Secrecy Capacity of LiFi Systems

Hanaa Abumarshoud[1], Mohammad Dehghani Soltani[2], Majid Safari[2], and Harald Haas[1]

[1]LiFi R&D Centre, Technology & Innovation Centre, Department of Electronic & Electrical Engineering, The University of Strathclyde, Glasgow, UK
[2]School of Engineering, University of Edinburgh, Edinburgh, UK

Invited paper

ABSTRACT

Radio frequency (RF) signals propagate through most materials that we are surrounded by while light is blocked by many of these materials. This feature makes wireless networks based on light (which are also referred to as LiFi networks) inherently more secure. However, it can also lead to sudden link failure if the legitimate data link is blocked because of user movements or changes in device orientation. In this paper, the secrecy capacity has been analysed with the consideration of imperfect channel state information, random device orientation and probability of link blockage for the case of a single eavesdropper. It has been found that the secrecy capacity almost doubles in a standing activity as opposed to a sitting activity and that the density of blocking objects degrades the secrecy capacity in single access point networks. It is evident that environmental factors and user behaviour have a significant impact on the secrecy performance and, thus, need to be considered for robust physical layer security (PLS) design in LiFi networks.

Keywords: Physical layer security, secrecy capacity, link blockage, random orientation and light-fidelity (LiFi)

1. INTRODUCTION

According to the recent Cisco report, it is predicted that the average mobile data traffic will reach 77 exabytes per month in 2022.[1] This immense data traffic requirement would be supported by fifth generation (5G) and beyond cellular networks. LiFi, as a subset of optical wireless communications (OWCs), is a high-speed bidirectional and fully networked wireless communication technology in which visible light and infrared light sources are used for the downlink and the uplink, respectively.[2,3] Compared to radio frequency (RF) networks, LiFi offers considerable advantages such as the availability of huge and unregulated spectrum resource as well as the ability to easily confine and control the spatial distribution of light. These benefits have put LiFi in the scope of academic and industrial research.

LiFi systems inherently provide enhanced security in comparison to RF networks as the light does not penetrate through walls and opaque objects. However, security problems emerge due to the broadcast feature of LiFi systems, which makes LiFi in principle as vulnerable as other RF wireless systems if the eavesdroppers exist within the coverage area of the LiFi access point (AP) of interest. In order to ensure a robust and secure connection for legitimate users, various physical layer security (PLS) techniques can be employed. However, it is not straightforward to directly develop the PLS solutions used in RF systems for LiFi. This is due to the natural distinctions in LiFi systems such as the requirement of real and positive signals, as well as the peak-power constraints imposed by the dynamic range of light-emitting diodes (LEDs).[4] Apart from these differences, LiFi channels are also highly influenced by user behaviour like blockage and random device orientation. Hence, it is important to assess the impact of these user-induced probabilistic factors on the secrecy analysis of LiFi systems.

A number of surveys have been reported in the related literature regarding PLS in visible light communication (VLC) systems.[5,6] In,[5] the PLS in OWCs, including free space optical (FSO) systems and VLC, has

Further author information: (Send correspondence to H.H. :E-mail: harald.haas@strath.ac.uk)
H.A.: E-mail: hanaa.abumarshoud@strath.ac.uk
M.D.S.: E-mail: m.dehghani@ed.ac.uk
M.S.: E-mail: majid.safari@ed.ac.uk
H.H. :E-mail: harald.haas@strath.ac.uk

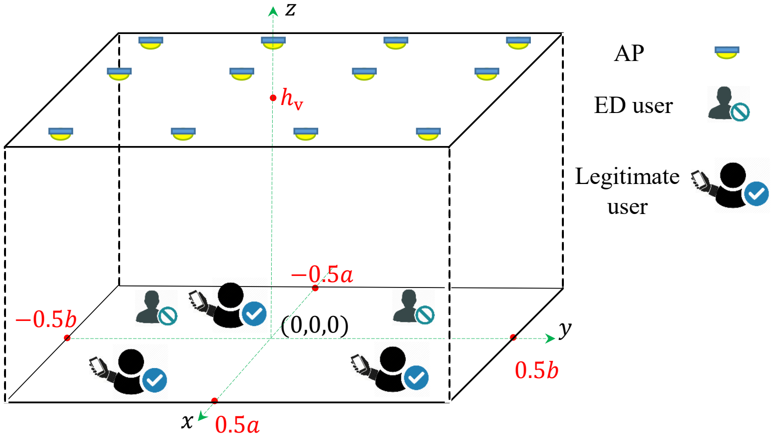

Figure 1. System configuration: a LiFi system with multiple APs, legitimate users and eavesdroppers (ED users).

been reviewed. The authors in[6] recently surveyed the latest applications of PLS in VLC networks. Various VLC system configurations, including single-input-single-output (SISO), multiple-input-single-output (MISO) and multiple-input-multiple-output (MIMO) as well as hybrid RF/VLC networks have been considered and the secrecy capacity performance for each of them has been evaluated. The work in[7] studied methods and solutions to enhance the security and provide more secure communication links for LiFi. It is noted that the majority of studies considering PLS in LiFi networks assume that the optical channel is deterministic and that the LiFi AP has perfect knowledge of the channel gain of all users, including potential eavesdroppers.[8–11]

In this paper, we aim to provide more realistic insights into the secrecy performance in LiFi systems by analysing the secrecy capacity under the assumption of imperfect knowledge of the eavesdropper's channel state information (CSI), probability of link blockage and random device orientation. The rest of the paper is organised as follows: Section 2 describes the LiFi system and channel model. Section 3 presents the derived secrecy capacity expressions, Section 4 shows the simulation and analytic results while Section 5 concludes the paper.

