theory*, vol. 49, no. 7, pp. 1691–1706, 2003.

[23] J. G. Smith, “The information capacity of amplitude and variance-constrained scalar Gaussian channels,” *J. Inf. Control*, vol. 18, no. 3, pp. 203–219, 1971.

[24] T. Komine, M. Nakagawa, “Fundamental analysis for visible-light communication system using LED lights,” *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 100–107, 2004.

[25] A. Wiesel, Y. C. Eldar, S. Shamai, ”Zero-Forcing Precoding and Generalized Inverses”, *IEEE Trans. on Signal Process.*, vol. 56, no. 9, pp. 4409–4418, 2008.

[26] Q. H. Spencer, A. L. Swindlehurst, M. Haardt, ”Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels”, *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, 2004.

[27] C. B. Peel, B. M. Hochwald, A. L. Swindlehurst, ”A vector-perturbation technique for near-capacity multiantenna multiuser communication-part I: channel inversion and regularization”, *IEEE Trans. on Commun.*, vol. 53, no. 1, pp. 195–202, 2005.

[28] V. Stankovic, M. Haardt, "Generalized Design of Multi-User MIMO Precoding Matrices", *IEEE Trans. Wireless Commun.*, vol. 7, no. 3, pp. 953–961, 2008.

[29] C. E. Shannon, “A mathematical theory of communication,” *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.

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

[31] T. Cover, J. Thomas, “Elements of Information Theory,” *Wiley Interscience*, 2006.

[32] L. Vandenberghe, S. Boyd, S-P. Wu, “Determinant maximization with linear matrix inequality constraints,” *SIAM J. Matrix Anal. Appl.*, vol. 19, no. 2, pp. 499–533, 1998.

[33] M. Grant, S. Boyd, “CVX: Matlab software for disciplined convex programming version 2.1,” *http://cvxr.com/cvx/*, Jan. 2015.

[34] J. Lofberg, “YALMIP: a toolbox for modeling and optimization in MATLAB,” in *Proc. IEEE International Symposium on Computer Aided Control Systems Design*, pp. 284–289, 2004.

[35] D. M. Bradley, R. C. Gupta, “On the distribution of the sum of n nonidentically distributed uniform random variables,” *Ann. Inst. Stat. Math*, vol. 54, no. 3, pp. 689–700, 2002.