Physical-Layer Security for MISO Visible Light Communication Channels

Ayman Mostafa, *Student Member, IEEE,* and Lutz Lampe, *Senior Member, IEEE*

***Abstract*—This paper considers improving the confidentiality of visible light communication (VLC) links within the framework of physical-layer security. We study a VLC scenario with one transmitter, one legitimate receiver, and one eavesdropper. The transmitter has multiple light sources, while the legitimate and unauthorized receivers have a single photodetector, each. We characterize secrecy rates achievable via transmit beamforming over the multiple-input, single-output (MISO) VLC wiretap channel. For VLC systems, intensity modulation (IM) via light-emitting diodes (LEDs) is the most practical transmission scheme. Because of the limited dynamic range of typical LEDs, the modulating signal must satisfy certain amplitude constraints. Hence, we begin with deriving lower and upper bounds on the secrecy capacity of the scalar Gaussian wiretap channel subject to amplitude constraints. Then, we utilize beamforming to obtain a closed-form secrecy rate expression for the MISO wiretap channel. Finally, we propose a robust beamforming scheme to consider the scenario wherein information about the eavesdropper's channel is imperfect due to location uncertainty. A typical application of the proposed scheme is to secure the communication link when the eavesdropper is expected to exist within a specified area. The performance is measured in terms of the worst-case secrecy rate guaranteed under all admissible realizations of the eavesdropper's channel.**

***Index Terms*—Visible light communication, intensity modulation, amplitude constraint, physical-layer security, secrecy capacity bounds, MISO wiretap VLC channel, robust beamforming, worst-case secrecy rate.**

I. Introduction

VISIBLE light communication (VLC) is an enabling technology that exploits the lighting infrastructure for short-range wireless communication links. The IEEE 802.15.7 standard, released in 2011 [1], was a major step towards the commercialization and widespread deployment of VLC networks. VLC links benefit from the license-free light spectrum, immunity to radio frequency (RF) interference, and the use of inexpensive light-emitting diodes (LEDs) and photodiodes (PDs) for up- and down-conversion, respectively. In addition, VLC systems can be piggybacked on the existing lighting infrastructure where legacy incandescent light bulbs and fluorescent lamps are being replaced by LED-based luminaires with increased lifetime, reduced energy consumption, higher luminous efficacy, and pleasant user experience [2]. Moreover, due to line-of-sight (LoS) propagation and confinement of light waves by opaque surfaces, VLC links cause limited or no inter-network interference. Such advantages qualify VLC links for realizing small-size cells, often referred to as "atto-cells", in fifth generation (5G) networks with coverage ranges on the order of a few meters.

With the unprecedented increase in traffic volumes over wireless networks, data privacy and confidentiality are becoming a major concern for users as well as network administrators. Typical security mechanisms are implemented at upper layers of the network stack via access control, password protection, and end-to-end encryption. Such schemes are deemed to be secure as long as the storage capacity and computational power of potential eavesdroppers remain within certain limits. During the past few years, however, physical-layer security has emerged as a promising research area to complement conventional encryption techniques and provide a first line of defense against eavesdropping attacks. Physical-layer security refers to the techniques which exploit the channel characteristics in order to hide information from unauthorized receivers, without reliance on upper-layer encryption [3]–[9]. The fundamental idea behind physical-layer security is to sacrifice a fraction of the communication rate, that otherwise would be used for data transmission, in order to confuse potential eavesdroppers and diminish their capability to infer information, via carefully-designed signaling and/or coding schemes.

The framework of information-theoretic security was pioneered by Shannon [10] who proposed a cipher system to achieve *perfect secrecy* over noiseless channels intercepted by unauthorized users. Almost two decades later, Wyner [11] considered secure transmission over noisy channels via the *wiretap* channel model. In addition, he proposed a fundamental information-theoretic security measure, termed as the *secrecy capacity*. Wyner proved that the secrecy capacity is non-zero as long as the eavesdropper's channel is *degraded* with respect to (w.r.t.) the receiver's channel, regardless of the decoding technology or computational power available to the eavesdropper.

Motivated by Wyner's work, information theoreticians considered characterizing the secrecy performance of a variety of channel models. In [12], the secrecy capacity of the scalar, i.e., single-input, single-output (SISO), Gaussian wiretap channel was obtained as the difference between the channel capacities of the source-destination and source-eavesdropper links. A single-letter characterization of the secrecy capacity of the *non-degraded* wiretap channel was obtained by Csiszár and Körner in [13]. However, their expression involves stochastic mapping and maximization over an auxiliary random variable

Manuscript received May 28, 2014; revised November 10, 2014 and March 19, 2015; accepted April 10, 2015. This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). The material in this paper was presented in part at the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, June 2014.

A. Mostafa and L. Lampe are with the Department of Electrical and Computer Engineering, The University of British Colombia, Vancouver, BC, V6T 1Z4, Canada (e-mail: {amostafa,lampe}@ece.ubc.ca).

whose optimum choice is not straightforward. Therefore, it does not provide much help in obtaining analytical expressions for the secrecy capacity of multiple-antenna systems. The secrecy capacity of the multiple-input, multiple-output (MIMO) Gaussian wiretap channel was considered in [14]–[18]. For the special case of multiple-input, single-output (MISO) channels, it was shown in [19] that beamforming is a secrecy capacity-achieving strategy, and zero-forcing is optimum at asymptotically high signal-to-noise ratio (SNR).

Despite LoS propagation and better signal confinement, compared to RF channels, the VLC channel, without optical fibers or any sort of wave-guiding, is still of broadcast nature. That makes VLC links inherently susceptible to eavesdropping by unintended or unauthorized users having access to the physical area illuminated by the data transmitters. Typical scenarios include public areas such as classrooms, meeting rooms, libraries, shopping malls, and aircrafts, to name a few.

Unlike RF channels, conventionally modelled as a Gaussian channel with average power constraint, the most practical communication scheme for VLC systems is intensity modulation (IM) along with direct detection (DD) [20], [21]. Typical LEDs exhibit nonlinear current-light characteristics which can be partially compensated via pre-distorters, right before the LED, to mitigate harmonic distortion [22]. However, the dynamic range of the LED is inherently limited. Therefore, the modulating signal must satisfy certain *amplitude constraints* to avoid clipping distortion. Hence, IM/DD channels are typically modelled with amplitude constraints imposed on the channel input, rather than conventional average power constraints [23], [24].

Compared to the massive body of literature on the average power-constrained Gaussian wiretap channels, literature on the information-theoretic secrecy performance of amplitude-constrained wiretap channels is rather scarce. In his seminal paper [25, Section 26], Shannon referred to the difficulty of obtaining an analytical expression for the capacity of peak-limited channels. Instead, he derived a loose lower bound and an asymptotic upper bound which is valid for high peak SNR. Out of his Ph.D. work [26], [27], Smith came up with the rather surprising result that the capacity-achieving distribution for the amplitude-constrained Gaussian channel is discrete with a finite number of mass points. In [28], Arimoto proposed an iterative numerical algorithm to compute the capacity of arbitrary discrete memoryless channels. Closed-form lower and upper bounds on the capacity of amplitude-constrained Gaussian channels were derived in [24]. In [29], Ozel *et al.* followed the approach devised in [27] and proved that the secrecy capacity-achieving distribution for the amplitude-constrained Gaussian wiretap channel is discrete with finite support. To the best of our knowledge, no work in the literature, other than [29], has considered the secrecy performance of amplitude-constrained Gaussian wiretap channels.

In this paper, we consider enhancing the confidentiality of VLC links via physical-layer security techniques. In particular, we are interested in characterizing the secrecy rates achievable in a typical VLC scenario consisting of one transmitter, one legitimate receiver, and one eavesdropper, as illustrated in Fig. 1. We begin with deriving lower and upper bounds on the secrecy capacity of the amplitude-constrained Gaussian wiretap channel. Then, we leverage beamforming to derive a closed-form lower bound on the secrecy capacity of the MISO channel. We also characterize secrecy rates achievable via zero-forcing beamformers. Finally, we consider a VLC scenario wherein the eavesdropper is expected to exist within a specified physical area. Thus, the eavesdropper's channel information is not perfectly known to the transmitter. The design problem is to devise a *robust* beamforming scheme which improves the worst-case secrecy rate guaranteed under all admissible channel realizations of the eavesdropper's link. Instead of solving a difficult max-min worst-case maximization problem, we propose a suboptimal, but essentially simple, beamforming scheme based on first-order Taylor's approximation of the LEDs emission pattern. Numerical results show the superior performance of the robust scheme in terms of worst-case secrecy rates.

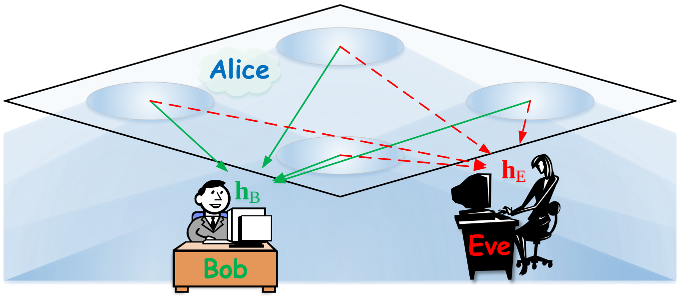

Fig. 1. A VLC network consisting of one sender (Alice), who utilizes the light sources for data transmission, one legitimate receiver (Bob), and one eavesdropper (Eve).

The remainder of the paper is organized as follows. We state the adopted notation in Section II-A, describe the VLC channel model in Section II-B, recall the relevant definitions of beamforming and zero-forcing in Section II-C, and discuss the system model in Section II-D. Lower and upper bounds on the secrecy capacity of the amplitude-constrained Gaussian wiretap channel are provided in Section III-A, while we derive a secrecy rate expression for the MISO case in Section III-B. In Section IV, we formulate the worst-case secrecy rate maximization problem and devise the robust beamforming scheme. Numerical results obtained by simulating a typical VLC scenario are presented in Section V. Finally, we provide concluding remarks in Section VI.

II. Preliminaries

A. Notation

The following notation is adopted throughout the paper. We refer to the transmitter, legitimate receiver, and eavesdropper as "Alice", "Bob", and "Eve", respectively. The set of n-dimensional, real-valued numbers is denoted by $\mathcal{R}^n$, and the set of n-dimensional, non-negative, real-valued numbers is denoted by $\mathcal{R}^n_+$. Bold characters denote column vectors, and vector transposition is denoted by the superscript $\{\cdot\}^{\mathrm{T}}$. The all-ones column vector is denoted by $\mathbb{1}$, and its dimension will be clear from the context. The curled inequality symbol

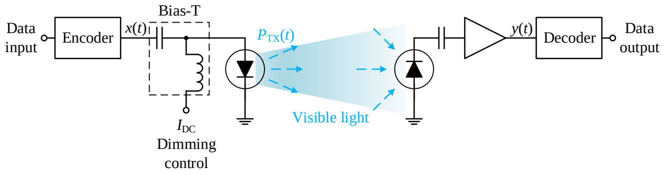

Fig. 2. A simplified block diagram of a PAM VLC system.