2. SYSTEM MODEL

2.1 LiFi System Configuration

We consider an indoor LiFi network where the LEDs act as APs, providing illumination as well as communication functionalities. It is assumed that the LEDs are point sources that follow Lambertian patterns and work in the linear range of the current-to-power curve. The AP aims to transmit confidential messages to a legitimate user in the presence of an eavesdropper within its coverage area. Fig. 1 shows a general configuration of the indoor LiFi network with both legitimate and eavesdropper users. When an AP transmits a signal to legitimate users, passive eavesdroppers can also receive the signal and decode it. We refer to the AP, legitimate user and eavesdropper as Alice, Bob and Eve, respectively. At the receiver side, a photodiode (PD) is mounted on the user equipment (UE) to detect the received signal by means of direct detection. The orientation of UEs is assumed to follow a Laplace distribution as shown in[12] for static users. The received signals at Bob and Eve are expressed as:

$$y_B = h_B x + z_B, \tag{1}$$

and

$$y_E = h_E x + z_E, \tag{2}$$

respectively, where x is the transmitted signal, h_B and h_E denote the channel gain of Bob and Eve, respectively. Also, $z_B \sim \mathcal{N}(0, \sigma_B^2)$ and $z_E \sim \mathcal{N}(0, \sigma_E^2)$ denote the additive white Gaussian noise at Bob and Eve with variances σ_B^2 and σ_E^2, respectively. Since VLC systems employ intensity modulation at the transmitter and direct detection at the receiver, the optical signal x follows the following constraint:

$$x \geq 0, \tag{3}$$

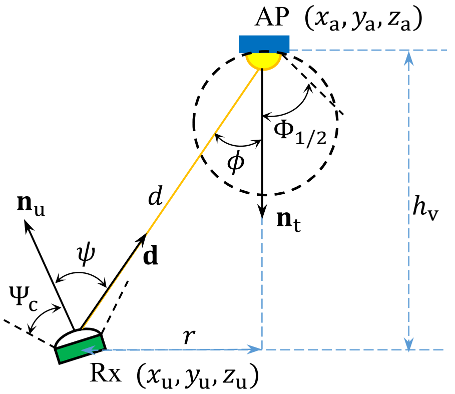

Figure 2. Geometry of LOS propagation.

which states that the signal must be strictly non-negative. Moreover, for practical considerations, the average signal power is constrained by the nominal optical intensity in order to guarantee that the required illumination level is satisfied, which can be mathematically expressed as:

$$E(x) = \zeta P, \tag{4}$$

where $\zeta \in (0, 1]$ is the power dimming factor and P is the LED nominal optical power.

2.2 Light Propagation Model

We focus on the downlink transmission of a LiFi network, where the communication is based on a line-of-sight (LOS) link. It is assumed that the LiFi cells are far from the walls so that the diffuse links are negligible. The LOS link geometry is illustrated in Fig. 2. The direct current (DC) gain of the LOS link between the AP and the receiver is given as follows:[4]

$$H_{\mathrm{LOS}} = \frac{(m+1)A}{2\pi d^2} \cos^m \phi \; g(\psi) \cos\psi \; \mathrm{rect}\left(\frac{\psi}{\Psi_c}\right), \tag{5}$$

where d is the Euclidean distance between the UE and the AP; A is the physical area of the detector; ϕ and ψ are the angle of radiance with respect to the axis normal to the AP plane, and the angle of incidence with respect to the axis normal to the receiver plane, respectively. Furthermore, $\mathrm{rect}(\frac{\psi}{\Psi_c}) = 1$ for $0 \leq \psi \leq \Psi_c$ and 0 otherwise. The receiver field of view (FOV) is denoted by Ψ_c. The optical concentrator, $g(\psi)$, is $g(\psi) = \dfrac{\varsigma^2}{\sin^2 \Psi_c}$ for $0 \leq \psi \leq \Psi_c$, where ς stands for the refractive index; otherwise $g(\psi) = 0$. The Lambertian order is given as, $m = -\frac{1}{\log_2(\cos \Phi_{1/2})}$, where $\Phi_{1/2}$ is the half-intensity angle.[4] The radiance angle ϕ and the incidence angle ψ of the AP and the receiver can be calculated using the rules from analytical geometry as:

$$\cos\phi = \frac{-\mathbf{d} \cdot \mathbf{n}_t}{\|\mathbf{d}\|}, \qquad \cos\psi = \frac{\mathbf{d} \cdot \mathbf{n}_u}{\|\mathbf{d}\|}, \tag{6}$$

where $\mathbf{n}_t = [0, 0, -1]^T$ and $\mathbf{n}_u$ are the normal vectors at the AP and the receiver planes, respectively and $\mathbf{d}$ denotes the distance vector from the receiver to the AP. The symbols $\cdot$ and $\|\cdot\|$ denote the inner product and the Euclidean norm operators, respectively. Also, $(.)^T$ denotes the transpose operator.

2.3 Blockage Model

LOS blockage can significantly affect the user performance in LiFi systems. In this study, we consider the effect of dynamic blockage which results from other users moving in the proximity of the UE.[13] In fact, once the UE is connected to an AP, the dynamic blockers are the only cause of blockage under the assumption that the user does not move or change its direction. The bodies of moving users are the main source of dynamic blockage. In this study and similar to,[14] a human body is modeled as a cylinder with radius of l_b and height of h_b as shown

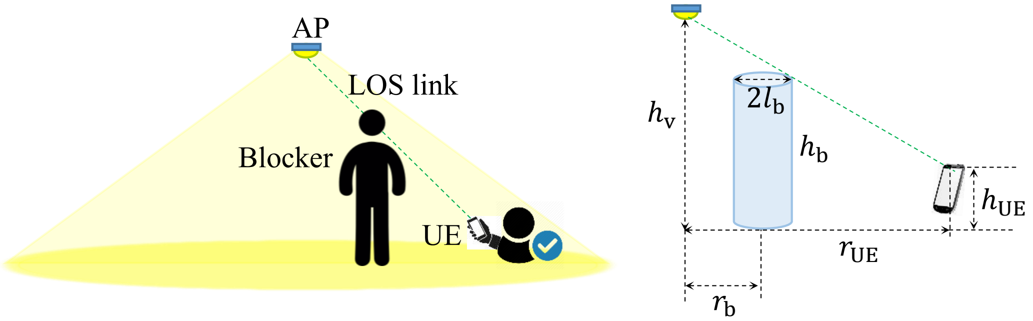

Figure 3. Geometry of link blockage

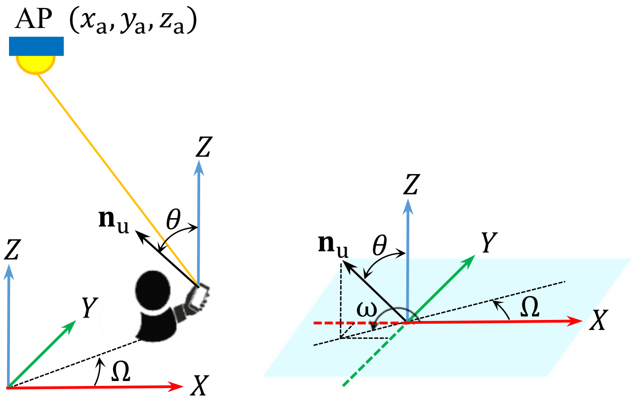

Figure 4. Geometry of a randomly-oriented UE and its spherical coordinates.

in Fig. 3. Assuming a Poisson point process (PPP) distribution with a density of κ_b for the blockers, the average probability of the link blockage is given as:

$$\mathcal{P}_b = 1 - \exp\left(-c_0 r_\mathrm{UE}\right), \tag{7}$$

where $c_0 = 2l_\mathrm{b}\kappa_\mathrm{b}\frac{h_\mathrm{b}-h_\mathrm{UE}}{h_\mathrm{v}-h_\mathrm{UE}}$ with h_UE and h_v as the height of the UE and the AP, respectively. It is clear that the average probability of link blockage depends on the geometry of the blockers as well as their density.

2.4 Random Orientation

Device orientation is an important factor that can significantly influence the performance of UEs. However, the majority of related studies have ignored the impact of device orientation in their analysis. The statistics of device orientation have been derived through a set of experimental measurements for both sitting and walking activities in.[12] The normal vector, $\mathbf{n}_\mathrm{u}$, can be expressed in terms of the polar angle, θ, and azimuth angle, ω, in the spherical coordinates as shown in Fig 4. Accordingly, we have:

$$\mathbf{n}_\mathrm{u} = [\sin(\theta)\cos(\omega), \sin(\theta)\sin(\omega), \cos(\theta)]^\mathrm{T}. \tag{8}$$

The azimuth angle ω shows the angle between the positive direction of the X axis and the projection of $\mathbf{n}_\mathrm{u}$ in the XY-plane. Here, we define $\Omega = \omega + \pi$ as the direction that the user is facing.[12]

Substituting (8) in (6) and (5), it can be inferred that when the UE location and the direction in which the user is facing are fixed, the channel gain depends on the polar angle θ. The experimental measurements reported in[12] confirmed that the polar angle θ follows a Laplace distribution for sitting activities with the mean and variance of $\mu_\theta = 41°$ and $\sigma_\theta = 7.68°$, respectively. Therefore, the probability density function (PDF) of the polar angle is given as:[12]

$$f(\theta) = \frac{\exp\left(-\frac{|\theta-\mu_\theta|}{b_\theta}\right)}{2b_\theta}. \tag{9}$$

Based on the Laplace distribution for θ, it is shown that the channel gain follows a truncated Laplace distribution as follows:[12]

$$f_{\mathrm{H}}(h) = \frac{\exp\left(-\frac{|h-\mu_{\mathrm{H}}|}{b_{\mathrm{H}}}\right)}{b_{\mathrm{H}}\left(2-\exp\left(-\frac{h_{\max}-\mu_{\mathrm{H}}}{b_{\mathrm{H}}}\right)\right)} + F_{\theta}\left(\theta_0\right)\delta(h), \tag{10}$$

where $h_{\min} \leq h \leq h_{\max}$; the mean and scale parameter of the channel gain are given as:

$$\mu_{\mathrm{H}} = \frac{H_0}{d^{m+2}}\left(\lambda_1 \sin\mu_{\theta} + \lambda_2 \cos\mu_{\theta}\right), \tag{11a}$$

$$b_{\mathrm{H}} = \frac{H_0}{d^{m+2}} b_{\theta} |\lambda_1 \cos\mu_{\theta} - \lambda_2 \sin\mu_{\theta}|, \tag{11b}$$

where $H_0 = \frac{(m+1)Ag_{\mathrm{f}}\varsigma^2 h_{\mathrm{v}}^m}{2\pi\sin^2\Psi_{\mathrm{c}}}$. The factors λ_1 and λ_2 depends on the UE location and facing direction of the user, which are given as:

$$\lambda_1 = \frac{r}{d}\cos\left(\Omega - \tan^{-1}\left(\frac{y_{\mathrm{u}}-y_{\mathrm{a}}}{x_{\mathrm{u}}-x_{\mathrm{a}}}\right)\right), \tag{12a}$$

$$\lambda_2 = \frac{h_{\mathrm{v}}}{d}. \tag{12b}$$

where h_{v} and r are respectively the vertical and horizontal distance between the UE and the AP as shown in Fig. 2. Note that in (10), $F_{\theta}\left(\theta_0\right) = \int_0^{\theta_0} f(\theta)\mathrm{d}\theta$, where $\theta \leq \theta_0$ results in $\psi \leq \Psi_{\mathrm{c}}$, and therefore, the channel gain becomes zero. The angle θ_0 is given as:

$$\theta_0 = \cos^{-1}\left(\frac{\cos\Psi_{\mathrm{c}}}{\sqrt{\lambda_1^2+\lambda_2^2}}\right) + \tan^{-1}\left(\frac{\lambda_1}{\lambda_2}\right). \tag{13}$$