$\preceq$ between two vectors denotes componentwise inequality, and $|\cdot|$ denotes componentwise absolute value. Expected value is denoted by $\mathbb{E}\{\cdot\}$, variance by $\mathbb{var}\{\cdot\}$, differential entropy by $\mathbb{h}(\cdot)$, relative entropy by $\mathbb{D}(\cdot\|\cdot)$, and mutual information by $\mathbb{I}(\cdot;\cdot)$. We use $\log(\cdot)$, without a base, to denote natural logarithms, and information rates are specified in (nats/channel use), unless otherwise indicated. We use SNR to denote the *peak*, rather than average, signal-to-noise ratio. A lower-case character x denotes one realization of the random variable X. Subscripts $\{\cdot\}_{\mathrm{B}}$ and $\{\cdot\}_{\mathrm{E}}$ denote Bob's and Eve's relevance, respectively.

B. The VLC Channel Model

We consider a DC-biased pulse-amplitude modulation (PAM) VLC scheme whose simplified block diagram is illustrated in Fig. 2. The transmit element is an illumination LED driven by a fixed bias current $I_{\mathrm{DC}} \in \mathcal{R}_{+}$. The DC bias sets the *average* radiated optical power and, consequently, adjusts the illumination level. The data signal $x(t) \in \mathcal{R}$, $t = 1, 2, 3, \cdots$, is a zero-mean current signal superimposed on I_{DC}, via, e.g., a bias-T circuit, to imperceptibly modulate the *instantaneous* optical power $P_{\mathrm{TX}}(t)$ emitted from the LED. Since $\mathbb{E}\{X(t)\} = 0$, the data signal does not contribute to the average optical power and, therefore, it does not affect the illumination level. In order to maintain linear current-light conversion and avoid clipping distortion, the total current $I_{\mathrm{DC}} + x(t)$ must be constrained within some range $I_{\mathrm{DC}} \pm \alpha I_{\mathrm{DC}}$, where $\alpha \in [0, 1]$ is termed as the *modulation index*. Thus, $x(t)$ must satisfy the amplitude constraint $|x(t)| \leq A \ \forall t$, where $A = \alpha I_{\mathrm{DC}}$.

Then, using an appropriate pre-distorter [22], the electro-optical conversion can be modeled as $P_{\mathrm{TX}}(t) = \eta\left(I_{\mathrm{DC}} + x(t)\right)$ where η (W/A) is the current-to-light conversion efficiency of the LED. The optical power collected by the receiver is given by $P_{\mathrm{RX}}(t) = G P_{\mathrm{TX}}(t)$ where $G < 1$ is the path gain. A PD of responsivity R (A/W) converts the incident optical power into a proportional current $R P_{\mathrm{RX}}(t)$. Then, the DC bias is removed, and the signal is amplified via a transimpedance amplifier of gain T (V/A) to produce a voltage signal $y(t) \in \mathcal{R}$, which is a scaled, but noisy, version of the transmitted signal $x(t)$. Dominant noise sources are the thermal noise in the receiver electronic circuits, i.e., pre-amplifier noise, and shot noise due to ambient illumination from sunlight and/or other light sources. Both noise processes are well-modelled as signal-independent, zero-mean, additive, white Gaussian noise (AWGN) [23], [30].

Therefore, the VLC channel in Fig. 2 can be modelled as

$$y(t) = hx(t) + w(t), \tag{1}$$

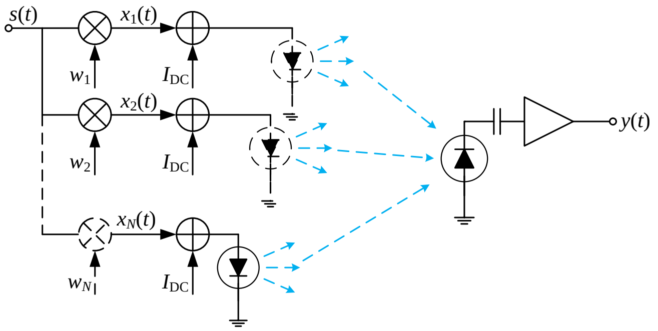

Fig. 3. Transmit beamforming over a MISO PAM VLC channel.

where $h = \eta G R T$, $h \in \mathcal{R}_{+}$, is the channel gain and $W(t) \sim \mathcal{N}\left(0, \sigma^2\right)$ is the noise process.

Notice that the channel model in (1) considers only LoS propagation and ignores reflections from surrounding surfaces. Such a model is valid for most indoor scenarios wherein light fixtures are attached to the ceiling and facing down, making reflections significantly weaker than LoS components [31], [32].

Assuming an LED with a generalized Lambertian emission pattern, the path gain G is given by [33]

$$G = \begin{cases} \frac{1}{2\pi}(m+1)\cos^{m}(\phi)\frac{A_{\mathrm{RX}}}{d^2}\cos\psi & |\psi| \leq \psi_{\mathrm{FoV}} \\ 0 & |\psi| > \psi_{\mathrm{FoV}} \end{cases}, \tag{2}$$

where $m = \frac{-\log 2}{\log\cos\phi_{\frac{1}{2}}}$ is the order of Lambertian emission with half irradiance at semi-angle $\phi_{\frac{1}{2}}$ (measured from the optical axis of the LED), ϕ is the angle of irradiance, A_{RX} is the receiver collection area, d is the LoS distance between the LED and PD, ψ is the angle of incidence (measured from the axis normal to the receiver surface), and ψ_{FoV} is the receiver field-of-view (FoV) semi-angle. The receiver collection area is given by [32]

$$A_{\mathrm{RX}} = \frac{n^2}{\sin^2(\psi_{\mathrm{FoV}})} A_{\mathrm{PD}}, \tag{3}$$

where n is the refractive index of the optical concentrator and A_{PD} is the PD area.

C. Beamforming and Zero-Forcing

Definition 1 (Transmit Beamforming): Consider a transmitter with N transmit elements. Then, for a transmitted signal vector $\mathbf{x}(t) \in \mathcal{R}^N$, we refer to the transmission scheme as *beamforming* if $\mathbf{x}(t)$ can be factorized as $\mathbf{x}(t) = \mathbf{w}s(t)$, where $\mathbf{w} \in \mathcal{R}^N$ is a *fixed vector*, termed as the *beamformer*, while $s(t) \in \mathcal{R}$ is the transmitted data symbol, i.e., S is a random variable.

Definition 2 (Zero-Forcing Beamformer): For a transmit beamforming scheme $\mathbf{x}(t) = \mathbf{w}s(t)$ and a single-element receiver with channel gain vector $\mathbf{h} \in \mathcal{R}^N$, we refer to $\mathbf{w}$ as a *zero-forcing beamformer*, w.r.t. the specified receiver, if $\mathbf{w}$ satisfies $\mathbf{h}^{\mathrm{T}}\mathbf{w} = 0$, i.e., if $\mathbf{w}$ is in the null space of $\mathbf{h}^{\mathrm{T}}$.

Fig. 3 depicts a simplified block diagram of a MISO VLC system utilizing transmit beamforming. Notice that, although the VLC channel described in Section II-B utilizes IM, Definitions 1 and 2 are still applicable since the DC bias at the transmitter ensures the non-negativity of the total current driving the LEDs. Notice also that, for a zero-mean signal $s(t)$, beamforming does not affect the illumination level. It is also crucial to notice that a zero-forcing beamformer ensures only that the data signal at the receiver is suppressed to zero. However, the DC component and, consequently, the illumination level at the receiver (or anywhere else) remain unchanged.

D. System Model

We consider the VLC scenario illustrated in Fig. 1. The room is illuminated by N_{A} down-facing light fixtures attached to the ceiling, and also utilized by Alice for data transmission. Each fixture consists of multiple LEDs modulated by the same current signal, e.g., the LEDs are connected in series. In addition, the LEDs in a single fixture are sufficiently-close such that their channel gains, to a single receiver, are identical. Bob and Eve have a single PD, each, and their terminals are positioned up-facing.

Utilizing the VLC channel model in (1), the signals received by Bob and Eve, respectively, are given by

$$y(t) = \mathbf{h}_{\mathrm{B}}^{\mathrm{T}}\mathbf{x}(t) + w_{\mathrm{B}}(t) \tag{4a}$$

$$z(t) = \mathbf{h}_{\mathrm{E}}^{\mathrm{T}}\mathbf{x}(t) + w_{\mathrm{E}}(t), \tag{4b}$$

where $\mathbf{x}(t) \in \mathcal{R}^{N_{\mathrm{A}}}$ is the transmitted signal vector, $\mathbf{h}_{\mathrm{B}}$ and $\mathbf{h}_{\mathrm{E}} \in \mathcal{R}_{+}^{N_{\mathrm{A}}}$ are fixed channel gain vectors, and $w_{\mathrm{B}}(t)$ and $w_{\mathrm{E}}(t)$ are independent and identically-distributed Gaussian noises whose samples are $\mathcal{N}\left(0, \sigma^2\right)$ random variables. The transmitted signal $\mathbf{x}(t)$ is subject to the amplitude constraint

$$|\mathbf{x}(t)| \preceq A\mathbb{1} \quad \forall t. \tag{5}$$

The fundamental problem addressed in this paper is: Alice shall transmit confidential messages to Bob, and keep the information entirely hidden from Eve, without using secret-key encryption. To formulate the problem properly, we recall relevant definitions from information theory [4], [34].

A $\left(2^{nR}, n\right)$ code for a real-valued Gaussian MISO channel subject to an amplitude constraint $|\mathbf{x}| \preceq A\mathbb{1}$ consists of an index set $\mathcal{M} = \left\{1, 2, \cdots, 2^{nR}\right\}$, a stochastic encoder $\mathcal{E} : \mathcal{M} \to \mathcal{X}^n$ which maps each index $m \in \mathcal{M}$ into a codeword $\mathbf{x}(t)|_{t=1}^{n}$, $\mathbf{x}(t) \in \mathcal{R}^{N_{\mathrm{A}}}$, according to transition probabilities $p_{\mathcal{X}^n|\mathcal{M}}$, and a deterministic decoder $\mathcal{D} : \mathcal{Y}^n \to \mathcal{M}$ which maps the received sequence $y(t)|_{t=1}^{n}$, $y(t) \in \mathcal{R}$, to an estimate $\hat{m} = \mathcal{D}\left(y(t)|_{t=1}^{n}\right)$, $\hat{m} \in \mathcal{M}$. Each codeword $\mathbf{x}(t)|_{t=1}^{n}$ must satisfy the amplitude constraint $|\mathbf{x}(t)| \preceq A\mathbb{1}$ $\forall t$. The rate of information transmission is R (bits/channel use). An error event occurs when $\hat{m} \neq m$, and the communication reliability is measured in terms of the average error probability P_e^n.

By considering the wiretap channel in (4), $\mathbb{I}(M; Y^n)$ measures the amount of information attainable by Bob within n channel uses, while $\mathbb{I}(M; Z^n)$ measures the amount of information leaked to Eve. A communication rate R_s is said to be achievable and fully secure, i.e., R_s is an *achievable secrecy rate*, if there exists a $\left(2^{nR_s}, n\right)$ code such that

$$\lim_{n\to\infty} P_e^n = 0 \tag{6a}$$

$$\lim_{n\to\infty} \mathbb{I}\left(M; Z^n\right) = 0, \tag{6b}$$

where (6a) is the reliability constraint, i.e., reliable connection between Alice and Bob, while (6b) is the *strong secrecy* constraint. The *secrecy capacity* is the supremum of all achievable secrecy rates [4].

Given the wiretap channel in (4), we are interested in characterizing communication rates between Alice and Bob, subject to the amplitude constraint in (5) and reliability and secrecy constraints in (6).

III. Achievable Secrecy Rates

We first derive lower and upper bounds on the secrecy capacity of the scalar Gaussian wiretap channel subject to an amplitude constraint. Then, we utilize the lower bound along with beamforming to characterize achievable secrecy rates for the MISO case.

A. Bounds on the Secrecy Capacity for the SISO Channel

If only a single light fixture is utilized for data transmission, or all the fixtures are modulated by identical current signals, e.g., due to hardware or wiring limitations, the wiretap channel model in (4) simplifies to

$$y(t) = h_{\mathrm{B}}x(t) + w_{\mathrm{B}}(t) \tag{7a}$$

$$z(t) = h_{\mathrm{E}}x(t) + w_{\mathrm{E}}(t). \tag{7b}$$

If $h_{\mathrm{B}} \leq h_{\mathrm{E}}$, then Alice-Bob channel is *stochastically degraded* w.r.t. Alice-Eve channel and the secrecy capacity is essentially zero. Alternatively, if $h_{\mathrm{B}} > h_{\mathrm{E}}$, then the secrecy capacity is given by [4]

$$C_s^{\mathrm{SISO}} = \max_{p_X} \left(\mathbb{I}(X;Y) - \mathbb{I}(X;Z)\right) \tag{8a}$$

$$\text{s.t.}\ |x| \leq A. \tag{8b}$$

Because of the amplitude constraint, obtaining a closed-form solution for (8) is a formidable task, if not unfeasible. However, it was shown in [29] that the maximization problem in (8) is convex. Furthermore, it was shown that the optimum distribution p_X^*, which maximizes $\mathbb{I}(X;Y) - \mathbb{I}(X;Z)$, is discrete with a finite number of mass points. Therefore, (8) can be efficiently solved using numerical methods. Nevertheless, closed-form expressions are often of great interest for system design purposes. In the following, we provide closed-form lower and upper bounds on the secrecy capacity of (8).

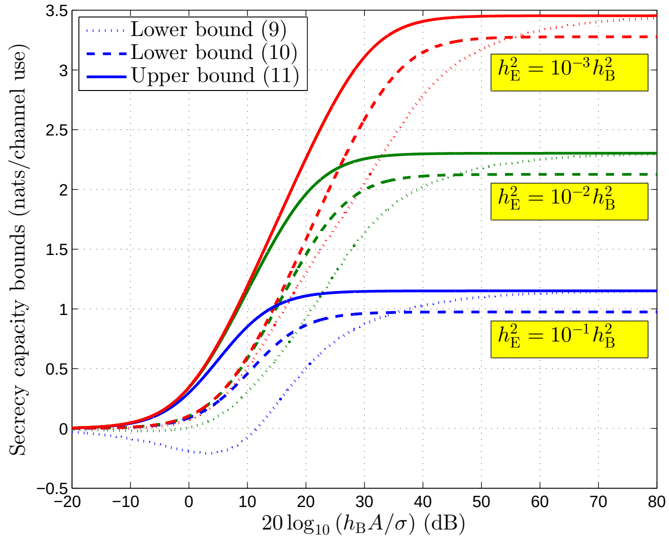

Fig. 4. Secrecy capacity bounds of Theorem 1.

Theorem 1: The secrecy capacity of the Gaussian wiretap channel in (7), subject to the amplitude constraint $|x(t)| \leq A \; \forall t$, is lower-bounded by each of the following two bounds

$$\begin{aligned} C_s^{\text{SISO}} \geq{}& \frac{1}{2}\log\left(1+\frac{2h_{\text{B}}^2A^2}{\pi e\sigma^2}\right) \\ &- \left(1-2\mathcal{Q}\left(\frac{\delta+h_{\text{E}}A}{\sigma}\right)\right)\log\frac{2(h_{\text{E}}A+\delta)}{\sqrt{2\pi\sigma^2}\left(1-2\mathcal{Q}\left(\frac{\delta}{\sigma}\right)\right)} \\ &- \mathcal{Q}\left(\frac{\delta}{\sigma}\right) - \frac{\delta}{\sqrt{2\pi\sigma^2}}e^{-\frac{\delta^2}{2\sigma^2}} + \frac{1}{2} \end{aligned} \tag{9}$$

$$C_s^{\text{SISO}} \geq \frac{1}{2}\log\frac{6h_{\text{B}}^2A^2+3\pi e\sigma^2}{\pi e h_{\text{E}}^2A^2+3\pi e\sigma^2}, \tag{10}$$

and is upper-bounded by

$$C_s^{\text{SISO}} \leq \frac{1}{2}\log\frac{h_{\text{B}}^2A^2+\sigma^2}{h_{\text{E}}^2A^2+\sigma^2}, \tag{11}$$

where δ in (9) is a free parameter such that $\delta > 0$, and $\mathcal{Q}(\cdot)$ is the $\mathcal{Q}$-function.

Proof: See Appendices A and B.

Notice that the lower bound in (9) exploits the lower and upper bounds on the capacity of the IM channel studied in [24]. Notice also that the upper bound in (11) is the secrecy capacity of the Gaussian wiretap channel subject to the average power constraint $\mathbb{E}\{X^2\} \leq A^2$. Therefore, (11) can be concluded by relaxing the amplitude constraint $|x| \leq A$ into the average power constraint $\mathbb{E}\{X^2\} \leq A^2$. Nevertheless, we provide a rigorous proof for (11) in Appendix B and introduce a general approach for upper-bounding the secrecy capacity of degraded wiretap channels.

Fig. 4 presents the bounds of Theorem 1. Three groups of bounds are shown using $20\log_{10}(h_{\text{B}}/h_{\text{E}}) = 10, 20,$ and 30 dB. Lower bound (9) is calculated using $\delta = \sigma\log(1+2h_{\text{E}}A/\sigma)$ as proposed in [24]. As can be seen, both (9) and (10) along with (11) tightly bound the secrecy capacity at asymptotically low and high SNR_{B}. Notice that (10) incurs a fixed gap of $\log\sqrt{\pi e/6} = 0.1765$ nats/channel use at asymptotically high SNR_{B}. Nevertheless, since typical VLC links operate at SNR values well below 40 dB (see, e.g., Fig. 7), (10) is appropriate for VLC scenarios. Furthermore, (10) is more analytically-tractable and, therefore, it will be used to obtain secrecy rate expressions for the MISO channel.

B. Achievable Secrecy Rates for the MISO Case

A single-letter characterization of the secrecy capacity of the non-degraded wiretap channel was given by Csiszár and Körner as [13]

$$C_s^{\text{MISO}} = \max_{p_{\mathbf{UX}}}\left(\mathbb{I}(\mathbf{U};Y) - \mathbb{I}(\mathbf{U};Z)\right), \tag{12}$$

where $\mathbf{U}$ is an auxiliary random vector that satisfies the Markov relation $\mathbf{U} \to \mathbf{X} \to (Y, Z)$. Unlike the scalar case, the optimization problem in (12) is, in general, non-convex. Furthermore, the optimum selection of $\mathbf{U}$ is not clear. For the Gaussian MISO channel with average power constraint, it was shown in [19] that the secrecy capacity is achieved via beamforming, i.e., the choice $\mathbf{U} = \mathbf{X} = \mathbf{w}S$ is optimum, where $\mathbf{w}$ is the beamformer and S is a random variable.

An achievable secrecy rate for the MISO channel with amplitude constraint can be obtained by lower-bounding the secrecy capacity in (12) as follows.

$$\begin{aligned} C_s^{\text{MISO}} &\overset{\text{(a)}}{\geq} \max_{p_{\mathbf{X}}}\left(\mathbb{I}(\mathbf{X};Y) - \mathbb{I}(\mathbf{X};Z)\right) \\ &\overset{\text{(b)}}{\geq} \max_{\mathbf{w},p_S}\left(\mathbb{I}(\mathbf{w}S;Y) - \mathbb{I}(\mathbf{w}S;Z)\right) \\ &\overset{\text{(c)}}{\geq} \max_{\mathbf{w}}\frac{1}{2}\log\frac{6A^2\mathbf{w}^{\text{T}}\mathbf{h}_{\text{B}}\mathbf{h}_{\text{B}}^{\text{T}}\mathbf{w}+3\pi e\sigma^2}{\pi eA^2\mathbf{w}^{\text{T}}\mathbf{h}_{\text{E}}\mathbf{h}_{\text{E}}^{\text{T}}\mathbf{w}+3\pi e\sigma^2}, \end{aligned} \tag{13}$$

where (a) follows from setting $\mathbf{X} = \mathbf{U}$, (b) from choosing $\mathbf{X} = \mathbf{w}S$ such that $|\mathbf{w}| \preceq \mathbb{1}$ and $|s| \leq A$, i.e., restricting the transmission scheme to beamforming, and (c) from choosing a uniform distribution p_S over the interval $[-A, A]$ and utilizing the lower bound in (10).

Although suboptimal, beamforming is preferable as it is a linear operation with low implementation complexity. Furthermore, it reduces the vector channel into a scalar version which enables the use of well-developed scalar channel codes. The lower bound in (13) provides a design equation for the MISO case where the problem is reduced to finding an appropriate beamformer $\mathbf{w}$.

1) Optimum Beamforming: The optimum beamformer $\mathbf{w}^*$ which maximizes the secrecy rate in (13) is given by

$$\mathbf{w}^* = \arg\max_{\mathbf{w}}\frac{1}{2}\log\frac{6A^2\mathbf{w}^{\text{T}}\mathbf{h}_{\text{B}}\mathbf{h}_{\text{B}}^{\text{T}}\mathbf{w}+3\pi e\sigma^2}{\pi eA^2\mathbf{w}^{\text{T}}\mathbf{h}_{\text{E}}\mathbf{h}_{\text{E}}^{\text{T}}\mathbf{w}+3\pi e\sigma^2} \tag{14a}$$

$$\text{s.t.}\; |\mathbf{w}| \preceq \mathbb{1}. \tag{14b}$$

Since $\mathbf{h}_{\text{B}}\mathbf{h}_{\text{B}}^{\text{T}}$ and $\mathbf{h}_{\text{E}}\mathbf{h}_{\text{E}}^{\text{T}}$ are positive semi-definite matrices (as both are singular), the problem in (14) is a maximization of the ratio of two convex quadratic functions with box constraints. Such a problem is non-convex, and obtaining a local maximum has been shown to be NP-hard [35]. Nevertheless, several approaches have been proposed, e.g., in [36], [37], to obtain suboptimal solutions. A typical algorithm begins with converting the problem into a parametric, non-convex, quadratic problem, as proposed in [38]. Then, a local maximum is found via active-set or interior methods.