Finally, it should be noted that the support range of the channel gain in (10) is $h_{\min} \leq h \leq h_{\max}$ with

$$h_{\min} = \begin{cases} \frac{H_0}{d^{m+2}}\cos\Psi_{\mathrm{c}}, & \cos\ \psi < \cos\Psi_{\mathrm{c}} \\ \dfrac{H_0}{d^{m+2}}\min\{\lambda_1, \lambda_2\}, & \text{o.w}, \end{cases} \tag{14a}$$

$$h_{\max} = \begin{cases} \dfrac{H_0}{d^{m+2}}\lambda_2, & \text{if } \lambda_1 < 0 \\ \dfrac{H_0}{d^{m+2}}\sqrt{\lambda_1^2+\lambda_2^2}, & \text{if } \lambda_1 \geq 0. \end{cases} \tag{14b}$$

3. SECRECY CAPACITY ANALYSIS

In this section, we derive lower bounds for the secrecy capacity in LiFi systems when the Alice-Bob link is subject to eavesdropping by a single eavesdropper. To this end, we assume a VLC link with an average optical power constraint as described in Section 2. Since the eavesdropper is typically a passive user that does not share its information with the AP, we assume that the AP only acquires partial knowledge about the location of Eve. It is noted that a similar assumption was adopted in,[15] where it was assumed that the AP can utilise built-in motion sensors deployed in LED fixtures to predict the existence of passive eavesdroppers. More specifically, we assume that Alice obtains imperfect CSI of Eve, which is modeled as a normally distributed random variable. It is noted that this assumption has been previously adopted as a reasonable model for imperfect CSI in indoor VLC systems in.[16–18] As a result, we define: $h_E \sim \mathcal{N}(\mu, \sigma^2)$, where μ is the expected value of the channel gain of Eve. We start our analysis with an assumption of a deterministic channel gain of Bob and then move to more realistic assumptions which include the effect of random receiver orientation.

Proposition 1: For the case of a single eavesdropper with normally distributed CSI, $h_E \sim \mathcal{N}(\mu, \sigma^2)$, the expected lower bound for the secrecy capacity as calculated at Alice can be expressed as:

$$\mathcal{C}_s^{1\mathrm{E}} \geq \frac{1}{4}\ln\left(\frac{e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2\sigma_E^{-2}}\right)\Upsilon(\kappa) - \frac{1}{2}\ln\left(\zeta^2P^2(\mu^2+\sigma^2)) + \sigma_E^2\right), \tag{15}$$

where κ is the maximum value of the square of Eve's channel gain, and $\Upsilon(\kappa) = \mathrm{erf}\left(\frac{\sqrt{\kappa}-\mu}{\sqrt{2\sigma^2}}\right) + \mathrm{erf}\left(\frac{\sqrt{\kappa}+\mu}{\sqrt{2\sigma^2}}\right)$ and $\mathrm{erf}(w)$ is the error function evaluated as $\frac{1}{\sqrt{\pi}}\int_{t=-w}^{w} e^{-t^2}dt$. Also, σ_B^2 and σ_E^2 denote the variance of receiver noise at Bob and Eve, respectively, and $\zeta \in (0,1]$ is the dimming factor.

Proof. For a VLC channel with average optical power constraints, the secrecy capacity with the existence of a single eavesdropper is lower-bounded by:[19]

$$\mathcal{C}_s^{1\mathrm{E}} \geq \frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2} \times \frac{e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2}{\zeta^2P^2h_E^2 + \sigma_E^2}\right), \tag{16}$$

since the CSI of Eve is modelled to follow a normal distribution,[16–18] i.e., $h_E \sim \mathcal{N}(\mu, \sigma^2)$, we denote the square of the channel gain of Eve as y and obtain its PDF as follows:

$$\begin{aligned} F_Y(y) &= \mathbb{P}[Y \leq y] = \mathbb{P}[h_E^2 \leq y] = \mathbb{P}[|h_E| \leq \sqrt{y}] \\ &= \mathbb{P}[-\sqrt{y} < h_E < \sqrt{y}] = \Phi(\sqrt{y}) - \Phi(-\sqrt{y}), \end{aligned} \tag{17}$$

where $\Phi(.)$ denotes the CDF of normal distribution. Differentiating with respect to y we get,

$$\begin{aligned} f_Y(y) = F_Y'(y) &= \frac{1}{2\sqrt{y}}\phi(\sqrt{y}) + \frac{1}{2\sqrt{y}}\phi(-\sqrt{y}) \\ &= \frac{1}{2\sqrt{2\pi\sigma^2y}}e^{-\frac{(\sqrt{y}-\mu)^2}{2\sigma^2}} + \frac{1}{2\sqrt{2\pi\sigma^2y}}e^{-\frac{(-\sqrt{y}-\mu)^2}{2\sigma^2}}. \end{aligned} \tag{18}$$

Accordingly, the secrecy capacity with imperfect CSI of Eve can be lower-bounded as:

$$\begin{aligned} \mathcal{C}_s^{1\mathrm{E}} &\geq \int_{y=0}^{\kappa} \frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2} \times \frac{e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2}{\zeta^2P^2y + \sigma_E^2}\right) f_Y(y)dy \\ &= \int_{y=0}^{\kappa}\left[\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\right) + \frac{1}{2}\ln\left(e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2\right)\right] f_Y(y)dy - \int_{y=0}^{\kappa}\frac{1}{2}\ln\left(\zeta^2P^2y + \sigma_E^2\right) f_Y(y)dy \end{aligned} \tag{19}$$

where κ denotes maximum value of the y. The first integral evaluates to:

$$\left[\frac{1}{4}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\right) + \frac{1}{4}\ln\left(e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2\right)\right] \times \left(\mathrm{erf}\left(\frac{\sqrt{\kappa}-\mu}{\sqrt{2\sigma^2}}\right) + \mathrm{erf}\left(\frac{\sqrt{\kappa}+\mu}{\sqrt{2\sigma^2}}\right)\right). \tag{20}$$

To evaluate the second integral, we use Jensen's inequality which states that $\mathbb{E}[\phi(y)] \leq \phi(\mathbb{E}[y])$ for random variable y and a convex function ϕ. Hence we can write:

$$\int_{y=0}^{\kappa}\frac{1}{2}\ln\left(\zeta^2P^2y + \sigma_E^2\right) f_Y(y)dy \leq \frac{1}{2}\ln\left(\zeta^2P^2(\mu^2+\sigma^2)) + \sigma_E^2\right), \tag{21}$$

by combining (21) and (20), we obtain the lower bound for the secrecy capacity in (15), which completes the proof. □

3.1 Effect of Link Blockage

LOS blockage causes disruption in the Alice-Bob link, which could lead to a degradation in Bob's secrecy capacity. Next, we evaluate the secrecy capacity taking into consideration the blockage probability of Bob, $\mathcal{P}_b$, which could be calculated based on the blockage model presented in Section 2.3. Based on this, Alice could evaluate the secrecy capacity and secrecy outage probability of the Alice-Bob link by utilizing the information available about the probability of a blockage occurring, i.e., the density of the moving objects in the room and the coordinates of Bob.

Proposition 2: Assuming a blockage probability of $\mathcal{P}_b$, the secrecy capacity can be lower-bounded as:

$$\ddot{\mathcal{C}}_s^{1\mathrm{E}} \geq (1-\mathcal{P}_b)\,\mathcal{C}_s^{1\mathrm{E}} + \frac{1}{4}\mathcal{P}_b\ln(\sigma_E^2)\Upsilon(\kappa) - \frac{1}{2}\mathcal{P}_b\ln(\zeta^2P^2(\mu^2+\sigma^2) + \sigma_E^2), \tag{22}$$

where $\Upsilon(\kappa)$ and $\mathcal{C}_s^{1\mathrm{E}}$ are defined in (15).

Proof. Under the assumption of Bob's link blockage, the secrecy capacity can be lower-bounded as:

$$\ddot{\mathcal{C}}_s^{1_{\mathrm{E}}} \geq (1-\mathcal{P}_b) \times \left[\mathcal{C}_s^{1_{\mathrm{E}}}|\text{no blockage}\right] + \mathcal{P}_b \times \left[\mathcal{C}_s^{1_{\mathrm{E}}}|\text{blockage}\right], \tag{23}$$

since Bob's channel gain is equal to zero when blockage occurs, the secrecy capacity lower-bound in (16) under blockage reduces to:

$$\begin{aligned}\mathcal{C}_s^{1_{\mathrm{E}}}|\text{blockage} &\geq \int_{y=0}^{\kappa} \frac{1}{2} \ln\left(\frac{\sigma_E^2}{\zeta^2 P^2 y + \sigma_E^2}\right) f(y) dy \\ &\geq \int_{y=0}^{\kappa} \frac{1}{2} \ln(\sigma_E^2) f(y) dy - \int_{y=0}^{\kappa} \frac{1}{2} \ln(\zeta^2 P^2 y + \sigma_E^2) f(y) dy \\ &\geq \frac{1}{4} \ln(\sigma_E^2) \left(\operatorname{erf}\left(\frac{\sqrt{\kappa}-\mu}{\sqrt{2\sigma^2}}\right) + \operatorname{erf}\left(\frac{\sqrt{\kappa}+\mu}{\sqrt{2\sigma^2}}\right)\right) - \frac{1}{2}\ln(\zeta^2 P^2(\mu^2+\sigma^2)+\sigma_E^2).\end{aligned} \tag{24}$$

Thus, the total secrecy capacity under the assumption of link blockage evaluates to:

$$\ddot{\mathcal{C}}_s^{1_{\mathrm{E}}} \geq (1-\mathcal{P}_b)\,\mathcal{C}_s^{1_{\mathrm{E}}} + \frac{1}{4}\mathcal{P}_b \ln(\sigma_E^2) \left(\operatorname{erf}\left(\frac{\sqrt{\kappa}-\mu}{\sqrt{2\sigma^2}}\right) + \operatorname{erf}\left(\frac{\sqrt{\kappa}+\mu}{\sqrt{2\sigma^2}}\right)\right) - \frac{1}{2}\mathcal{P}_b \ln(\zeta^2 P^2(\mu^2+\sigma^2)+\sigma_E^2), \tag{25}$$

which gives the expression in (22), which completes the proof. □

3.2 Effect of Random Receiver Orientation

In the following, we derive the secrecy capacity while taking into account the random receiver orientation model in Section 2.4.