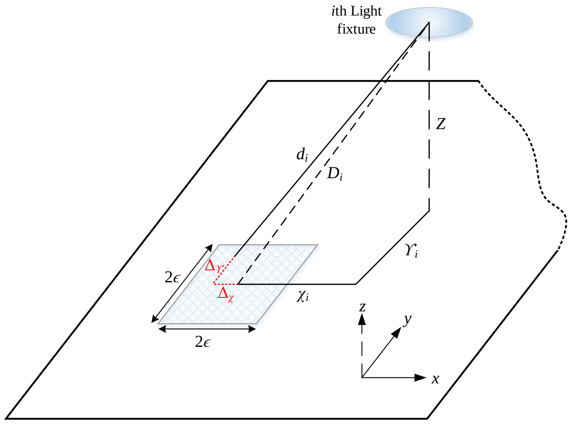

Fig. 5. Geometry for the robust beamforming problem. The highlighted area identifies possible locations for Eve.

2) Zero-Forcing Beamforming: The secrecy rate in (13) can be further lower-bounded by restricting $\mathbf{w}$ to be within Eve's null space. Thus, the optimum zero-forcing beamformer $\mathbf{w}_{\text{ZF}}$ is obtained by

$$\mathbf{w}_{\text{ZF}} = \arg\max_{\mathbf{w}} \mathbf{h}_{\text{B}}^{\text{T}}\mathbf{w} \tag{15a}$$

$$\text{s.t.} \begin{cases} |\mathbf{w}| \preceq \mathbb{1} \\ \mathbf{h}_{\text{E}}^{\text{T}}\mathbf{w} = 0 \end{cases}. \tag{15b}$$

Replacing $\mathbf{w}$ in (13) with $\mathbf{w}_{\text{ZF}}$ results in the secrecy rate

$$R_s^{\text{ZF}} = \frac{1}{2}\log\left(1 + \frac{2A^2\mathbf{w}_{\text{ZF}}^{\text{T}}\mathbf{h}_{\text{B}}\mathbf{h}_{\text{B}}^{\text{T}}\mathbf{w}_{\text{ZF}}}{\pi e \sigma^2}\right). \tag{16}$$

Unlike the optimum beamforming case in (14), the maximization problem in (15) is linear and, therefore, it can be solved with lower computational complexity. Furthermore, the zero-forcing beamformer is sufficient to achieve the secrecy rate in (16) without resorting to stochastic encoding.

IV. Robust Beamforming

For the wiretap channel, it is reasonable to assume that Bob's channel is accurately known to Alice, via, e.g., feedback from Bob. On the other hand, Eve is typically a malicious user, and will not feed back her channel information to Alice. Nevertheless, in a typical VLC scenario, with the path gain as given in (2), Alice can map Eve's *uncertain* location information into an *estimate* of her channel gain. Thus, an interesting design problem is to secure the connection between Alice and Bob when Eve is expected to exist within a specified area, without knowing her exact location. A relevant practical scenario would be, e.g., a governmental office with certain areas accessible to the public, and among them are potential eavesdroppers.

Fig. 5 illustrates the scenario with uncertainty about Eve's location. For simplicity, we consider only two-dimensional location uncertainty, and assume that Eve's height is fixed and is accurately known to Alice. Extension to three-dimensional uncertainty should be straightforward. Without loss of generality, we assume that Eve's location is bounded by a square of area $2\epsilon \times 2\epsilon$, i.e., Eve is located somewhere at $(\chi_{\text{E}} + \Delta_\chi, \Upsilon_{\text{E}} + \Delta_\Upsilon)$, where χ_{E} and Υ_{E} are measured w.r.t. some reference point at Eve's height, e.g., the room center, while $|\Delta_\chi|$ and $|\Delta_\Upsilon|$ are bounded as $|\Delta_\chi| \le \epsilon$ and $|\Delta_\Upsilon| \le \epsilon$. From this location information, Alice can estimate Eve's channel with some bounded error.

If Alice adopts a beamforming strategy and perfectly knows Bob's channel, then the achievable secrecy rate is given by (13) as a function of Eve's exact location, i.e., $R_s(\mathbf{w}, \Delta_\chi, \Delta_\Upsilon)$. For a fixed beamformer $\mathbf{w}$, there exists a worst-case Eve's location $\big(\chi_{\text{E}} + \Delta_\chi^*(\mathbf{w}), \Upsilon_{\text{E}} + \Delta_\Upsilon^*(\mathbf{w})\big)$, $\big|\Delta_\chi^*(\mathbf{w})\big| \le \epsilon$, $\big|\Delta_\Upsilon^*(\mathbf{w})\big| \le \epsilon$, which minimizes the achievable secrecy rate. Such secrecy rate is termed as the *worst-case* secrecy rate $R_s^{\text{wc}}(\mathbf{w})$, and is a function of $\mathbf{w}$. By definition, achieving $R_s^{\text{wc}}(\mathbf{w})$ is guaranteed regardless of Eve's exact location $(\chi_{\text{E}} + \Delta_\chi, \Upsilon_{\text{E}} + \Delta_\Upsilon)$. Then, the design problem is to find the beamformer $\mathbf{w}_{\text{RB}}$ which maximizes the worst-case secrecy rate over all admissible beamformers $|\mathbf{w}| \preceq \mathbb{1}$. Such a transmission strategy will be termed as *robust* beamforming.

To simplify the problem formulation, we rewrite Eve's channel gain as a function of her location. Assume that the ith light fixture is located at $(\chi_{\text{A},i}, \Upsilon_{\text{A},i}, Z)$, where $\chi_{\text{A},i}$ and $\Upsilon_{\text{A},i}$ are measured w.r.t. the reference point, while Z is the vertical distance between the light fixtures and Eve. Then, for $i \in \{1, 2, \cdots, N_{\text{A}}\}$, the channel gain $h_{\text{E},i}$, when $|\psi_i| \le \psi_{\text{FoV}}$, i.e., when the ith light fixture is within Eve's FoV, can be written as

$$\begin{aligned} h_{\text{E},i} &= \frac{\eta}{2\pi}(m+1)\left(\frac{Z}{d_i}\right)^m \frac{A_{\text{RX}}}{d_i^2}\left(\frac{Z}{d_i}\right) RT \\ &= K d_i^{-(m+3)} \\ &= K\left((\chi_i + \Delta_\chi)^2 + (\Upsilon_i + \Delta_\Upsilon)^2 + Z^2\right)^{-\frac{m+3}{2}}, \end{aligned} \tag{17}$$

where $\chi_i = \chi_{\text{E}} - \chi_{\text{A},i}$, $\Upsilon_i = \Upsilon_{\text{E}} - \Upsilon_{\text{A},i}$, and $K = \frac{\eta}{2\pi}(m+1)Z^{m+1}A_{\text{RX}}RT$ is a constant.

Thus, the worst-case secrecy rate maximization problem can be formulated as

$$R_s^{\text{wc}*} = \max_{\mathbf{w}} \min_{\Delta_\chi, \Delta_\Upsilon} \frac{1}{2}\log\frac{6A^2\mathbf{w}^{\text{T}}\mathbf{h}_{\text{B}}\mathbf{h}_{\text{B}}^{\text{T}}\mathbf{w} + 3\pi e\sigma^2}{\pi e A^2\mathbf{w}^{\text{T}}\mathbf{h}_{\text{E}}\mathbf{h}_{\text{E}}^{\text{T}}\mathbf{w} + 3\pi e\sigma^2} \tag{18a}$$

$$\text{s.t.} \begin{cases} |\mathbf{w}| \preceq \mathbb{1} \\ |\Delta_\chi| \le \epsilon \\ |\Delta_\Upsilon| \le \epsilon \end{cases}, \tag{18b}$$

where, for $i \in \{1, 2, \cdots, N_{\text{A}}\}$,

$$h_{\text{E},i} = K\left((\chi_i + \Delta_\chi)^2 + (\Upsilon_i + \Delta_\Upsilon)^2 + Z^2\right)^{-\frac{m+3}{2}}. \tag{18c}$$

The max-min problem in (18) involves two optimization problems. The inner problem is to find the worst-case location for Eve $\big(\Delta_\chi^*(\mathbf{w}), \Delta_\Upsilon^*(\mathbf{w})\big)$ which minimizes R_s for a fixed $\mathbf{w}$. The outer problem is similar to (14) and involves finding the optimal beamformer $\mathbf{w}^*(\Delta_\chi, \Delta_\Upsilon)$ that maximizes R_s for a given location $(\Delta_\chi, \Delta_\Upsilon)$. Solving (18) is difficult mainly due to the mutual dependence between the optimization parameters in the inner and outer problems. In the following, we simplify (18) by considering the first-order Taylor series approximation of the channel gain in (17) at $(\Delta_\chi, \Delta_\Upsilon) = (0, 0)$.

Define $D_i = \sqrt{(\chi_i^2 + \Upsilon_i^2 + Z^2)}$, then, for $i \in \{1, 2, \cdots, N_\mathrm{A}\}$, Taylor's expansion of $h_{\mathrm{E},i}$ at $(\Delta_\chi, \Delta_\Upsilon) = (0, 0)$ is given by

$$\begin{aligned} & h_{\mathrm{E},i}(\Delta_\chi, \Delta_\Upsilon) \\ & = K \Big(D_i^{-(m+3)} \\ & \quad - (m+3)\chi_i D_i^{-(m+5)} \Delta_\chi \\ & \quad - (m+3)\Upsilon_i D_i^{-(m+5)} \Delta_\Upsilon \\ & \quad + \frac{m+3}{2} \left((m+5)\chi_i^2 D_i^{-(m+7)} - D_i^{-(m+5)} \right) \Delta_\chi^2 \\ & \quad + \frac{m+3}{2} \left((m+5)\Upsilon_i^2 D_i^{-(m+7)} - D_i^{-(m+5)} \right) \Delta_\Upsilon^2 \\ & \quad + (m+3)(m+5)\chi_i \Upsilon_i D_i^{-(m+7)} \Delta_\chi \Delta_\Upsilon + \cdots \Big) . \end{aligned} \tag{19}$$

For sufficiently small ϵ, $h_{\mathrm{E},i}$ can be approximated by the first three terms in (19) as

$$\begin{aligned} \tilde{h}_{\mathrm{E},i}(\Delta_\chi, \Delta_\Upsilon) &= K \Big(D_i^{-(m+3)} - (m+3)\chi_i D_i^{-(m+5)} \Delta_\chi \\ &\qquad - (m+3)\Upsilon_i D_i^{-(m+5)} \Delta_\Upsilon \Big) \\ &= K \left(\alpha_i + \beta_i \Delta_\chi + \Gamma_i \Delta_\Upsilon \right), \end{aligned} \tag{20}$$

where $\alpha_i = D_i^{-(m+3)}$, $\beta_i = -(m+3)\chi_i D_i^{-(m+5)}$, and $\Gamma_i = -(m+3)\Upsilon_i D_i^{-(m+5)}$.

We define the matrix $\tilde{\mathbf{H}}_\mathrm{E} \in \mathcal{R}^{N_\mathrm{A} \times 3}$ as

$$\tilde{\mathbf{H}}_\mathrm{E} = \begin{bmatrix} \alpha_1 & \beta_1 & \Gamma_1 \\ \alpha_2 & \beta_2 & \Gamma_2 \\ \vdots & \vdots & \vdots \\ \alpha_{N_\mathrm{A}} & \beta_{N_\mathrm{A}} & \Gamma_{N_\mathrm{A}} \end{bmatrix} . \tag{21}$$

Then, for sufficiently small ϵ, $\mathbf{h}_\mathrm{E}(\Delta_\chi, \Delta_\Upsilon)$ can be approximated by

$$\tilde{\mathbf{h}}_\mathrm{E} = K \tilde{\mathbf{H}}_\mathrm{E} \begin{bmatrix} 1 \\ \Delta_\chi \\ \Delta_\Upsilon \end{bmatrix} . \tag{22}$$

The columns of $\tilde{\mathbf{H}}_\mathrm{E}$ span a three-dimensional vector space $\tilde{\mathcal{H}}_\mathrm{E}$. If Alice has more than three transmit elements, i.e., $N_\mathrm{A} \geq 4$, we propose restricting the transmit beamformer $\mathbf{w}$ into the null space of $\tilde{\mathcal{H}}_\mathrm{E}$. Such a beamformer would significantly degrade the received signal at Eve provided that her actual location is fairly close to $(\chi_\mathrm{E}, \Upsilon_\mathrm{E})$.

The approximation in (22), along with restricting $\mathbf{w}$ within the null space of $\tilde{\mathcal{H}}_\mathrm{E}$, lead to a considerable simplification of (18) and allow decoupling the optimization variables in order to solve two disjoint maximization problems. In particular, the robust beamforming problem can be reformulated as

$$\mathbf{w}_\mathrm{RB} = \arg \max_{\mathbf{w}} \mathbf{h}_\mathrm{B}^\mathrm{T} \mathbf{w} \tag{23a}$$

$$\text{s.t.} \begin{cases} |\mathbf{w}| \preceq \mathbb{1} \\ \tilde{\mathbf{H}}_\mathrm{E}^\mathrm{T} \mathbf{w} = \mathbf{0} \end{cases} , \tag{23b}$$

$$(\Delta_\chi^\mathrm{wc}, \Delta_\Upsilon^\mathrm{wc}) = \arg \max_{\Delta_\chi, \Delta_\Upsilon} \left| \mathbf{w}_\mathrm{RB}^\mathrm{T} \mathbf{h}_\mathrm{E} \right| \tag{24a}$$

$$\text{s.t.} \begin{cases} |\Delta_\chi| \leq \epsilon \\ |\Delta_\Upsilon| \leq \epsilon \end{cases} , \tag{24b}$$

and the resulting worst-case secrecy rate is obtained by

$$R_s^\mathrm{wc} = \frac{1}{2} \log \frac{6A^2 \mathbf{w}_\mathrm{RB}^\mathrm{T} \mathbf{h}_\mathrm{B} \mathbf{h}_\mathrm{B}^\mathrm{T} \mathbf{w}_\mathrm{RB} + 3\pi e \sigma^2}{\pi e A^2 \mathbf{w}_\mathrm{RB}^\mathrm{T} \mathbf{h}_\mathrm{E}^\mathrm{wc} \left(\mathbf{h}_\mathrm{E}^\mathrm{wc}\right)^\mathrm{T} \mathbf{w}_\mathrm{RB} + 3\pi e \sigma^2}, \tag{25}$$

where $\mathbf{h}_\mathrm{E}^\mathrm{wc} \equiv \mathbf{h}_\mathrm{E} \left(\Delta_\chi^\mathrm{wc}, \Delta_\Upsilon^\mathrm{wc} \right)$.

Notice that the maximization in (23), which is the design equation for the robust beamformer, is a linear problem. On the other hand, the maximization in (24), with $\mathbf{h}_\mathrm{E}$ as given in (17), is a non-convex problem, and is used to find Eve's location corresponding to the worst-case secrecy rate. Nevertheless, (24) can be simplified by approximating $\mathbf{h}_\mathrm{E}$ using the second-order terms of Taylor's expansion provided in (19), i.e.,

$$\tilde{\tilde{\mathbf{h}}}_\mathrm{E} = K \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ \vdots & \vdots & \vdots \\ a_{N_\mathrm{A}} & b_{N_\mathrm{A}} & c_{N_\mathrm{A}} \end{bmatrix} \begin{bmatrix} \Delta_\chi^2 \\ \Delta_\Upsilon^2 \\ \Delta_\chi \Delta_\Upsilon \end{bmatrix} , \tag{26}$$

where, for $i \in \{1, 2, \cdots, N_\mathrm{A}\}$,

$$\begin{aligned} a_i &= \frac{m+3}{2} \left((m+5)\chi_i^2 D_i^{-(m+7)} - D_i^{-(m+5)} \right), \\ b_i &= \frac{m+3}{2} \left((m+5)\Upsilon_i^2 D_i^{-(m+7)} - D_i^{-(m+5)} \right), \\ c_i &= (m+3)(m+5)\chi_i \Upsilon_i D_i^{-(m+7)} . \end{aligned}$$

Such an approximation results in a quadratic maximization problem, which is still non-convex, but is easier to solve.

V. Numerical Results

To validate the proposed schemes, we have numerically simulated a typical indoor VLC scenario. The problem geometry is illustrated in Fig. 6, and simulation parameters are provided in Table I. The room dimensions ($5 \times 5 \times 3$ m^3) and the number of light fixtures and their locations are quite similar to those in Room 5505, Fred Kaiser Building, Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver Campus. There exist 16 down-facing light fixtures attached to the ceiling. Each fixture consists of four LEDs, and each LED radiates one Watt optical power. The half-illuminance semi-angle is $60°$, which is a typical value for commercially-available high-brightness LEDs. Notice that LEDs with wide half-illuminance angles, e.g., $60°$, are preferred for general-purpose lighting to provide uniform illumination. The LEDs modulation index is set to 10%. Bob and Eve are located at height 0.85 m above the floor level, e.g., on desks, and their receivers have a $60°$ FoV (semi-angle). We use a Cartesian coordinate system (x, y) at the receivers height to identify their locations. The origin $(0, 0)$ corresponds to the room center, and all distances are measured in meters. Noise power is calculated using [32, eq. (6) and Table I] with a 70 MHz receiver bandwidth, and the result is averaged over the entire room area. The average electrical noise power is -98.82 dBm.

Fig. 7 shows the spatial distribution of the SNR at the receivers height without beamforming, i.e., $\mathbf{w} = \mathbb{1}$. As can be seen, the SNR reaches its maximum value, 39.40 dB, at the room center, and decays to 24.97 dB at the corners.

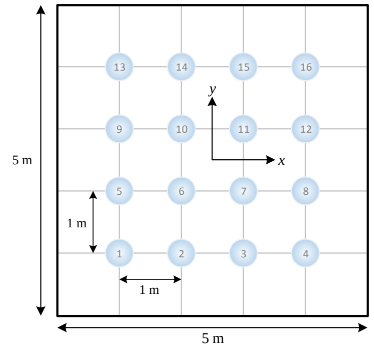

Fig. 6. Geometry of a VLC scenario with 16 light fixtures.

TABLE I
SIMULATION PARAMETERS.

Problem geometry	
Room dimensions $(W \times L \times H)$	$5 \times 5 \times 3$ m^3
Light fixtures (Alice) height	3 m
Receivers (Bob and Eve) height	0.85 m
Number of light fixtures N_A	16
Number of LEDs per fixture	4
Transmitter characteristics	
Average optical power per LED	1 W
Modulation index α	10%
LED half luminous intensity semi-angle $\phi_{\frac{1}{2}}$	60°
Receiver characteristics	
Receiver FoV ψ_FoV	60°
Lens refractive index n	1.5
PD responsivity R	0.54 (A/W
PD geometrical area A_PD	1 cm^2
Average electrical noise power σ^2	-98.82 dE

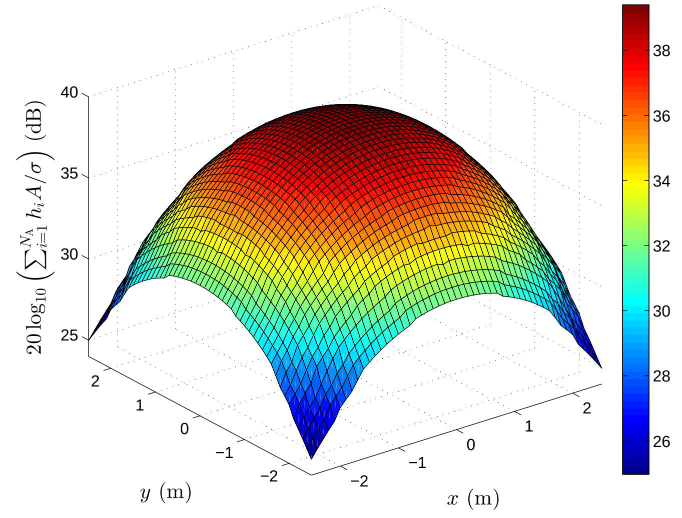

Fig. 7. Spatial distribution of the SNR at the receivers level (0.85 m above the floor level) without beamforming.

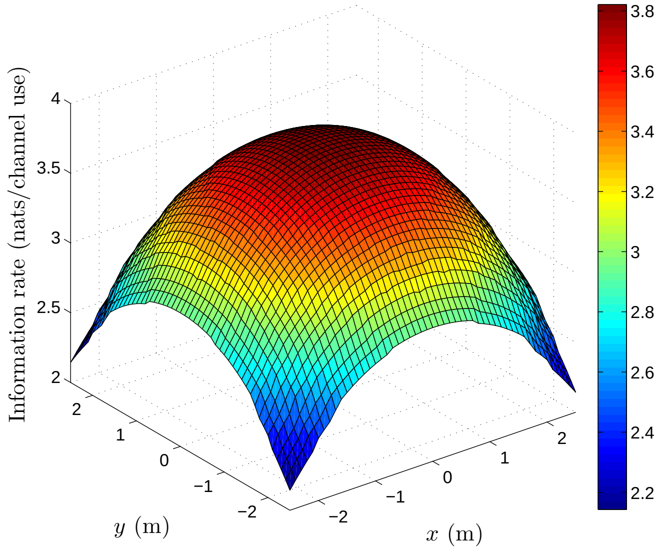

Fig. 8. Achievable communication rate, between Alice and Bob, as a function of Bob's location, without secrecy constraints.

Fig. 8 shows the achievable communication ra tween Alice and Bob, as a function of Bob's locati secrecy constraints. This rate is obtained using setting $\mathbf{w}_\text{ZF} = \mathbb{1}$.

Fig. 9 shows the secrecy rates achievable vi mal beamformer (14a) and zero-forcing beamform functions of A. Bob and Eve are located at (– and $(1.6, -0.7)$, respectively. Their channel gain provided in Table II with fixture indices corresponding to those illustrated in Fig. 6. As can be seen, the improvement in secrecy rate via optimal beamforming, compared to zero-forcing, is negligible and does not outweigh the simplicity of the zero-forcing scheme.

TABLE II
CHANNEL GAIN VECTORS

Fixture index	at $(-0.9, -2.0)$	at $(1.6, -0.7)$
	$\times 10^{-4}$	$\times 10^{-4}$
1	0.3482	0.0431
2	0.3765	0.1019
3	0.2042	0.2276
4	0.0843	0.3430
5	0.1823	0.0468
6	0.1928	0.1158
7	0.1222	0.2765
8	0.0597	0.4367
9	0.0756	0.0388
10	0.0783	0.0869
11	0.0579	0.1803
12	0.0345	0.2586
13	0.0321	0
14	0.0329	0.0495
15	0	0.0837
16	0	0.1063

In Fig. 10, Bob's location is fixed at $(-0.9, -2.0)$ and the secrecy rate in (16) is shown as a function of Eve's location within the entire room area. As expected, the secrecy rate significantly decreases when Eve is close to Bob. Once Eve is relatively far, e.g., more than about 2.5 m, the secrecy rate is almost independent of Eve's exact location. It is also interesting to characterize the loss in transmission rate caused by the secrecy constraint, i.e., $R_\text{B} - R_s$, by comparing the secrecy rates in Fig. 10 with $R_\text{B}(-0.9, -2.0) = 3.2256$ nats/channel use from Fig. 8.