Proposition 3: Considering random receiver orientation, the secrecy capacity with the existence of a single eavesdropper can be lower-bounded as:

$$\begin{aligned}\tilde{\mathcal{C}}_s^{1_E} \geq\; &\frac{1}{4}\Upsilon(\kappa) b_H \iota_1 e^{-\frac{\mu_H}{b_H}} \left(e^{\frac{\mu_H}{b_H}} \log\left(\frac{e\mu_H^2 P^2 \zeta^2}{2\pi\sigma_B^2}\right) - 2\mathrm{Ei}\left(\frac{\mu_H}{b_H}\right)\right) \\ &+ \frac{1}{4}\Upsilon(\kappa) b_H \iota_1 e^{\frac{\mu_H-\kappa_H}{b_H}} \left(2e^{\frac{\kappa_H}{b_H}}\,\mathrm{Ei}\left(-\frac{\kappa_H}{b_H}\right) - \log\left(\frac{e\kappa_H^2 P^2 \zeta^2}{2\pi\sigma_B^2}\right)\right) \\ &- \frac{1}{4}\Upsilon(\kappa) b_H \iota_1 \left(2e^{\frac{\mu_H}{b_H}}\,\mathrm{Ei}\left(-\frac{\mu_H}{b_H}\right) - \log\left(\frac{e\mu_H^2 P^2 \zeta^2}{2\pi\sigma_B^2}\right)\right) \\ &+ b_H \iota_1 \left(-e^{\frac{\mu_H-\kappa_H}{b_H}} - e^{-\frac{\mu_H}{b_H}} + 2\right) \left(\frac{1}{4}\Upsilon(\kappa)\log\left(\sigma_E^2\right) - \frac{1}{2}\log\left(P^2\zeta^2\left(\mu^2+\sigma^2\right)+\sigma_E^2\right)\right),\end{aligned} \tag{26}$$

where $\iota_1 = \frac{1}{b_{\mathrm{H}}\left(2-\exp\left(-\frac{h_{\max}-\mu_{\mathrm{H}}}{b_{\mathrm{H}}}\right)\right)}$, and κ_H denotes the maximum value of h_B.

Proof. Considering random orientation, the secrecy capacity can be lower-bounded as:

$$\tilde{\mathcal{C}}_s^{1_E} \geq \int_{\tilde{h}=0}^{\kappa_H} f_H(\tilde{h}) \times \mathcal{C}_s^{1_{\mathrm{E}}}(\tilde{h})\, d\tilde{h}, \tag{27}$$

substituting $f_H(\tilde{h})$ from (10) and $\mathcal{C}_s^{1_{\mathrm{E}}}(\tilde{h})$ from (15) we get:

$$\begin{aligned}\tilde{\mathcal{C}}_s^{1_E} \geq &\int_{\tilde{h}=0}^{\kappa_H} \frac{1}{4} f_H(\tilde{h}) \Upsilon(\kappa) \ln\left(\frac{eP^2\zeta^2\tilde{h}^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2}\right) d\tilde{h} \\ &+ \int_{\tilde{h}=0}^{\kappa_H} f_H(\tilde{h}) \left(-\frac{1}{2}\ln\big((P^2\zeta^2(\mu^2+\sigma^2)+\sigma_E^2\big) + \frac{1}{4}\Upsilon(\kappa)\ln(\sigma_E^2)\right) d\tilde{h},\end{aligned} \tag{28}$$

the first integral can be written as:

$$
\begin{aligned}
&\frac{1}{4}\Upsilon(\kappa)\mathcal{F}_1(\tilde{h})|_{\tilde{h}=0}^{\mu_H}+\frac{1}{4}\Upsilon(\kappa)\mathcal{F}_2(\tilde{h})|_{\tilde{h}=\mu_H}^{\kappa_H}\\
=&\frac{1}{4}\Upsilon(\kappa)\left(\mathcal{F}_1(\mu_H)-\mathcal{F}_1(0)\right)+\frac{1}{4}\Upsilon(\kappa)\left(\mathcal{F}_2(\kappa_H)-\mathcal{F}_2(\mu_H)\right) \qquad (29)\\
=&\frac{1}{4}\Upsilon(\kappa)\left(\mathcal{F}_1(\mu_H)+\mathcal{F}_2(\kappa_H)-\mathcal{F}_2(\mu_H)\right),
\end{aligned}
$$

where

$$
\mathcal{F}_1=\int_{\tilde{h}=0}^{\kappa_H}\left(\iota_1\exp\left(\frac{\tilde{h}-\mu_{\mathrm{H}}}{b_{\mathrm{H}}}\right)+F_\theta(\theta)\delta(\tilde{h})\right)\ln\left(\frac{eP^2\zeta^2\tilde{h}^2+2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h}, \qquad (30)
$$

and

$$
\mathcal{F}_2=\int_{\tilde{h}=0}^{\kappa_H}\left(\iota_1\exp\left(\frac{-\tilde{h}+\mu_{\mathrm{H}}}{b_{\mathrm{H}}}\right)+F_\theta(\theta)\delta(\tilde{h})\right)\ln\left(\frac{eP^2\zeta^2\tilde{h}^2+2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h}. \qquad (31)
$$

Noting the property of delta function, we can see that

$$
\int_{\tilde{h}=0}^{\kappa_H}F_\theta(\theta)\delta(\tilde{h})\ln\left(\frac{eP^2\zeta^2\tilde{h}^2+2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h}=F_\theta(\theta)\int_{\tilde{h}=0}^{\kappa_H}\delta(\tilde{h})\ln(1)d\tilde{h}, \qquad (32)
$$

which evaluates to zero. Furthermore, we note that $\mathcal{F}_1(0)=0$. Using a high SNR approximation and integration by parts, we get:

$$
\mathcal{F}_1(\tilde{h})=b_H\iota_1e^{-\frac{\mu_H}{b_H}}\left(e^{\frac{\tilde{h}}{b_H}}\log\left(\frac{e\tilde{h}^2P^2\zeta^2}{2\pi\sigma_B^2}\right)-2\mathrm{Ei}\left(\frac{\tilde{h}}{b_H}\right)\right) \qquad (33)
$$

and

$$
\mathcal{F}_2(\tilde{h})=b_H\iota_1e^{\frac{\mu_H-\tilde{h}}{b_H}}\left(2e^{\frac{\tilde{h}}{b_H}}\mathrm{Ei}\left(-\frac{\tilde{h}}{b_H}\right)-\log\left(\frac{e\tilde{h}^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right). \qquad (34)
$$