In Fig. 11, Eve's location is fixed at $(1.6, -0.7)$ and the secrecy rate (16) is shown as a function of Bob's location. Even when Bob is relatively far from Eve, the secrecy rate still depends on Bob's location due to the dependence of R_s^ZF

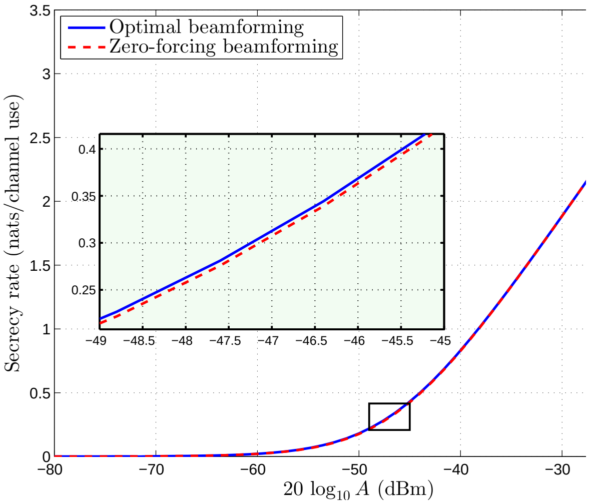

Fig. 9. Secrecy rates achievable via optimal beamforming (13) forcing beamforming (16) versus the amplitude constraint A in dBm. Bob and Eve are located at $(-0.9, -2.0)$ and $(1.6, -0.7)$, respectively, and their channel gains are provided in Table II. Noise power is -98.82 dBm.

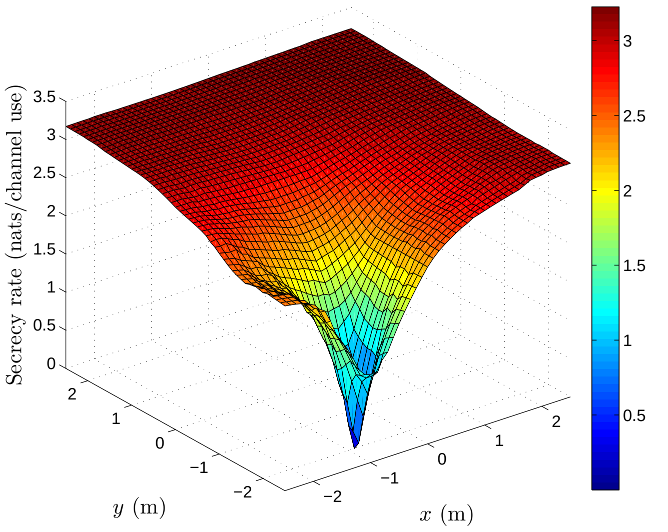

Fig. 10. Secrecy rate achievable via zero-forcing beamforming (16) as a function of Eve's location. Bob is located at $(-0.9, -2.0)$.

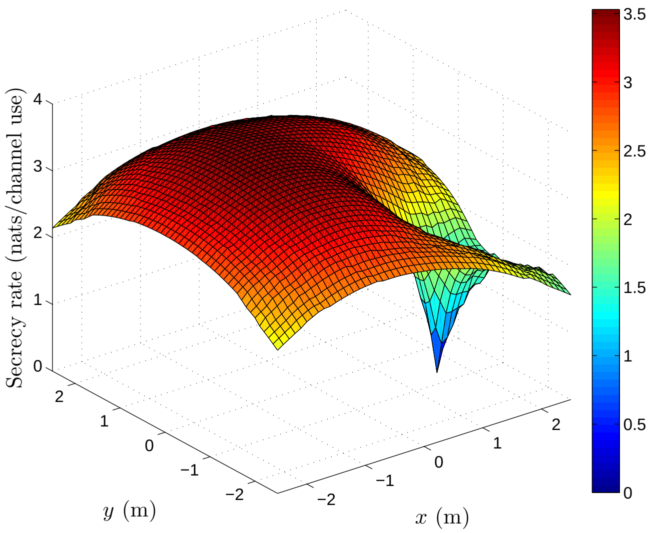

Fig. 11. Secrecy rate achievable via zero-forcing beamforming (16) as a function of Bob's location. Eve is located at $(1.6, -0.7)$.

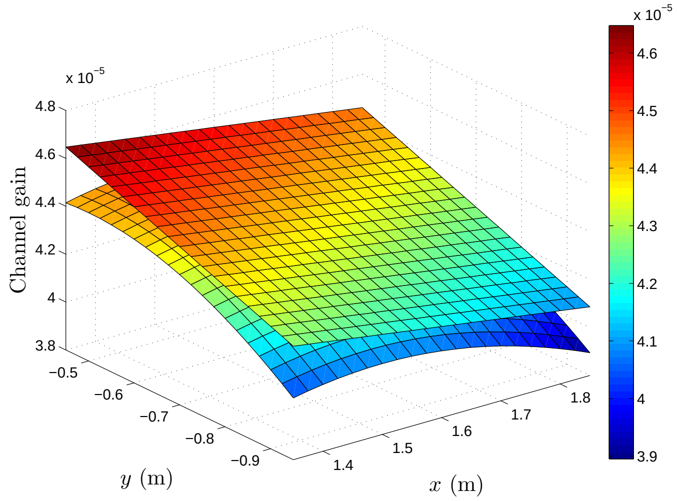

Fig. 12. Spatial distribution of the channel gain from Fixture 8 (see Fig. 6 for fixture indices) within a square of area $(0.5 \times 0.5 \text{ m}^2)$ centered at $(1.6, -0.7)$.

on $\mathbf{h}_{\rm B}$.

Fig. 12 highlights the error in estimating the channel gain caused by truncating Taylor's expansion after the first-order terms. The spatial distribution of the channel gain from Fixture 8 is shown within the square area bounded by $(1.6 \pm 0.25, -0.7 \pm 0.25)$. As expected, Taylor's approximation exhibits maximum error at the corners. The maximum relative error is 5.45% at $(1.85, -0.45)$.

Fig. 13 considers the robust beamforming problem and shows the improvement in the worst-case secrecy rate attained by applying the robust beamformer in (23a). Bob is located at $(-0.9, -2.0)$, and his channel gain is perfectly known to Alice. Eve is located somewhere within the square area $(1.6 \pm \epsilon, -0.7 \pm \epsilon)$. For relatively small ϵ, i.e., when Alice is quite certain about Eve's location, the non-robust beamformer exhibits a slightly-better performance. The reason is that two degrees of freedom are unnecessarily exploited with the robust beamformer to null out the signal at the directions of the second and third columns of $\tilde{\mathbf{H}}_{\rm E}$ in (21). As ϵ increases, the robust beamformer is clearly superior, and it slows down the decay in $R_s^{\rm wc}$ with increasing ϵ.

Finally, we validate the robust beamforming scheme over the entire room area, as shown in Fig. 14. We divide the room into 25 squares. Each square has an area of 1 m^2, and outlines possible locations for Eve. Bob is located at $(-0.9, -2.0)$, and his channel gain is perfectly known to Alice. Alice also knows which square bounds Eve's location, without knowing her exact location. From such information, Alice applies the robust beamformer in (23a). The resulting secrecy rate is shown as a function of Eve's location within each square. Worst-case secrecy rates $R_s^{\rm wc}$ are also shown. Notice that $R_s^{\rm wc}$ is zero when Bob and Eve are located within the same square, and it increases as Eve moves far away from Bob.

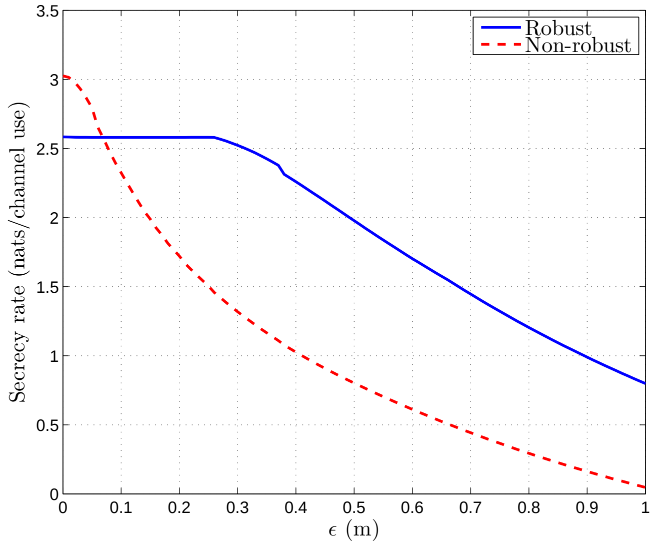

Fig. 13. Worst-case secrecy rate (25) versus ϵ, half the side length of the square outlining possible locations of Eve. Bob is located at $(-0.9, -2.0)$ and Eve's location is bounded by $(1.6 \pm \epsilon, -0.7 \pm \epsilon)$.

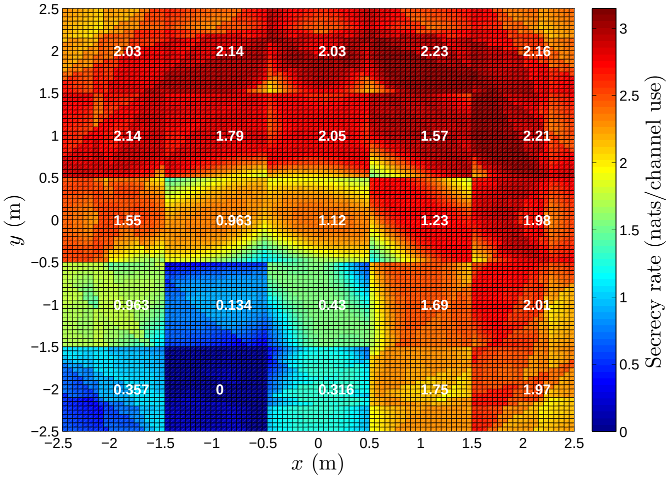

Fig. 14. Secrecy rate as a function of Eve's location when the robust beamformer (23a) is applied. Eve's location information is quantized into 25 squares, each of area 1 m^2, and the quantized location information is available to Alice. Bob is located at $(-0.9, -2.0)$. Worst-case secrecy rates (nats/channel use) are also shown inside each square.

VI. Conclusions

In this work, we proposed the use of physical-layer security techniques to enhance the confidentiality of VLC links. So far, there have been very few deployments of physical-layer security systems. One major shortcoming of such security schemes is performance sensitivity to channel information assumptions, especially for the eavesdropper's link. We believe, however, that VLC networks have a potential for the deployment of physical-layer security prototypes since realistic assumptions about the eavesdropper's channel can be made.