Thus, the first integral in (28) reduces to:

$$
\begin{aligned}
&\frac{1}{4}\Upsilon(\kappa)b_H\iota_1e^{-\frac{\mu_H}{b_H}}\left(e^{\frac{\mu_H}{b_H}}\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)-2\mathrm{Ei}\left(\frac{\mu_H}{b_H}\right)\right)\\
&+\frac{1}{4}\Upsilon(\kappa)b_H\iota_1e^{\frac{\mu_H-\kappa_H}{b_H}}\left(2e^{\frac{\kappa_H}{b_H}}\mathrm{Ei}\left(-\frac{\kappa_H}{b_H}\right)-\log\left(\frac{e\kappa_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right) \qquad (35)\\
&-\frac{1}{4}\Upsilon(\kappa)b_H\iota_1\left(2e^{\frac{\mu_H}{b_H}}\mathrm{Ei}\left(-\frac{\mu_H}{b_H}\right)-\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right),
\end{aligned}
$$

The second integral in (28) evaluates to:

$$
b_H\iota_1\left(-e^{\frac{\mu_H-\kappa_H}{b_H}}-e^{-\frac{\mu_H}{b_H}}+2\right)\times\left(\frac{1}{4}\Upsilon(\kappa)\log\left(\sigma_E^2\right)-\frac{1}{2}\log\left(P^2\zeta^2\left(\mu^2+\sigma^2\right)+\sigma_E^2\right)\right). \qquad (36)
$$

Combining (35) and (36) we get the expression in (26), which completes the proof. □

4. RESULTS

In this section, we present Monte-Carlo simulations and analytic results to evaluate the secrecy performance under realistic channel assumptions, i.e., imperfect CSI for Eve, link blockage and random receiver orientation. We consider a LiFi system with the parameters listed in Table 1. Also, we assume that the blockers are uniformly distributed in the room. The blockers dimensions and density follow the parameters given in Table 1, where $k_b^1=0.2$ and $k_b^2=0.8$ indicate low and high blockers' density, respectively, as considered in.[20] The markers in the figures represent simulation results while the solid lines represent the analytical derivations.

Fig. 5 shows the effect of link blockage on the secrecy capacity for different simulation setups where L_B^1 and L_B^2 denote that Bob is in a standing or a setting position, respectively. We can see that simulation results are in close agreement with the analytic results in Proposition 1 for the case with no blockage as well as Proposition

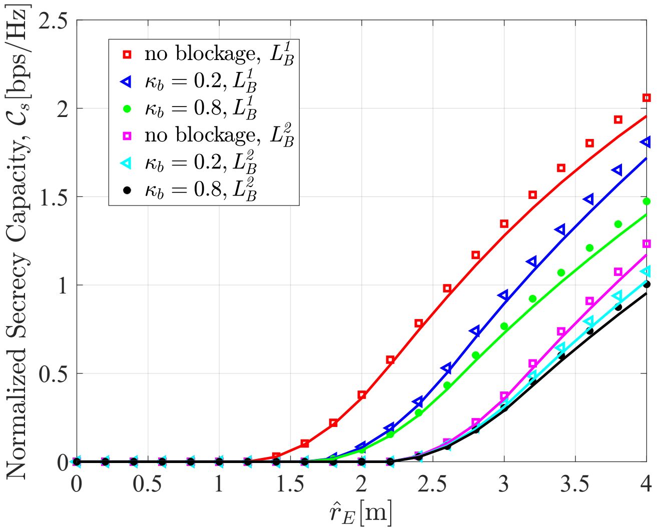

Figure 5. Effect of link blockage on the secrecy capacity.

2 for the scenario where link blockage is considered. It can be also seen that higher blockage probability, i.e. higher blockers' density, results in reduced secrecy performance.

Next, we examine the effect of receiver orientation in Fig. 6. We can see that simulation results are in agreement with the analytic results expressed in Proposition 3. It can be seen that random receiver orientation significantly reduces the secrecy performance compared to a fixed orientation scenario, i.e., when the receiver device is assumed to be directed vertically upwards. For the case of the user location L_B^1, random receiver orientation results in almost 25% degradation in the secrecy capacity compared to the scenario with fixed receiver orientation. This highlights the importance of considering the random behaviour of the optical channel when designing secrecy mechanisms for LiFi systems.

Table 1. Simulation Parameters

Description	**Notation**	**Value**
Transmit SNR	ρ	120 dB
Transmitter semi-angle	φ_k	60 deg
FOV of the PDs	ϕ_{c_k}	90 deg
Physical area of PD	A_k	1.0 cm^2
Refractive index of PD lens	n	1.5
Gain of optical filter	$T_s(\phi_k)$	1.0
Alice location	L_A	$(0.0, 0.0, 2.5)$ m
Blocker height	h_b	1.75 m
Blockers' radius	l_b	0.15 m
Blockers' density (non-dense)	k_b^1	0.2
Blockers' density (dense)	k_b^2	0.8

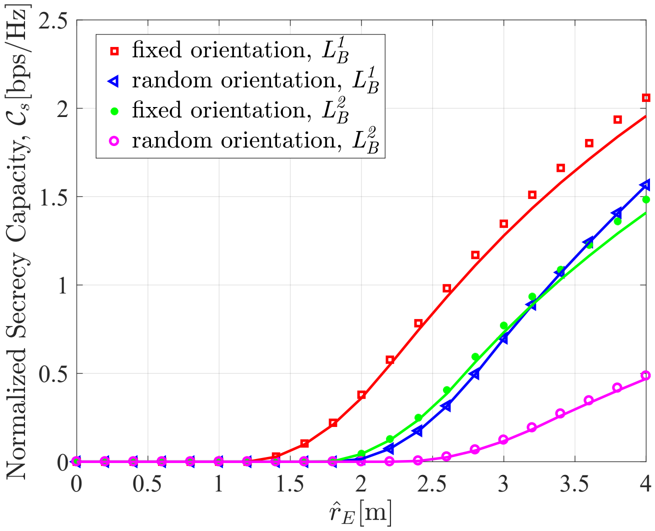

Figure 6. Effect of random receiver orientation on the secrecy capacity.