Unlike RF channels, the VLC channel is well-modelled with amplitude constraints imposed on the channel input, making it difficult to obtain analytical expressions for the secrecy capacity, even for the simple SISO case. Therefore, we derived closed-form lower and upper bounds on the secrecy capacity of the amplitude-constrained wiretap channel. Then, we utilized beamforming to obtain achievable secrecy rates for the MISO channel. We have shown that zero-forcing is an appropriate strategy for secure transmission over MISO VLC channels. Although suboptimal, zero-forcing is preferable as it is an achievability strategy that eliminates the need to use secrecy codes which involve stochastic encoding. We have also proposed a practical robust beamforming scheme which considerably improves worst-case secrecy rates when information about the eavesdropper's channel is imperfect due to location uncertainty. The robust scheme directly addresses the aforementioned problem of performance sensitivity to channel assumptions.

Appendix A
Derivation of the Lower Bounds on Secrecy Capacity

A. *Lower Bound* (9) *of Theorem 1*

The secrecy capacity in (8) can be lower-bounded by the difference between the channel capacities of Alice-Bob and Alice-Eve links as follows.

$$\begin{aligned} C_s^{\mathrm{SISO}} &= \max_{p_X} \left(\mathbb{I}(X;Y) - \mathbb{I}(X;Z) \right) \\ &\overset{(a)}{\geq} \max_{p_X} \mathbb{I}(X;Y) - \max_{p_X} \mathbb{I}(X;Z) \\ &= C_{\mathrm{B}} - C_{\mathrm{E}}, \end{aligned} \tag{27}$$

where (a) follows from the inequality

$$\max_{\mathbf{u}} \left(f_1(\mathbf{u}) - f_2(\mathbf{u}) \right) \geq \max_{\mathbf{u}} f_1(\mathbf{u}) - \max_{\mathbf{u}} f_2(\mathbf{u})$$

for arbitrary functions f_1 and f_2. Then, C_{B} and C_{E}, respectively, can be lower- and upper-bounded by [24, Theorem 5]

$$C_{\mathrm{B}} \geq \frac{1}{2} \log \left(1 + \frac{2 h_{\mathrm{B}}^2 A^2}{\pi e \sigma^2} \right), \tag{28a}$$

$$\begin{aligned} C_{\mathrm{E}} \leq &\left(1 - 2\mathcal{Q}\left(\frac{\delta + h_{\mathrm{E}} A}{\sigma} \right) \right) \log \frac{2(h_{\mathrm{E}} A + \delta)}{\sqrt{2\pi\sigma^2}\left(1 - 2\mathcal{Q}\left(\frac{\delta}{\sigma}\right)\right)} \\ &+ \mathcal{Q}\left(\frac{\delta}{\sigma} \right) + \frac{\delta}{\sqrt{2\pi\sigma^2}} e^{-\frac{\delta^2}{2\sigma^2}} - \frac{1}{2}, \end{aligned} \tag{28b}$$

where $\delta > 0$ is a free parameter. Finally, plugging (28) into (27) results in the lower bound in (9).

B. Lower Bound (10) *of Theorem 1*

Another lower bound on the secrecy capacity of (8) can be obtained as follows.

$$\begin{aligned}
C_s^{\mathrm{SISO}} &= \max_{p_X} \left(\mathbb{I}(X;Y) - \mathbb{I}(X;Z)\right)\\
&= \max_{p_X} \left(\mathbb{h}(Y) - \mathbb{h}(Y|X) - \mathbb{h}(Z) + \mathbb{h}(Z|X)\right)\\
&= \max_{p_X} \left(\mathbb{h}(Y) - \mathbb{h}(Z)\right)\\
&= \max_{p_X} \left(\mathbb{h}(h_{\mathrm{B}}X + W_{\mathrm{B}}) - \mathbb{h}(Z)\right)\\
&\overset{(a)}{\geq} \max_{p_X} \left(\frac{1}{2}\log\left(e^{2\mathbb{h}(h_{\mathrm{B}}X)} + e^{2\mathbb{h}(W_{\mathrm{B}})}\right)\right.\\
&\qquad\qquad \left. -\frac{1}{2}\log 2\pi e \times \mathtt{var}\left\{Z\right\}\right)\\
&\overset{(b)}{\geq} \frac{1}{2}\log\left(4h_{\mathrm{B}}^2A^2 + 2\pi e\sigma^2\right) - \frac{1}{2}\log 2\pi e\left(\frac{4h_{\mathrm{E}}^2A^2}{12} + \sigma^2\right)\\
&= \frac{1}{2}\log\frac{6h_{\mathrm{B}}^2A^2 + 3\pi e\sigma^2}{\pi e h_{\mathrm{E}}^2A^2 + 3\pi e\sigma^2}, \qquad (29)
\end{aligned}$$

where (a) follows from lower-bounding $\mathbb{h}(h_{\mathrm{B}}X + W_{\mathrm{B}})$ using the entropy-power inequality [34, Theorem 17.7.3], and upper-bounding $\mathbb{h}(Z)$ by the differential entropy of a Gaussian random variable with variance $\mathtt{var}\{Z\}$, and (b) from dropping the maximization, choosing a uniform distribution p_X over the interval $[-A, A]$, and substituting $\mathbb{h}(h_{\mathrm{B}}X) = \log(2h_{\mathrm{B}}A)$ and $\mathtt{var}\{Z\} = \mathtt{var}\{h_{\mathrm{E}}X\} + \mathtt{var}\{W_{\mathrm{E}}\} = (2h_{\mathrm{E}}A)^2/12 + \sigma^2$.

Appendix B
Derivation of the Upper Bound on Secrecy Capacity

We follow the approach proposed in [39], [40] to derive an upper bound on the secrecy capacity of the degraded wiretap channel using a *dual* expression for the secrecy capacity.

A. Duality-Based Upper Bound on Conditional Mutual Information

Theorem 2: The conditional mutual information $\mathbb{I}(X;Y|Z)$ is upper-bounded by

$$\mathbb{I}(X;Y|Z) \leq \mathbb{E}_{p_{XZ}}\left\{\mathbb{D}\big(p_{Y|XZ}(y|X,Z)\|q_{Y|Z}(y|Z)\big)\right\}, \quad (30)$$

where $p_{Y|XZ}$ is uniquely determined by the conditional distributions of the degraded wiretap channel, i.e., $p_{Y|X}$ and $p_{Z|Y}$, while $q_{Y|Z}$ is an arbitrary conditional distribution of Y given Z.

Proof: We begin with

$$\begin{aligned}
&\mathbb{I}(X;Y|Z)\\
&\quad = \int_{\mathcal{X}}\int_{\mathcal{Y}}\int_{\mathcal{Z}} p_{XYZ}(x,y,z)\log\frac{p_{Y|XZ}(y|x,z)}{p_{Y|Z}(y|z)}\,dx\,dy\,dz \quad (31)
\end{aligned}$$

and

$$\begin{aligned}
&\mathbb{E}_{p_{XZ}}\left\{\mathbb{D}\big(p_{Y|Z}(y|Z)\|q_{Y|Z}(y|Z)\big)\right\}\\
&\quad = \int_{\mathcal{X}}\int_{\mathcal{Y}}\int_{\mathcal{Z}} p_{XYZ}(x,y,z)\log\frac{p_{Y|Z}(y|z)}{q_{Y|Z}(y|z)}\,dx\,dy\,dz, \quad (32)
\end{aligned}$$

where $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are the support sets of X, Y, and Z, respectively. Adding (31) to (32), we obtain

$$\begin{aligned}
&\mathbb{I}(X;Y|Z) + \mathbb{E}_{p_{XZ}}\left\{\mathbb{D}\big(p_{Y|Z}(y|Z)\|q_{Y|Z}(y|Z)\big)\right\}\\
&\quad = \int_{\mathcal{X}}\int_{\mathcal{Y}}\int_{\mathcal{Z}} p_{XYZ}(x,y,z)\log\frac{p_{Y|XZ}(y|x,z)}{q_{Y|Z}(y|z)}\,dx\,dy\,dz\\
&\quad = \mathbb{E}_{p_{XZ}}\left\{\int_{\mathcal{Y}} p_{Y|XZ}(y|X,Z)\log\frac{p_{Y|XZ}(y|X,Z)}{q_{Y|Z}(y|Z)}\,dy\right\}\\
&\quad = \mathbb{E}_{p_{XZ}}\left\{\mathbb{D}\big(p_{Y|XZ}(y|X,Z)\|q_{Y|Z}(y|Z)\big)\right\}. \quad (33)
\end{aligned}$$

Then, the inequality in (30) follows by noting that the integral in (32) is always non-negative. □

Equality holds in (30) when $\mathbb{D}\big(p_{Y|Z}\|q_{Y|Z}\big) = 0$, i.e., when $q_{Y|Z} = p_{Y|Z}$ $\forall Z \in \mathcal{Z}$. Therefore, (30) can be written as

$$\mathbb{I}(X;Y|Z) = \min_{q_{Y|Z}} \mathbb{E}_{p_X\, p_{Z|X}}\left\{\mathbb{D}\big(p_{Y|XZ}(y|X,Z)\|q_{Y|Z}(y|Z)\big)\right\}. \quad (34)$$

Notice that the input distribution p_X in (34) is arbitrary, and there exists a unique distribution p_X^* that maximizes $\mathbb{I}(X;Y|Z)$, subject to the channel input constraints, resulting in the secrecy capacity C_s, i.e.,

$$C_s = \min_{q_{Y|Z}} \max_{p_X} \mathbb{E}_{p_X\, p_{Z|X}}\left\{\mathbb{D}\big(p_{Y|XZ}(y|X,Z)\|q_{Y|Z}(y|Z)\big)\right\}. \quad (35)$$

Then, by dropping the minimization and choosing an arbitrary conditional distribution $q_{Y|Z}$, we obtain the following upper bound on the secrecy capacity.

Lemma 1: An upper bound on the secrecy capacity of the degraded wiretap channel is given by

$$C_s \leq \mathbb{E}_{p_X^*\, p_{Z|X}}\left\{\mathbb{D}\big(p_{Y|XZ}(y|X,Z)\|q_{Y|Z}(y|Z)\big)\right\} \quad (36)$$

for an arbitrary conditional distribution $q_{Y|Z}$.