5. CONCLUSION

In this paper, we provided lower bounds for the secrecy capacity in realistic LiFi systems when imperfect CSI of the eavesdropper, the probability of link blockage and random device orientation were considered. We showed that these random factors can have a significant effect on the secrecy capacity and, thus, need to be taken into account in order to enhance the security of LiFi links. For example, the existence of high density blockers or random receiver orientation can lead to a 25% loss in the secrecy capacity. We believe that designing secrecy measures for LiFi systems based on these realistic assumptions can enhance the secrecy capacity and make the system more robust to the random adverse factors in the optical channel. Our future work will evaluate the realistic secrecy performance when multiple eavesdroppers attempt to decode the legitimate user's signal. Also, we will investigate PLS design where resource allocation and access point selection is performed based on maximising the achievable secrecy capacity by employing the expressions derived in this paper.

REFERENCES

[1] "Cisco visual networking index: Forecast and trends, 2017-2022," tech. rep., Cisco (Feb. 2019).

[2] Ayyash, M., Elgala, H., Khreishah, A., Jungnickel, V., Little, T., Shao, S., Rahaim, M., Schulz, D., Hilt, J., and Freund, R., "Coexistence of WiFi and LiFi toward 5G: concepts, opportunities, and challenges," *IEEE Commun. Mag.* **54**(2), 64–71 (2016).

[3] Figueiredo, M., Alves, L. N., and Ribeiro, C., "Lighting the wireless world: The promise and challenges of visible light communication," *IEEE Consum. Electron. Mag.* **6**(4), 28–37 (2017).

[4] Kahn, J. M. and Barry, J. R., "Wireless infrared communications," *Proceedings of the IEEE* **85**, 265–298 (Feb. 1997).

[5] Obeed, M., Salhab, A. M., Alouini, M., and Zummo, S. A., "Survey on physical layer security in optical wireless communication systems," in [*2018 Seventh International Conference on Communications and Networking (ComNet)*], 1–5 (Nov. 2018).

[6] Arfaoui, M. A., Soltani, M. D., Tavakkolnia, I., Ghrayeb, A., Safari, M., Assi, C. M., and Haas, H., "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surveys Tuts.* **22**(3), 1887–1908 (2020).

[7] Mostafa, A. and Lampe, L., "Physical-layer security for indoor visible light communications," in [*2014 IEEE International Conference on Communications (ICC)*], 3342–3347 (June 2014).

[8] Mostafa, A. and Lampe, L., "Securing visible light communications via friendly jamming," in [*2014 IEEE Globecom Workshops (GC Wkshps)*], 524–529 (Dec. 2014).

[9] Shen, H., Deng, Y., Xu, W., and Zhao, C., "Secrecy-oriented transmitter optimization for visible light communication systems," *IEEE Photon. J.* **8**, 1–14 (Oct. 2016).

[10] Arfaoui, M. A., Ghrayeb, A., and Assi, C. M., "Secrecy performance of multi-user MISO VLC broadcast channels with confidential messages," *IEEE Trans. Wireless Commun.* **17**(11), 7789–7800 (2018).

[11] Zhao, X., Chen, H., and Sun, J., "On physical-layer security in multiuser visible light communication systems with non-orthogonal multiple access," *IEEE Access* **6**, 34004–34017 (2018).

[12] Soltani, M. D., Purwita, A. A., Zeng, Z., Haas, H., and Safari, M., "Modeling the random orientation of mobile devices: Measurement, analysis and LiFi use case," *IEEE Trans. Commun.* **67**, 2157–2172 (March 2019).

[13] Jain, I. K., Kumar, R., and Panwar, S. S., "The impact of mobile blockers on millimeter wave cellular systems," *IEEE J. Sel. Areas Commun.* **37**(4), 854–868 (2019).

[14] Dong, K., Liao, X., and Zhu, S., "Link blockage analysis for indoor 60 GHz radio systems," *Electronics Letters* **48**, 1506–1508 (Nov.r 2012).

[15] Yin, L. and Haas, H., "Physical-layer security in multiuser visible light communication networks," *IEEE J. Sel. Areas Commun.* **36**, 162–174 (Jan. 2018).

[16] Marshoud, H., Sofotasios, P. C., Muhaidat, S., Karagiannidis, G. K., and Sharif, B. S., "On the performance of visible light communication systems with non-orthogonal multiple access," *IEEE Trans. Wireless Commun.* **16**, 6350–6364 (Oct. 2017).

[17] Ying, K., Qian, H., Baxley, R. J., and Yao, S., "Joint optimization of precoder and equalizer in MIMO VLC systems," *IEEE J. Sel. Areas Commun.* **33**, 1949–1958 (Sep. 2015).

[18] Ma, H., Lampe, L., and Hranilovic, S., "Coordinated broadcasting for multiuser indoor visible light communication systems," *IEEE Trans. Commun.* **63**, 3313–3324 (Sep. 2015).

[19] Wang, J., Liu, C., Wang, J., Wu, Y., Lin, M., and Cheng, J., "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Trans. Commun.* **66**, 6423–6436 (Dec. 2018).

[20] Soltani, M. D., Wu, X., Safari, M., and Haas, H., "Bidirectional user throughput maximization based on feedback reduction in LiFi networks," *IEEE Trans. Commun.* **66**, 3172–3186 (July 2018).