B. Upper Bound (11) *of Theorem 1*

Substituting for $\mathbb{D}(\cdot\|\cdot)$ in (36), we obtain

$$\begin{aligned}
C_s &\leq \mathbb{E}_{p_X^* p_{Z|X}}\left\{\int_{\mathcal{Y}} p_{Y|XZ}(y|X,Z)\log\frac{p_{Y|XZ}(y|X,Z)}{q_{Y|Z}(y|Z)}\,dy\right\}\\
&= \underbrace{\mathbb{E}_{p_X^*}\left\{\int_{\mathcal{Y}}\int_{\mathcal{Z}} p_{YZ|X}(y,z|X)\log p_{Y|XZ}(y|X,z)\,dy\,dz\right\}}_{I_1}\\
&\quad \underbrace{-\mathbb{E}_{p_X^*}\left\{\int_{\mathcal{Y}}\int_{\mathcal{Z}} p_{YZ|X}(y,z|X)\log q_{Y|Z}(y|z)\,dy\,dz\right\}}_{I_2}.
\end{aligned} \quad (37)$$

We define $\gamma_{\mathrm{B}}^2 = \sigma^2/h_{\mathrm{B}}^2$ and $\gamma_{\mathrm{E}}^2 = \sigma^2/h_{\mathrm{E}}^2$. Thus,

$$\begin{aligned}
I_1 &= \mathbb{E}_{p_X^*\, p_{YZ|X}}\left\{\log p_{Y|XZ}(Y|X,Z)\right\}\\
&= -\mathbb{h}(Y|X,Z)\\
&= -\left(\mathbb{h}(Y|X) + \mathbb{h}(Z|X,Y) - \mathbb{h}(Z|X)\right)\\
&= -\frac{1}{2}\log\left(2\pi e\frac{\gamma_{\mathrm{B}}^2(\gamma_{\mathrm{E}}^2 - \gamma_{\mathrm{B}}^2)}{\gamma_{\mathrm{E}}^2}\right). \quad (38)
\end{aligned}$$

To calculate I_2, we choose $q_{Y|Z}$ as

$$q_{Y|Z}(y|z) = \frac{1}{\sqrt{2\pi s^2}} e^{-\frac{(y-\mu z)^2}{2s^2}}, \tag{39}$$

where μ and s^2 are constants to be determined in (42).

For a degraded Gaussian wiretap channel, we have

$$\begin{aligned} p_{YZ|X}(y,z|x) &= p_{Y|X}(y|x)\, p_{Z|XY}(z|x,y) \\ &= p_{Y|X}(y|x)\, p_{Z|Y}(z|y) \\ &= \frac{1}{\sqrt{2\pi\gamma_{\mathrm{B}}^2}} e^{-\frac{(y-x)^2}{2\gamma_{\mathrm{B}}^2}} \frac{1}{\sqrt{2\pi(\gamma_{\mathrm{E}}^2-\gamma_{\mathrm{B}}^2)}} e^{-\frac{(z-y)^2}{2(\gamma_{\mathrm{E}}^2-\gamma_{\mathrm{B}}^2)}}. \end{aligned} \tag{40}$$

Therefore,

$$\begin{aligned} I_2 = -\mathbb{E}_{p_X^*} \Bigg\{ & \frac{1}{\sqrt{2\pi\gamma_{\mathrm{B}}^2}} \int_{-\infty}^{\infty} e^{-\frac{(y-X)^2}{2\gamma_{\mathrm{B}}^2}} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\left(\gamma_{\mathrm{E}}^2-\gamma_{\mathrm{B}}^2\right)}} \times \\ & e^{-\frac{(z-y)^2}{2(\gamma_{\mathrm{E}}^2-\gamma_{\mathrm{B}}^2)}} \left(-\frac{1}{2}\log 2\pi s^2 - \frac{(y-\mu z)^2}{2s^2}\right) dy\, dz \Bigg\} \\ = \frac{1}{2}\log 2\pi s^2 + \mathbb{E}_{p_X^*} \Bigg\{ & \frac{1}{\sqrt{2\pi\gamma_{\mathrm{B}}^2}} \int_{-\infty}^{\infty} e^{-\frac{(y-X)^2}{2\gamma_{\mathrm{B}}^2}} \times \\ & \frac{1}{2s^2}\left(\mu^2\left(\gamma_{\mathrm{E}}^2-\gamma_{\mathrm{B}}^2\right) + (\mu-1)^2 y^2\right) dy \Bigg\} \\ = \frac{1}{2}\log 2\pi s^2 & \\ + \mathbb{E}_{p_X^*} & \left\{\frac{1}{2s^2}\left(\mu^2\left(\gamma_{\mathrm{E}}^2-\gamma_{\mathrm{B}}^2\right) + (\mu-1)^2\left(X^2+\gamma_{\mathrm{B}}^2\right)\right)\right\} \\ \leq \frac{1}{2}\log 2\pi s^2 + & \frac{1}{2s^2}\left(\mu^2\left(\gamma_{\mathrm{E}}^2-\gamma_{\mathrm{B}}^2\right) + (\mu-1)^2\left(A^2+\gamma_{\mathrm{B}}^2\right)\right) \end{aligned} \tag{41}$$

where the last inequality follows from $\mathbb{E}_{p_X^*}\{X^2\} \leq A^2$. To minimize the expression in (41), we choose

$$\mu = \frac{A^2+\gamma_{\mathrm{B}}^2}{A^2+\gamma_{\mathrm{E}}^2}, \tag{42a}$$

$$s^2 = \frac{(A^2+\gamma_{\mathrm{B}}^2)(\gamma_{\mathrm{E}}^2-\gamma_{\mathrm{B}}^2)}{A^2+\gamma_{\mathrm{E}}^2}. \tag{42b}$$

Plugging (42) into (41) and adding the result to (38), we obtain

$$\begin{aligned} C_s &\leq \frac{1}{2}\log\frac{(A^2+\gamma_{\mathrm{B}}^2)\gamma_{\mathrm{E}}^2}{(A^2+\gamma_{\mathrm{E}}^2)\gamma_{\mathrm{B}}^2} \\ &= \frac{1}{2}\log\frac{h_{\mathrm{B}}^2 A^2+\sigma^2}{h_{\mathrm{E}}^2 A^2+\sigma^2}. \end{aligned} \tag{43}$$

Notice that the upper bound in (43) can be obtained by relaxing the amplitude constraint into the average power constraint $\mathbb{E}\{X^2\} \leq A^2$ and calculating the secrecy capacity of the resulting channel. Nevertheless, the proposed framework is useful for deriving upper bounds on the secrecy capacity of arbitrary degraded channels since Lemma 1 holds for arbitrary distributions $p_{Y|X}$ and $p_{Z|Y}$, i.e., the main and degraded channels need not be Gaussian.

ACKNOWLEDGMENT

The authors would like to thank Prof. Steve Hranilovic at McMaster University for insightful comments and suggestions.

REFERENCES

[1] "IEEE Standard for Local and Metropolitan Area Networks–Part 15.7: Short-Range Wireless Optical Communication Using Visible Light," *IEEE Std 802.15.7-2011*, pp. 1–309, 2011.

[2] R. Lenk and C. Lenk, *Practical Lighting Design With LEDs*. Wiley, 2011.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, ser. Foundations and Trends® in Communications and Information Theory. Now Publishers, 2009, vol. 5, no. 4-5.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, October 2011.

[5] R. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

[6] H. Wen, *Physical Layer Approaches for Securing Wireless Communication Systems*, ser. SpringerBriefs in Computer Science. Springer, 2013.

[7] X. Zhou, L. Song, and Y. Zhang, Eds., *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[8] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*, ser. SpringerBriefs in Electrical and Computer Engineering. Springer, 2014.

[9] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third quarter 2014.

[10] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[11] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[12] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[13] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[14] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, Sept 2009.

[15] R. Liu and H. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 3, pp. 1235–1249, March 2009.

[16] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.

[17] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[18] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

[19] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[20] K. Tae-Gyu, "Visible-light communications," in *Advanced Optical Wireless Communication Systems*, S. Arnon, J. R. Barry, G. K. Karagiannidis, R. Schober, and M. Uysal, Eds. Cambridge University Press, 2012, pp. 351–368.

[21] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, "Visible light communications," in *Optical Wireless Communications: System and Channel Modelling with MATLAB®*. CRC Press, 2013, pp. 443–496.

[22] H. Elgala, R. Mesleh, and H. Haas, "Predistortion in optical wireless transmission using OFDM," in *Ninth International Conference on Hybrid Intelligent Systems*, vol. 2, Aug 2009, pp. 184–189.

[23] S. Hranilovic and F. Kschischang, "Optical intensity-modulated direct detection channels: signal space and lattice codes," *IEEE Transactions on Information Theory*, vol. 49, no. 6, pp. 1385–1399, June 2003.

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

[25] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, July/October 1948.

[26] J. G. Smith, *On the Information Capacity of Peak and Average Power Constrained Gaussian Channels*. Ph.D. dissertation, Department of Electrical Engineering, University of California, Berkeley, California, 1969.

[27] ——, "The information capacity of amplitude- and variance-constrained scalar Gaussian channels," *Journal of Information and Control*, vol. 18, pp. 203–219, 1971.

[28] S. Arimoto, "An algorithm for computing the capacity of arbitrary discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 14–20, Jan 1972.

[29] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with an amplitude constraint," in *2012 IEEE Information Theory Workshop (ITW)*, Sept 2012, pp. 139–143.

[30] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 100–107, 2004.

[31] J. Grubor, S. Randel, K.-D. Langer, and J. Walewski, "Broadband information broadcasting using LED-based interior lighting," *Journal of Lightwave Technology*, vol. 26, no. 24, pp. 3883–3892, Dec 2008.

[32] L. Zeng et al., "High data rate multiple input multiple output (MIMO) optical wireless communications using white LED lighting," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 9, pp. 1654–1662, 2009.

[33] J. Kahn and J. Barry, "Wireless infrared communications," *Proceedings of the IEEE*, vol. 85, no. 2, pp. 265–298, Feb 1997.

[34] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley, 2006.

[35] E. Wong, *Active-Set Methods for Quadratic Programming*. Ph.D. dissertation, University of California, San Diego, 2011.

[36] J.-Y. Gotoh and H. Konno, "Maximization of the ratio of two convex quadratic functions over a polytope," *Computational Optimization and Applications, 20*, pp. 43–60, 2001.

[37] H. P. Benson, "Fractional programming with convex quadratic forms and functions," *European Journal of Operational Research, 173 - Elsevier*, pp. 351–369, 2005.

[38] W. Dinkelbach, "On nonlinear fractional programming," *Management Science*, vol. 13, no. 7, pp. 492–498, 1967.

[39] A. Lapidoth and S. Moser, "Capacity bounds via duality with applications to multiple-antenna systems on flat-fading channels," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2426–2467, Oct 2003.

[40] S. M. Moser, *Duality-Based Bounds on Channel Capacity*. Ph.D. dissertation, Swiss Federal Institute of Technology, Zürich, 2004.

Ayman Mostafa (S'08) received the B.Sc. degree with honours in electrical engineering from Alexandria University, Egypt in 2006, and the M.A.Sc. degree in electrical engineering from McMaster University, Hamilton, ON, Canada in 2012. He is currently working towards the Ph.D. degree in electrical engineering at The University of British Columbia, Vancouver, BC, Canada. His current research interests are in the areas of optical wireless communications, secure communications, and signal processing techniques for physical-layer security.

Lutz Lampe (M'02-SM'08) received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the University of Erlangen, Erlangen, Germany, in 1998 and 2002, respectively. Since 2003, he has been with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada, where he is a Full Professor. His research interests are broadly in theory and application of wireless, optical wireless and power line communications. Dr. Lampe was the General (Co-)Chair for 2005 ISPLC and 2009 IEEE ICUWB and General (Co-)Chair for the 2013 IEEE SmartGridComm. He is currently an Associate Editor of the IEEE WIRELESS COMMUNICATIONS LETTERS and the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and has served as an Associate Editor and a Guest Editor of several IEEE TRANSACTIONS and journals. He was a (co-)recipient of a number of Best Paper Awards, including awards at the 2006 IEEE International Conference on Ultra-Wideband (ICUWB), 2010 IEEE International Communications Conference (ICC), and 2011 IEEE International Conference on Power Line Communications (ISPLC).